The Pennsylvania State University
The Applied Research Laboratory
P.O. Box 30
State College, PA 16804

Understanding Security
Update 4

By
Brice A. Toth
Caleb Severn
Jonathan Hoerr

Technical Report No. TR 13-003
5 March 2015

Supported By:

Office of the Secretary of Defense Rapid Reaction Technology Office
Contract No. N00024-12-D-6402/0078

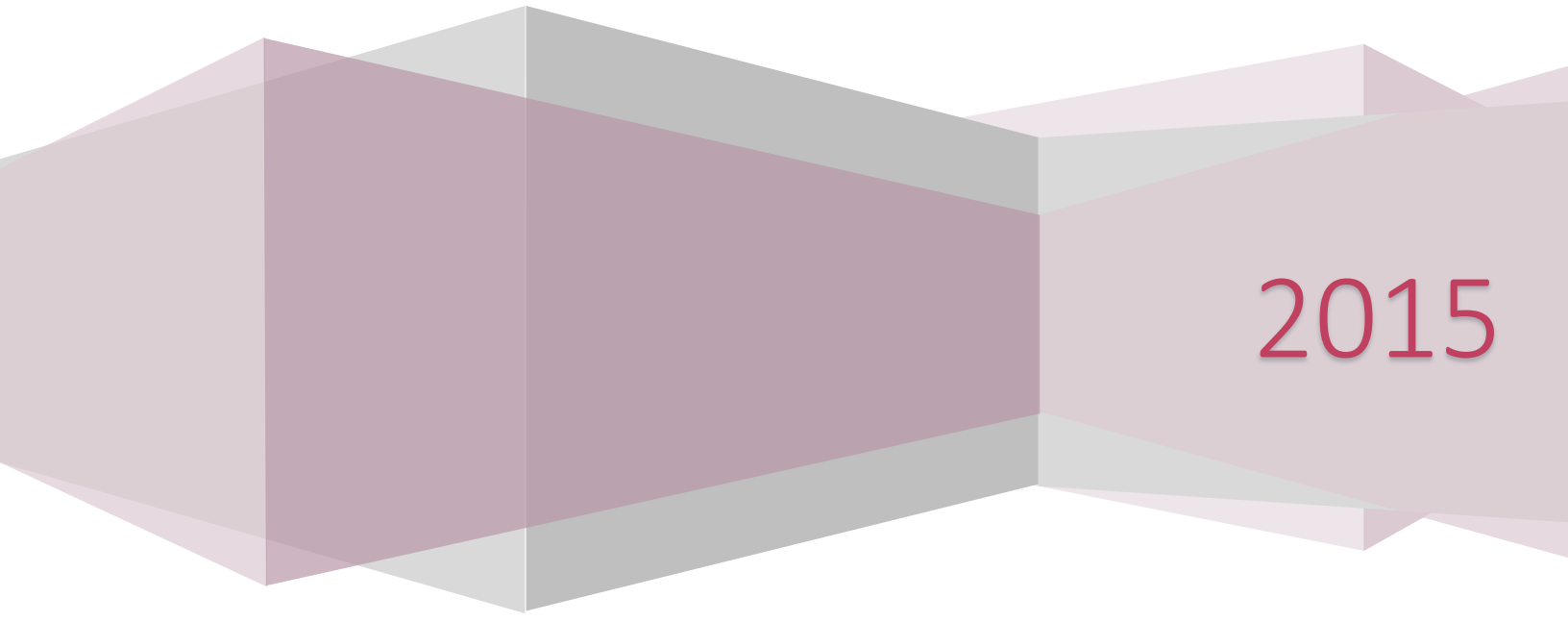
ABSTRACT

Understanding Security is targeted to incite immediate action to secure the critical information held at Small to Medium Businesses (SMBs). Special focus is given throughout to establish business value that will drive substantive action. First, the realities of escalating informational threats to SMBs are illuminated through examples and details of attacks. Second, a list of '100 things under $100' that can be done to mitigate risks and vulnerabilities is provided. The inclusion of specific measures in this list follows the findings of a survey of small businesses and a realistic assessment of the current state of security and the expertise and capabilities possessed by SMBs. Context and sufficient technical detail are provided for espionage techniques, organizational policies and contemporary computer technologies to allow managers to understand the driving factors for these measures.

Applied Research Laboratory
The Pennsylvania State University

Understanding Security

Brice A. Toth
Caleb J. Severn
Jonathan Hoerr



2015

Disclaimer

The Applied Research Laboratory provides this document as a guideline for solutions to computer security threats. Implementation of any of the suggestions herein is performed at the sole risk of the implementer. ARL does not warrant explicitly nor implicitly that these suggested protections will completely protect the implementer's data and systems.

Further dissemination of this document is prohibited without the written permission of the Applied Research Laboratory.

Acknowledgements

This work was supported by the Office of the Secretary of Defense through the Rapid Reaction Technology Office. The content of the information does not necessarily reflect the position or policy of the Government, and no official endorsement should be inferred.

About the Authors

Brice Toth is a project manager and software engineer at the Applied Research Lab (ARL) at the Pennsylvania State University. For more than fifteen years, Brice has developed software and infrastructure solutions for both ARL and external customers. His recent projects have focused on network security for pilot programs under the Office of the Secretary of Defense.

Caleb Severn is a PhD student in computer science at the Pennsylvania State University. In addition to basic research in network simulation and evaluation, Caleb develops training materials and security publications at the ARL. Over the previous decade, Caleb worked in control networks and industrial security.

Jonathan Hoerr is an administrator and software engineer at the ARL at the Pennsylvania State University. Jonathan heads development of security-critical web applications for pilot programs under the Office of the Secretary of Defense. Jonathan specializes in cloud infrastructure and web security.

Executive Summary

The Approach of Understanding Security

In the fast moving, globalized world, maintaining a strong and leading national security capability requires developing not just new technology but also new approaches to protecting information advantage. The majority of technological innovations occur at small to medium businesses (SMBs). This endows SMBs with an inherent value as targets for espionage. Despite this inherent importance, in the past the SMBs that hold valuable patents and trade secrets had largely been buffered from the brunt of government- and corporate-sponsored espionage. This is no longer the case.

The approach of *Understanding Security* is to incite immediate action to secure the critical information held at SMBs. Four key points establish the necessity of substantive information security at SMBs.

- Adversaries are numerous and determined. This fact has been made widely known by reports in popular media of Advanced Persistent Threats (for example APT-1 reported by Mandiant), Anonymous, and other sophisticated adversaries. Major data breaches that expose the personal or financial information of tens of millions of customers are also grabbing headlines and costing those companies hundreds of millions of dollars.
- Almost all SMBs are already being targeted. SMBs can realistically expect to be attacked, even if they have multiple degrees of separation from any customer that is a major defense supplier. Phishing emails, social engineering and other popular techniques for the initial penetration of an organization are explained in detail later. The realization that phishing and other attacks are already happening, and the consequences of these attacks, arouse management at SMBs to acknowledge the cumulative threat posed by ongoing attacks.
- Vulnerabilities are abundant. The vast majority of attacks exploit glaring lapses in controls and procedures or computer configurations. Common vulnerabilities are often known or open issues at SMBs. Example attack techniques are illuminated to stimulate energy and priority in mitigating such vulnerabilities.
- Mitigations against most attacks are neither expensive nor difficult. It is estimated that four mitigation techniques can prevent 85% of attacks [1]. Other publications give similar estimates. Security is part of risk management and the investment required to achieve a sensible security posture will almost surely have a positive return on investment.

The Contribution of Understanding Security

Technological Solutions for Manufacturing Advanced Products (TSMAP) is an endeavor to understand and facilitate new ways to develop and source military technologies. As one component of TSMAP, *Understanding Security* acts to secure the increasingly distributed defense supply base by communicating practical security practices to SMBs. These efforts are sponsored by the Office of the Secretary of Defense Rapid Reaction Technology Office.

The bulk of the information here entails a list of *100 things under $100* (and growing, now 160 things) that can be done in the short term to harden real information systems at SMBs. The intention of distributing this list is to impart the expertise needed to upgrade information security systems from completely unprotected to moderately protected or better, given resource constraints on SMBs. This list also demonstrates that this upgrade can be done quickly and with minimal personnel requirements and cash outlay. Every technique is accompanied by an estimated priority, difficulty and efficacy so that a security upgrade can begin with solid first steps without the organization necessarily developing a comprehensive risk analysis and security plan beforehand.

The techniques in *Understanding Security* have been refined throughout a campaign to observe, audit and converse with small defense suppliers. One central finding is that SMBs have limited resources to implement security, often including only part-time IT personnel. A common trend also emerges that executives at SMBs have heard of attacks, infection of networks, and information theft. There is also a vague impression that action is required. However, the actual form of attacks, and how to detect these attacks, remains unknown. Beyond this, most popular treatment of cyber security relegates mitigation to procuring a managed enterprise firewall, or outside consultation, and considering the problem to be solved. In contrast to the message of *Understanding Security*, this treatment encourages apathy at SMBs where budget space for security products, consultations, or subscriptions does not exist.

High-cost issues, such as detailed considerations for implementing a formal training program, institutional architecture for layered security, etc. are largely omitted here. This is due, in part, to the observation that the existing literature is biased to a large business model and so existing coverage of higher-level issues is better than that for practical techniques. References are given to several such publications for the benefit of those organizations that wish to take further steps toward reaching the next level of security.

Why Small Business Needs Security

One important reason for the lack of interest in stealing from SMBs in the past was the high degree of separation between intellectual property and monetizable technology. In many cases, a long and expensive phase of product development follows procurement of an SMB, and its promising intellectual property, by a larger organization. In this common case, by the time the market value of a technology has been demonstrated the associated intellectual property has already been secured under the umbrella protection of a larger organization.

In this light, the process of integrating SMBs into the defense supply chain can be viewed as two contrary flows of information. Intellectual property flows up the supply chain to the pinnacle suppliers and military. Concurrently, a wide selection of best practices flow downward to the SMBs, including security practices.

Why the Threat Topology has changed

Three factors now combine to make information security a crucial action item for SMBs. First, changes to the procurement strategy of the U.S. military have interrupted the traditional counter-flow of security practices. Budget pressures and shorter lead times have forced the military supply structure to transition to horizontal markets. Accordingly, the defense supply

base has become more distributed, often with top-tier suppliers performing only final integration. Innovation continues to flow upward to the military, but new products are delivered faster and at lower prices. Unfortunately, the traditional counter-flow of security practices is interrupted when components are delivered as commodities from SMBs.

The result is that much of the intellectual property, critical defense supply and utility infrastructure are managed by companies that self-identify as neither critical nor defense companies. Further, these companies often do not allocate substantial resources to information security, and often do not know what security measures should be implemented or how to do so. The result is prime targets that are heretofore oblivious to being targets. This leads to higher risk for the entire supply chain.

Second, large-tier defense suppliers have worked diligently over more than a decade to become more secure. The result is a widened gap in the hardness of information systems between large corporation and SMB models. This widened gap leaves SMBs as even more opportune targets than they were in the past. Aside from the valuable information directly held at SMBs, indirect attack techniques like cross-site scripting and waterholing provide attack vectors into the defense supply chain through low-tier suppliers and even newsgroups, payroll, and other websites operated by organizations that do not invent or manufacture anything.

Third, the costs of espionage have decreased considerably. As with government surveillance, in the past the limiting factor for espionage was the cost of doing so. The internet has made casting a wide net feasible. The highly connected nature of the modern office has opened the internal human and physical organization of naïve SMBs to the internet, easing information gathering in preparation for targeted espionage.

Security as a Business Plan

One hurdle to overcoming apathy with regard to securing and self-monitoring networks at SMBs is the need to demonstrate the value of security at the bottom-line of SMBs. The loss or realistic threat of loss of competitive information is one motivation. Reports of espionage during competitive bid processes have become commonplace. Intellectual property and residual sales are also at risk from mundane threats like vendor theft and disgruntled employees. Such issues are poorly handled by ad hoc departmental actions and signal for a security plan.

Beyond this, defense, aerospace, medical, financial and other industries have begun to rollout mandatory, minimal security practices for all vendors. These minimum practices will increasingly be enforced as contractual obligations, such as with the Defense Federal Acquisition Regulation Supplement (DFARS). *Understanding Security* provides a mapping to NIST 800-53 and DFARS for the benefit of suppliers who are subject to that clause. Industry standards and legal regulations govern the prudent handling of personal information in many jurisdictions.

Finally, 'best practice' in security has stabilized. The top techniques and critical controls from U.S. [2] [3] [4] [5] and foreign [1] bodies are now aligned and have already become de facto standards. Following this regularization of definitions, precedent for prudent procedural consideration for information security can be established. Reasonable expectation of secure information handling, analogous to the reasonable expectation of prudent procedural consideration for safety, is a legal precedent facing all organizations in the very near future.

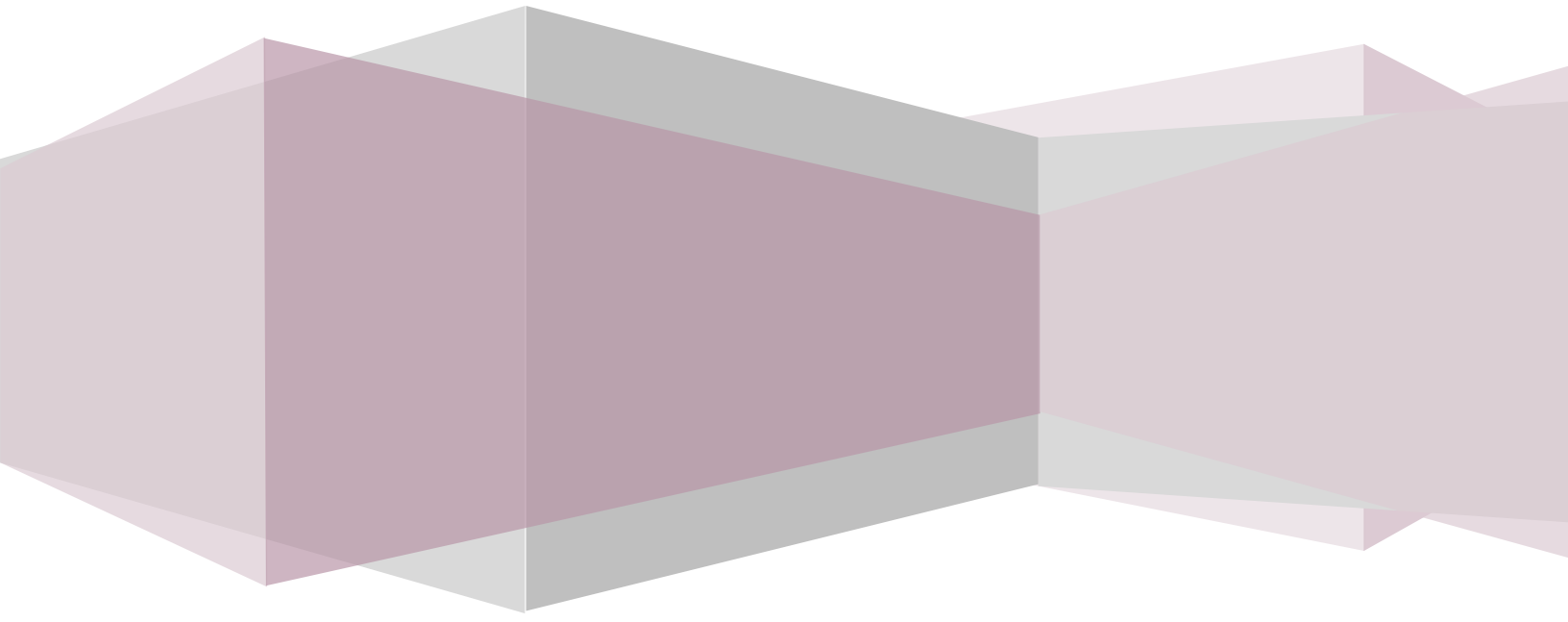
Table of Contents

Applied Research Laboratory
The Pennsylvania State University

Understanding Security

INTRODUCTION TO THE SERIES

Brice A. Toth
Caleb J. Severn
Jonathan Hoerr



About the Series

Purpose of the Series

Industrial espionage and state-sponsored cybertheft have become widespread. Hackers have found soft targets in the vulnerable computer infrastructure guarding critical information. Large organizations have moved to increase security, leaving smaller organizations as more attractive targets. In response, the US Department of Defense (DoD) has moved to secure its supply base. The *Understanding Security* series of documents results from one such initiative, Technological Solutions for Manufacturing Advanced Products, sponsored by the Office of the Secretary of Defense Rapid Reaction Technology Office.

The *Understanding Security* series is intended to provide guidance for small to medium businesses as they attempt to harden their organizations against information threats. The strategy of *Understanding Security* is to provide concrete, actionable, self-contained tips for hardening information systems in the short term. Accordingly, the tips included here require a minimum of investment in infrastructure or expertise. This approach is in contrast to security standards that aim to define either metamodels for security or templates for self-enforcement or auditing [3] [1] [4].

Immediate actions being the end goal, specific product offerings are discussed. These offerings are a sample of those available, and are given to provide, at minimum, a contact point to get started. Free or low-cost products are favored, where available. This product information is freely available industry knowledge. Inclusion of a product here does not constitute the official endorsement of any governmental or standards body.

Intended Audience

For the purposes of the *Understanding Security* series, organizations can be categorized into one of three designations.

- Small-Tier organizations have neither full time, dedicated IT staff nor dedicated computer security staff. This designation includes organizations with part time IT staff or IT staff who share time with responsibilities in other disciplines.
- Mid-Tier organizations have full time, dedicated IT staff but no dedicated computer security staff.
- Large-Tier organizations have full time, dedicated computer security staff.

Understanding Security is applicable to any small to medium business. However, the specific target audience is owners and IT managers at Small-Tier and Mid-Tier DoD suppliers who need guidance to comply with evolving security expectations for defense contractors. While some information herein might prove useful, *Understanding Security* is not targeted for Large-Tier organizations. Understanding Security does not provide guidance for creating classified information systems.

A survey of DoD suppliers found a high proportion of Small-Tier organizations. Small-Tier organizations were also found to have the softest information infrastructure. Accordingly, the security tips included here are organized by the tiers above to make clear what security practices apply to the information security of even the smallest organizations.

What to Expect from the Volumes

While news about widespread cyber-attacks might be unsettling, the first steps to actually implementing information security for one's own company might not be obvious. This barrier can inhibit even launching an effort. Each volume of this series strives to provide an accessible list of tips to overcome this barrier and jumpstart small business security.

Terms like 'cyber-security' or 'anti-virus' are used frequently, but information security is a more general issue that encompasses the entire effort to secure organizational assets. Likewise, the methods of computer security are part of a comprehensive information security system, and both complement and extend traditional physical security.

Consequently, 'Step 0' to implementing information security is to understand the requirements at a high level and the functional analogy between the methods of physical and computer security. Like door locks and security cameras for a building, many tools can harden a computer system to attack or aid forensic analysis of an attack. However, as with an access door left unlocked, the tools of computer security do little good if prudent procedures and policies are not established and followed. Even before a procedure for securing a facility can be created, an inventory of all entry points must be completed. Likewise, before a network can be secured, all IT assets must be inventoried.

The first volumes of this series address the primary concerns of an organization that is beginning a security upgrade.

Information Asset Inventory

To effectively protect its informational assets, an organization must first know what information it possesses, what information is sensitive, what security and IT assets it possesses, and consolidate disparate knowledge of known vulnerabilities so that these can be addressed. Eventually, when deciding the prudent level of investment to protect assets, the impact of compromise of these assets must be established. This volume provides a checklist of common assets that must be recorded.

Training and Policies

Organizational architecture and culture are more difficult to 'upgrade' than hardware and software. Nevertheless, the reality is that good security tools minimally require knowledgeable setup and often trained operators to be useful. Worse, untrained employees who misunderstand or begrudge security policy are not only the weak link in information security, but possibly active adversaries. These tips explain and motivate some important security training and policies for small business.

Tools and Configurations

The inclination of most small business owners when initiating a security upgrade is to look at both new tools and hardening existing equipment. New tools promise to find network backdoors, automatically patch software vulnerabilities, etc. These tips list some industry-proven and indispensable security tools that help administrate a secure computing ecosystem. In many cases, existing infrastructure can be 'upgraded' by hardening configurations to plug security holes.

Organization of a Volume

Each volume is broken into two top-level categories. A Small-Tier organization should be able to implement Small-Tier tips. A Mid-Tier organization should be able to implement both Small-Tier and Mid-Tier tips.

The information in the volumes is broken into small sections that should be readable in one sitting. We refer to these small sections as tips.

- A security tip is self-contained, or nearly so.
- Each tip includes one or more security techniques and enough detail to understand at a high level the 'why' and 'how' of the techniques.
- Techniques are summarized in a table at the beginning of each tip.
- When not everyday knowledge, a tip will include motivation for adopting the techniques, often by examples of vulnerabilities or exploits thereby remedied.

Security Technique

- Each technique is a functional decomposition down to a level that should be easily broken into concrete tasks. For example, controlled access could be broken down into installing paddle locks on every external door and adding an automatic gate to the driveway.
- Each technique will identify the business value, recommended priority, expected effectiveness and end user of the technique to aid making a wish list of upgrades.
- Costs are broken down into employee morale, upfront expense (combined cash and labor), and ongoing maintenance (combined).

Summary of Security Techniques

Below is an itemized summary of the mitigation techniques that are suggested throughout the volumes of *Understanding Security*. This list adopts a process-centric perspective in that 'priority' here is priority for scheduling upgrades. In short, this list is ordered by what works best and is easiest to implement immediately. This approach is in contrast to prioritizing by ultimate importance, and reflects the overall approach of *Understanding Security* to encourage small businesses to plug as many holes as fast as they can. A similar 'quick win' approach is used for prioritization in [6].

For the benefit of organizations that have a long-standing commitment to security but need to evolve priorities, it is instructive to consider how this list compares to a similar list five or ten years ago. Inertial attacks and daily compromise of infrastructure and industrial controls are now realities in the wild. Awareness and preparation for attacks on industrial networks and physical controls lag that for traditional IT targets. In the traditional IT realm, fallback techniques like virus scanning are now bypassed by most targeted attacks and so drop in priority. In fact, training and the human element have increased in priority relative to technical fortifications as a whole; this follows modern trends that show a majority of initial penetrations exploit human weakness rather than software flaw or configuration error.

Each line item here references a corresponding technique on the indicated page. Further explanation and motivation can be found in the discussion there.

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
1	PT.PAS.2	37	**Password composition** rules ensure minimum complexity	High	High	Medium	Low	Low
2	PT.ACC.4	42	**Computer timeout** mitigates vulnerability from non-conformance in locking computers	High	High	Low	Low	Low
3	PT.SUP.1	64	**Manual updates** reduce the frequency of compromise of infrastructure and industrial controls	High	High	Low	Low	Low
4	PT.SUP.2	64	**Automatic updates** patch the vulnerabilities exploited by most malware	High	High	Low	Low	Low
5	PT.SWI.4	66	**Minimal installation** reduces vulnerability surface for all computers	High	High	Medium	Low	Low
6	PT.REM.1	75	**Encrypted connections** mitigate the threat of eavesdropping on credentials and data even locally	High	High	Low	Low	Low
7	PT.ROL.8	100	**Account reclamation** mitigates threats from former or disgruntled employees	High	High	Low	Low	Low
8	TC.CSH.1	117	**Infrastructure password** reduces unauthorized access by anonymous clients or by using default password	High	High	Low	Low	Low
9	TC.WLK.5	119	**Isolating development systems** reduces the frequency of vulnerable testing systems appearing on visible networks	High	High	Medium	Low	Low
10	TC.FIR.1	137	**Simple firewall** rules reduce configuration errors and harden firewall configuration	High	High	Low	Low	Low
11	TC.WRL.1	139	**Hardened Wi-Fi** configuration prevents many known attacks	High	High	Low	Low	Low
12	PT.PAS.3	37	**Password expiration** mitigates damages from credential compromise	High	High	Medium	Low	Medium
13	PT.DCT.5	71	**Device sanitization** mitigates the vector for information loss through discarded, resold or transferred devices	High	High	Low	Low	Medium
14	PT.ACC.1	42	**Controlled physical access** to sensitive assets is a prerequisite to most other security measures	High	High	Low	Medium	Low
15	PT.SUP.3	64	**Domain version control** reduces effort to manage patch versioning and enforces conformity	High	High	Low	Medium	Low

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
16	PT.DIN.1	68	**Automatic backup** reduces the frequency of accidental data loss	High	High	Low	Medium	Low
17	PT.PAS.6	86	**Role-based accounts** increase the security of sensitive operations and critical accounts	High	High	Medium	Medium	Low
18	PT.ROL.3	96	**Role-based permissions** mitigates vulnerability to multi-vector attacks and reduces damages from breach of a system	High	High	Medium	Medium	Low
19	TC.WLK.6	119	**Isolating industrial networks** mitigates threat of attacks on the most vulnerable and critical systems	High	High	Low	Medium	Low
20	TC.SIM.2	154	**Centralized configuration policy** enforces security policy across a domain and reduce nonconforming configurations	High	High	Medium	Medium	Low
21	PT.BUY.1	35	**Employee buy-in** and self-monitoring require training in the business impact of security failures	High	High	Low	Medium	Medium
22	PT.PHY.1	48	**Document shredding** reduces information loss through refuse	High	High	Medium	Medium	Medium
23	PT.DCT.4	71	**Encryption key management** reduces the probability of massive data loss or bulk theft	High	High	Low	Medium	Medium
24	TC.HST.4	124	**Application whitelisting** mitigates threat due to abundant sources of executable files	High	High	High	Medium	Medium
25	PT.PAS.4	37	**Account lockout** eliminates trivial password cracking attacks from frontend interfaces	High	Medium	Medium	Low	Low
26	PT.ACC.5	42	**Visitor sign in** demonstrates security expectations, increases conformance and aids investigation	High	Medium	Low	Low	Low
27	PT.PSH.5	55	**Incoming email filtering** removes bulk malicious email	High	Medium	Low	Low	Low
28	PT.PSH.6	55	**Late email filtering** mitigates waterholing threat	High	Medium	Low	Low	Low
29	PT.SWI.2	66	**Newest browser** reduces frequency of infection when browsing	High	Medium	Low	Low	Low
30	PT.SWI.3	66	**Baseline installation** reduces nonconformance by establishing secure settings for use by most employees	High	Medium	Medium	Low	Low
31	PT.REM.2	75	**Remote authentication** reduces frequency of remote intrusion and mitigates risks from third-parties	High	Medium	Low	Low	Low
32	PT.REM.3	75	**Remote roles** reduce attack surface and slow penetration during attacks from outside accounts	High	Medium	Low	Low	Low
33	TC.CSH.2	117	**SNMP audit** mitigates SNMP as an attack vector or minimally increases cost of malicious information gathering	High	Medium	Low	Low	Low
34	TC.CSH.3	117	**Minimal embedded servers** mitigates unused services as attack vectors and vulnerabilities in embedded servers	High	Medium	Low	Low	Low
35	TC.CSH.5	117	**Disable legacy services** mitigates the threat of eavesdropping	High	Medium	Low	Low	Low
36	TC.HST.3	124	**Automatic host scanning** maximizes the probability of detecting malware before it embeds itself	High	Medium	Low	Low	Low
37	TC.APP.1	127	**Secure browsers** reduce the frequency of infection from websites	High	Medium	Medium	Low	Low
38	TC.APP.2	127	**Streamlining application features** mitigates the majority of vulnerabilities	High	Medium	Medium	Low	Low
39	TC.APP.3	127	**Streamlining services** mitigates vectors to access and move across a network	High	Medium	Low	Low	Low
40	TC.APP.4	127	**Disabling autoplay** mitigates vulnerability due to removable media, especially for air-gapped networks	High	Medium	Low	Low	Low
41	TC.WRL.3	139	**Access point scanning** mitigates vulnerability due to wireless breaches and spoofed networks	High	Medium	Medium	Low	Low
42	TC.PEN.1	157	**Vulnerability scanning** identifies commonly exploited vulnerabilities	High	Medium	Low	Low	Low
43	TC.WAP.1	160	**Server scanning** identifies most common server vulnerabilities	High	Medium	Low	Low	Low

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
44	TC.IDS.3	162	**Packet monitoring** improves detection of initial infiltration activities and detection of compromised machines, limits exfiltration to external machines	High	Medium	Low	Low	Low
45	PT.SEN.5	52	**Pre-employment screening** reduces the frequency of inside adversaries	High	Medium	Low	Low	Medium
46	PT.PSH.7	55	**Client email filtering** mitigates email and website threats	High	Medium	Medium	Low	Medium
47	PT.PSH.8	55	**Attachment whitelisting** blocks most malware formats	High	Medium	Medium	Low	Medium
48	TC.HST.2	124	**Host intrusion detection** helps identify ongoing infection and slows infection progress	High	Medium	Medium	Low	Medium
49	TC.HST.1	124	**Host security suite** mitigates threats from most common malware and prevents most malware command connections	High	Low	Medium	Low	Medium
50	PT.PAS.1	37	**Password awareness** training reduces bad passwords, cheating, and disclosure	High	Medium	Low	Medium	Low
51	PT.SUP.4	64	**Update Management** improves patch regularity and response	High	Medium	Low	Medium	Low
52	PT.DIN.5	68	**Backup encryption** prevents leakage vectors through information storage	High	Medium	Low	Medium	Low
53	PT.REM.6	80	**Protocol enforcement** eliminates many vulnerabilities by forcing usage of newer protocols	High	Medium	Low	Medium	Low
54	PT.ROL.6	100	**Centralized account management** mitigates threats due to lost or compromised accounts	High	Medium	Medium	Medium	Low
55	PT.SRD.1	108	**Security roles** reduce the number of known issues and the frequency of oversights	High	Medium	Medium	Medium	Low
56	TC.WLK.1	119	**Eliminating obsolete machines** mitigates the most frequently exploited vulnerabilities	High	Medium	Low	Medium	Low
57	TC.WLK.2	119	**Eliminating obsolete protocols** reduces lingering vulnerabilities on largely updated networks	High	Medium	Low	Medium	Low
58	TC.WLK.3	119	**Eliminating rogue machines** eliminates the easiest targets on a network	High	Medium	Medium	Medium	Low
59	TC.WLK.4	119	**Eliminating temporary configurations** eliminates the easiest targets on a network	High	Medium	Medium	Medium	Low
60	PT.SME.3	61	**Social media password controls** reduces frequency of site hijacking	Medium	High	Medium	Low	Low
61	PT.DIN.3	68	**Device backup** mitigates the risk if accidental data loss	Medium	High	Medium	Low	Low
62	PT.REM.7	80	**Layered encryption m**itigates the threat of many attacks on encrypted connections	Medium	High	Medium	Low	Low
63	PT.CLO.2	82	**Cloud location guarantees** are necessary for government data or any location-sensitive data	Medium-High	High	Low	Low	Low
64	PT.DEV.5	91	**Remote sanitation** reduces the scope for physical attacks on misplaced devices	Medium	High	Low	Low	Low
65	TC.CSH.4	117	**Inventoried ports i**ncreases efficacy of network scans	Medium	High	Low	Low	Low
66	PT.DIN.2	68	**Offsite backup** provides integrity guarantees for data that must survive a single facility	Medium	High	Low	Medium	Low
67	PT.DEV.4	91	**Removable media encryption** reduces information loss by lost devices and travel incidents	Medium	High	Medium	Low	Medium
68	PT.DEV.8	94	**Travel laptops** reduce exposure of information during travel	Medium	High	Medium	Medium	Low
69	PT.DEV.10	94	**Pre-travel drive imaging** facilitates forensic analysis of loss incidents	Medium	High	Low	Low	Medium
70	TC.CAC.1	130	**Electronic File shredding** reduces risks from residual copies on disk	Medium	High	Medium	Low	Medium
71	TC.INV.4	148	**Secure network architecture** hardens an entire network and protects the most sensitive systems	Medium	High	Medium	Medium	Low
72	TC.HDD.1	152	**Drive destruction** mitigates loss vectors through used electronics	Medium	High	Low	Medium	Low
73	TC.HDD.2	152	**Drive degaussing** is the required destruction method for defense contractors	Medium-High	High	Low	Medium	Low
74	PT.BUY.2	35	**Procedural guidance** for every employee role increases conformance and reduces the frequency of incidents	High	Medium	Medium	Medium	High
75	PT.PHY.6	48	**Physical penetration testing** identifies threats to physical security	High	Medium	Low	Medium	Medium
76	PT.SEN.2	52	**Access control awareness** training increases the veracity of employee enforcement of access control, reduces the rate of success of tailgating and other infiltration behaviors	High	Medium	Low	Medium	Medium

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
77	PT.SEN.3	52	**Vendor vetting** reduces the frequency of physical intrusion by impostors	High	Medium	Medium	Medium	Medium
78	PT.SWI.1	66	**Newest OS version** increases the hardness of installations	High	Medium	Low	Medium	Medium
79	PT.CAC.1	73	**Collaboration awareness** training reduces the frequency of information spillage by unsecure communication	High	Medium	Medium	Medium	Medium
80	PT.DEV.7	94	**Travel awareness** training reduces infection on hostile networks and loss while traveling	High	Medium	Low	Medium	Medium
81	PT.RAC.3	105	**Reliability engineering** decreases the rate of failure and increases the availability of systems	High	Medium	Low	Medium	Medium
82	TC.CAC.2	130	**File encryption** mitigates risk due to data at rest and is necessary for effective segmentation of information	High	Medium	Medium	Medium	Medium
83	TC.WAP.2	160	**Web app testing** identifies common vulnerabilities easily and facilitates in-depth testing for malicious inputs	High	Medium	Low	Medium	Medium
84	PT.ACC.7	42	**Visitor badges** increase visitor conformity and preclude default acceptance of a novel person	Medium	Medium	Low	Low	Low
85	PT.ACC.10	42	**Audit of access controls** prevents decay of access security over time	Medium	Medium	Low	Low	Low
86	PT.CLO.5	82	**Cloud appliance encryption** increases the security of data at rest in the cloud	Medium	Medium	Low	Low	Low
87	PT.ROL.1	96	**Minimized shares** reduce the frequency of spillage and unauthenticated sessions	Medium	Medium	Medium	Low	Low
88	PT.SRD.3	108	**Security chiefs** are necessary for implementation of key handling and other high-level security controls	Medium	Medium	Low	Low	Low
89	TC.CAC.4	134	**Virtual networks** mitigate vulnerability to eavesdropping on remote links	Medium	Medium	Medium	Low	Low
90	TC.CAC.5	134	**Encrypted email** reduces the frequency of sensitive information sent in the clear	Medium	Medium	Medium	Low	Low
91	TC.CAC.6	134	**Secure web shares** reduce the frequency of data exposure over email	Medium	Medium	Medium	Low	Low
92	TC.WRL.2	139	**Wi-Fi host configuration** mitigates vulnerability due to host promiscuity	Medium	Medium	Medium	Low	Low
93	TC.SFT.2	143	**Pirated content** training mitigates threats from malicious websites	Medium	Medium	Low	Low	Low
94	TC.INV.1	135	**Network scanning** reduces number of undocumented hosts and processes	Medium	Medium	Low	Low	Low
95	PT.PAS.5	86	**Password cracking** reduces instances of weak passwords and provides a quantitative measure of improvement	Low	Medium	Low	Low	Low
96	TC.IDS.2	162	**Port obscurity** slows initial reconnaissance and reduces the noise that needs to be filtered from logs	Low	Medium	Low	Low	Low
97	PT.ACC.2	42	**Photo identification** is necessary for manual enforcement of access control at larger organizations	Low- High	Medium	Medium	Medium	Low
98	PT.ACC.3	42	**Locking computers** prevents unmediated, opportunistic access to a computer system	Medium	Medium	Medium	Medium	Low
99	PT.ACC.6	42	**Visitor escorts** reduce physical exfiltration and reconnaissance	Medium	High	Medium	Low	High
100	PT.ACC.8	42	**Visitor phone restriction** reduces unapproved release and photo reconnaissance	Medium	Medium	Low	Low	Medium
101	PT.ACC.9	42	**Employee camera restriction** reduces unapproved release	Medium	Medium	Medium	Medium	Medium
102	PT.AUT.1	45	**Two-factor entry** authentication prevents a single point of failure for access credentials	Medium	High	Medium	High	Low
103	PT.AUT.2	45	**Two-factor network authentication** prevents a single point of failure for account credentials	Medium	High	Medium	Medium	Medium
104	PT.PHY.2	48	**Camera surveillance** mitigates adversarial reconnaissance and aids investigation	Medium	Medium	Low	High	Low
105	PT.PHY.3	48	**Physical perimeter** reduces the frequency of physical infiltration	Medium	Medium	Low	High	Low
106	PT.PHY.4	48	**Security perimeter** mitigates physical infiltration and reconnaissance	Medium	High	Low	High	Medium
107	PT.PHY.5	48	**Alarm system** reduces exfiltration during physical intrusion	Medium	Medium	Low	High	Low
108	PT.SEN.1	52	**Social engineering awareness** training reduces the frequency of information theft and physical exfiltration	Medium	Low	Low	Medium	High

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
109	PT.PSH.1	55	**Email conversational awareness** training increases detection of fraudulent messages	Medium	Medium	Low	Medium	Medium
110	PT.PSH.4	55	**Mock phishing campaigns** provide memorable reinforcement experience	Medium	Medium	Medium	Medium	Medium
111	PT.PSH.9	55	**Fraud reporting** facilitates measuring and combating fraud on a large scale	Medium	Medium	Medium	Low	Medium
112	PT.PWS.1	59	**Phishing website awareness** training reduces trust in third-party websites and link clicking behaviors	Medium	Medium	Low	Medium	Medium
113	PT.SME.1	61	**Social media usage policy** mitigates social engineering reconnaissance and account correlation	Medium	Medium	Medium	Low	Medium
114	PT.SME.2	61	**Social media pre-release review** reduces frequency of unintended release and protects brand image	Medium	Medium	Medium	Low	Medium
115	PT.SME.4	61	**Social media safety awareness** training reduces personal vulnerability due to social media presence	Medium	Medium	Medium	Medium	Medium
116	PT.DIN.4	68	**Integrity monitoring** reduces the frequency of malicious data loss	Medium	Medium	Low	Medium	Low
117	PT.DCT.2	71	**Data access control** reduces the frequency of data leakage	Medium	Medium	Medium	High	Low
118	PT.DCT.3	71	**Data encryption policy** reduces the frequency of data theft	Medium	Medium	Low	Medium	Low
119	PT.CAC.2	73	**Secure channels** encourage usage of secure communication	Medium	Medium	Medium	Medium	Low
120	PT.CLO.1	82	**Cloud provider vetting** is necessary before a vendor can be trusted	Medium	Medium	Low	Medium	Low
121	PT.CLO.4	82	**Cloud appliance auditing** mitigates vulnerabilities in cloud instances	Medium	Medium	Low	Medium	Medium
122	PT.CLO.6	82	**Cloud uplink auditing** mitigates threats to communication with the cloud	Medium	Medium	Medium	Medium	Low
123	PT.NET.1	88	**Internet whitelisting** greatly restricts possible attack sources	Medium	High	High	High	Medium
124	PT.NET.2	88	**Extensible whitelist** reduces employee resistance and increases conformance	Medium	Medium	Low	Medium	Low
125	PT.NET.3	90	**Virtualized browsing** sidesteps the difficult task of protecting against host compromise	Medium	High	High	High	Medium
126	PT.DEV.1	91	**Removable media awareness** training reduces probability of compromise by removable media	Medium	Medium	Low	Medium	Medium
127	PT.DEV.2	91	**Removable media tracking** reduces information loss through removable media and insider threats	Medium	Medium	Medium	Medium	Medium
128	PT.DEV.3	91	**Personal device policy** increases conformance of devices and reduces network infection vectors	Medium	Medium	Medium	Medium	Medium
129	PT.DEV.6	91	**Remote work policy** reduces exposure to unsafe networks and vulnerability to remote intrusion from endpoints	Medium	Medium	Medium	Low	Medium
130	PT.DEV.9	94	**Pre-travel purge** reduces exposure of information during travel	Medium	Medium	Medium	Medium	Medium
131	PT.ROL.2	96	**Information labeling and demarcation** increases security of the most sensitive information	Medium	Medium	Medium	High	Medium
132	PT.ROL.4	96	**Specialized roles** mitigate threats due to uncommon and high-risk usage	Medium	Medium	Medium	Medium	Low
133	PT.ROL.5	96	**Role awareness** training reduces nonconformance by unqualified or naïve employees	Medium	Medium	Medium	Medium	Medium
134	PT.ROL.7	100	**Documented roles** reduce access creep and instances of vulnerability due to unqualified employees	Medium	Medium	Medium	Medium	Medium
135	PT.ROL.9	100	**Training controls** increase employee qualifications and reduce damages due to naïve non-conformance	Medium	High	Medium	Medium	Medium
136	PT.CRT.1	103	**Incident awareness training** increases the rate of reporting and reduces nonconformance	Medium	Medium	Low	Medium	Medium
137	PT.CRT.2	103	**Incident team** mitigates damages from information incidents	Medium	Medium	Low	Medium	Low
138	PT.CRT.3	103	**Incident reporting plan** is required in many industries and reduces delay to conform to reporting requirements	Medium-High	Medium	Low	Medium	Low

Rank	Code†	Page	Technique	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
139	PT.RAC.1	105	**Response scripting** reduces reaction time and increases effectiveness of responses to events	Medium	Medium	Medium	High	Medium
140	PT.RAC.2	105	**Identifying dependencies** increases the effectiveness and completeness of responses	Medium	Medium	Medium	Medium	Medium
141	PT.RAC.4	105	**Practiced response** increases efficacy of recovery efforts and decreases recovery time	Medium	Medium	Medium	Medium	Low
142	PT.SRD.2	108	**Security team training** increases competence of the security team	Medium	Medium	Low	Medium	Low
143	PT.AFF.1	110	**Vendor lockdown** extends security assurances transitively to information sent outside	Medium	Medium	Medium	Medium	Low
144	PT.AFF.2	110	**Vendor auditing** reduces retreat of security practices among outside vendors	Medium	Medium	Low	Medium	Low
145	TC.CAC.3	130	**Personal information scanning** reduces the amount of personal data at risk	Medium	Medium	Medium	Low	Medium
146	TC.FIR.2	137	**Blocking direct IP access** restricts command and control to bot controllers and slows expansion of influence	Medium	Medium	Low	Medium	Low
147	TC.SFT.1	143	**Restricting free applications e**liminates a common vector for Trojan horses	Medium	Medium	Medium	Medium	Low
148	TC.INV.2	135	**Automated inventory** aids enforcement of versioning and patching policies	Medium	Medium	Low	Low	Medium
149	TC.INV.3	135	**Documented network architecture** reduces instances of unnecessary network exposure	Medium	Medium	Medium	Medium	Low
150	TC.SIM.1	154	**Security Information and Event Management** (SEIM) provides visibility of network security	Medium	Medium	Low	Medium	Low
151	TC.PEN.2	157	**Penetration testing** identifies configuration- and operations-specific vulnerabilities	Medium	Medium	Low	Low	Medium
152	TC.IDS.1	162	**Log monitoring** is one of the primary methods for intrusion detection, better for detection of compromised hosts	Medium	Medium	Medium	Low	Medium
153	TC.STR.1	165	**Security team training** keeps security staff up to date and ensures competency in core areas	Medium	Medium	Low	Medium	Medium
154	PT.SEN.4	52	**Pre-interview screening** mitigates information loss through sentinels	Low	Medium	High	Medium	Low
155	PT.PSH.2	55	**Email technology awareness** training reduces link-following behaviors	Low	Medium	Medium	Medium	Medium
156	PT.PSH.3	55	**Phishing email examples** increase detection of fraud and reduce link-following behaviors	Low	Low	Low	Low	Medium
157	PT.PWS.2	59	**Web technology awareness** training reduces promiscuous browsing behaviors	Low	Medium	Medium	Medium	Medium
158	PT.DCT.1	71	**Data location tracking** reduces the frequency of lost or forgotten data	Low	Medium	Medium	Medium	Medium
159	PT.REM.4	77	**Web encryption awareness** training reduces the frequency of compromised credentials and leakage of personal information	Low	Medium	Low	Medium	Medium
160	PT.REM.5	80	**Man-in-the-middle awareness** training reduces the frequency of compromised credentials and leakage	Low	Medium	Low	Medium	Medium
161	PT.CLO.3	82	**Cloud attestation** reduces dependence on vendor integrity	Low	High	Low	Medium	Low

† Codes begin with a volume prefix to indicate they are either policy or material issues.

PT – Volume 2: Policies and Training

TC – Volume 3: Tools and Configurations

Security for the Beginner

Many organizations do not practice effective security because they do not know where to start. To 'get' security requires understanding the basics of what the goals are, why one would take a specific action, and how to know when a goal is attained. Do not worry, the decisions become as concrete as hiring a new employee. Ok, maybe worry a little, because the 'best' security plan is as elusive as the 'best' business plan. The objective of this section is to make the goals and tradeoffs as clear for security as they are for other facets of a business.

Those with a background in security management can safely skip this section.

Should I Worry about Security?

Security at many small businesses sits at an impasse. Owners and managers know companies are being attacked. However, proactive action based on conjecture is not the prerogative of a small business that must make money in the here and now. Lacking concrete motivation or a clear goal, leaders too often end up stuck in a loop asking 'could an attack happen to *us*?' or 'realistically, would an attack happen to *us*?'

A Breach is Likely

Regardless of the specifics of your business, yes, a successful attack is likely. Attackers want things like credit card numbers. This applies equally to personal ATM cards and customer payment information. Other times attackers simply want control of a large number of computers, be they laptops or servers.

For just one demonstration, homes, home offices and small businesses use inexpensive, vulnerable modems and wireless routers. Attackers cast a wide net and millions of such networks are be exposed to simple attacks. Tens of thousands of computers scan the internet looking for the signatures of vulnerable modems. The marginal cost of scanning one more internet address is almost nothing. These adversaries do not know or care if you are a home, home office, or medium business. A search engine like Shodan (http://www.shodanhq.com/) provides a searchable directory of millions of internet-connected devices. In addition, Wi-Fi networks at motels, restaurants and small offices in small towns are attacked with surprising frequency—even if typically with little sophistication. If you have Wi-Fi, a public map like the one at Wigle (https://wigle.net) likely shows both your home and office routers.

Security is Risk Management

The questions above are natural, but not useful when making investment decisions. A good investment analyst first understands the risk tolerance of a client. For example, consider retirement. Someone in his or her thirties wants to maximize the yearly return on investment averaged over a few decades. A short-term market rollercoaster ride is acceptable. On the other hand, someone a year from retirement cannot tolerate the risk of an investment that has a high average rate of return but also a significant probability of losing a third of its value over one year.

Some organizations can tolerate date theft. For example, the business model at a small manufacturing company might depend more on high entry cost than original intellectual property. Such an organization can tolerate a roller coaster of data breaches to save security spending. A fish farm that depends on well-researched feeding schedules to maximize yield per dollar of feed and eventually underbid competitors might be intolerant of data theft. This organization must spend more on security to reduce risk.

The goal of security at a business is to minimize the total cost of security spending and damages from losses.

Security is like insurance: our best hope is to lose as little money as possible. In a perfect world, no one would spend any money on security. In the real world, as an organization spends more money on security, the long-term risk of loss due to theft is reduced. In the above examples, the manufacturing company that depends on high entry cost has lower damages from theft and so rationally spends less on security. Conversely, the fish farm has high cost of theft and so rationally spends more on security.

Once an organization understands that managing security is about maximizing the bottom line, normal business rational apply. The cost of security is obvious because one can decide how much to spend. Estimating expected loss is more difficult. A few cases are easy, such as a business that loses several bids to an ex-employee who steals bid documents. In most cases, the cost of losses is subject to conjecture, uncontrollable factors, and all-around uncertainty. Like an insurance company, we must think like actuaries and estimate how much loss we expect. This is difficult because loss events are discrete, can be far between and have widely varying consequence, and might go unnoticed.

Effective security must be maintained over time. As with analyzing other long-term investments, the natural inclination of managers is to overvalue short-term factors and undervalue the probability of future loss. When a security expert seems to be advocating for increasing security, it is usually because the costs of information theft are being underestimated.

One standard solution for converting liability to overhead is insurance. Companies in the financial, retail and other sectors often insure themselves to some extent against damages due to security breaches. The coverage tends to fall partially under the umbrella of more general loss and liability. Coverage specifically for 'information theft and ensuing fallout' is increasingly demanded from insurance carriers.

However, insurance only spreads risk across a wider base; it does nothing to reduce risk. Insurance companies analyze risk and require a reasonable risk level as a prerequisite to underwriting a policy. Underwriters will not indemnify the owner of an information system that is structured for ease of theft any more than they will indemnify the owner of an oil refinery that is built with a coin-operated self-destruct button. Critical infrastructure companies, in the energy industry in particular, have notably struggled to attain insurance against cyber threats because security practices, including patching, for Supervisory Control and Data Acquisition (SCADA) systems and floor-level industrial controls are frequently so poor.

Analyzing the Bottom Line

In the executive summary are listed several business risks associated with information theft: competitive information and lost bids; customer information and canceled contracts; intellectual property and lost residual sales; standards compliance and legal liability.

To give a more concrete example, consider that an employee clicks on an email and activates a virus. The cost to wipe and reinstall a computer is obvious and can possibly be measured directly by the IT department. Estimating the cost of employees filtering phishing messages from their inbox after the address book that was stolen from the infected computer is used to widen the phishing attack is more difficult. If the employee that activated the virus has network access to other computers, shared drives, etc. the scope for loss gets more nebulous.

When talking to small businesses, we first ask at an abstract level 'are you secure enough?' The answer is usually yes, with variable amount of hesitation. Then we ask a series of concrete questions that might follow a sequence similar to that below.

- Do your employees receive phishing emails?
- Are computers sometimes infected?
- Can one employee, or an infected machine, access the entire company network?
- Do you think one of those infected machines attempted to access the rest of the network?
- Do you perform intrusion detection?
- If an infected machine were accessing the network, how long would it take to figure this out?
- How much information could be stolen in that time?
- What would be the cost of this theft? In bids, contracts, residual sales, reputation?
- Given the likely loss due to one compromised machine, scaled by the expected number of machine being compromised, is this risk acceptable?
- Do you have some idea of what it would cost to implement minimal access control and intrusion detection?
- Do you know how this minimal security would affect the probability of compromise, granularity of access, and the effectiveness of detection?
- How would the upgrade affect how much information can reasonably be stolen?
- Given the cost vs. benefit of preventative security, are you secure enough?

After looping back to the initial question, most managers and owners at SMBs change their initial answer. Almost any company finds that minimal security practice is rational risk management. More costly security measures can often be rationally omitted.

The Volumes of *Understanding Security* provide a list of security tips that range from simple tweaking of settings to employee awareness training. These tips usually include an attack-impact-mitigation scenario like the one suggested above, so that cost vs. benefit can be understood in an analogous way.

The bottom line is there are many things that can be done for under $100 cash outlay that substantially increase defense and usually decrease loss. Make no illusion, between planning,

procurement, installation and tuning, transforming a medium-sized business with no security to a reasonably secure workplace will require man-weeks upfront to implement and continued funding to maintain.

Fortunately, the tips in *Understanding Security* are largely independent, and can be implemented piecemeal. Inexpensive tips that address shortcomings that would be exposed during a review, like the one above, should be implemented sooner rather than later.

What is an Attack?

Many people want to ensure their organization is 'secure enough', and are willing to take action if necessary. However, it is difficult to confront an invisible enemy. It is also difficult to compare the merits of different moves when one does not have an intuitive sense for the game. Below an attack is outlined at a high level so that defense can be understood in context.

Attacks follow a repeatable pattern. The exact techniques used at each stage vary over time, but the basic flow of information remains the same since before computers: each stage gathers information for later stages.

Information Gathering

Information gathering is critical for targeted attacks. When a specific target is chosen, almost any attacker will invest in initial information gathering. For an attack that will use social engineering and physical penetration, information gathering is likely the single longest stage of an attack.

Unfortunately, it is difficult or impossible to detect or defend against information gathering. Much of the information gathering stage has moved to a public information search. This is known as 'search engine hacking'. Satellite pictures, legal proceedings, environmental violations, finances, real estate, and the people associated with all of this activity can be discovered through public records. This type of groundwork provides shrink-wrapped pretense and existing conversations that can be used by an impostor to trick employees into giving the adversary access.

Initial Penetration

Initial penetration gains a foothold within an organization. In a targeted attack, someone might come in person. A good social engineer can attain physical access more often than not. This is very difficult to stop because the training required of employees is prohibitively expensive for most organizations. Luckily, social engineers and in-person attacks are relatively rare. High-priority targets with new technology, critical bids, managing critical infrastructure, or supplying military customers should be vigilant.

The dominant tactics used for initial penetration are phishing and web application attacks. Phishing emails are malicious emails that try to trick the victim into clicking a link or opening an attachment. Most phishing emails are low quality, but when the attack becomes more targeted, emails can include known 'senders', personal information, and reference existing conversations.

Web application attacks are the closest method to traditional 'computer hacking'. Attackers take advantage of flaws in the way websites accept and process information to get the server software 'underneath' the web page to do unexpected things. It is still possible to exploit flaws in operating systems and services, but after two decades of security patches and with automatic updates, this has become less common. Embedded systems like scanners, routers, etc. that are not updated are the exception and can often be compromised by direct frontal assault.

Penetration is the hardest part of hacking, because once complete, the rest of the attack proceeds from the inside and under cover of the usual activities of the company.

Expanding Influence

In horror movies, the most insidious threats are those where the monsters replace or otherwise mimic humans. Likewise, the critical point to understand about attacks is that most of the actions during an attack come from 'friendly' computers. In security circles, experts say things like 'perimeter defense is not enough' and 'defend in depth' to address the need to detect threats that operate on the inside.

After penetration and compromise of a single machine, that machine will be used to scan other machines. When a soft target is found, this machine will be attacked, compromised, and used to scan other resources. Each successive machine possibly permits visibility and access to another segment of network.

Another critical observation is that stealth is key to a prolonged, pervasive attack. The idea of local scanning is that each segment of a network is scanned locally, so that little cross-network traffic is generated.

Exfiltration

Exfiltration involves actually transferring information. This stage should be easily detectable because of information flow external to the organization, but by this stage, several machines and network appliances are often compromised.

At many SMBs, really nothing is detected, so a sizable fraction of upload bandwidth can be used to transfer stolen information without repercussion. Terabytes of intellectual property are often stolen when a single intrusion detection appliance could stop have detected and automatically slowed the madness.

Widening the Attack

This stage is really a feedback loop back into penetration. Often, stolen information is used to expand an attack. For example, it is common to compromise one machine using a phishing email, steal the address book from the email client, and then use these contacts to generate better, more convincing emails for use in targeted spear phishing. Using exfiltrated information, personnel in other departments, offices, even different organizations can be targeted for phishing and social engineering.

Residence

It is easier to monitor and re-infect a network than to penetrate all over again. Therefore, adversaries will simple stay inside. After an entire network is owned, and there is nothing left to steal, the stealthy option is to reduce activity to a minimum. Network systems are monitored for change or new information. Once dormant, malware and hackers are very difficult to detect. This is what makes cleaning an owned network very difficult.

Scenarios like the one at Nortel Networks indicate that a network at a tech company can be totally owned by hackers for more than a decade. At an SMB that lacks intrusion detection, hackers can be brazen, scanning aggressively, and are likely never detected or removed from the network after gaining a foothold. New machine and upgrades that are added to the network can be attacked from every direction and are easily defeated.

Security Upgrade Discussion

The planning and execution of a security upgrade requires participation and coordination across administrative divisions. Therefore, a successful security upgrade requires securing the long-term support and participation of several stakeholders. Further, both a continued mandate for organizational transformation and continued financial support depend on 1) visibility of the security program, 2) continuing self-assessment by the security team, and 3) demonstration of the impact and value of the security program.

Security needs and management structure are peculiar to an organization, so a general approach to a security upgrade cannot be formulated. However, this section provides guidance and a beginning-to-end workflow that addresses many common concerns. The focus is on business considerations, and the detailed design of a training program is left to resources such as [7].

Step 1: Identify the Business Objective

As in any business scenario, the costs for a security upgrade must be justified by some payoff. Therefore, it is essential to first identify the high-level goal of a security upgrade. Common short-term objectives are:

- Pass an audit or address findings of a completed audit
- Meet a specific contractual obligation
- Mitigate ongoing information loss

These short-term goals are often approached with the expectation that they can be accomplished with a one-time budget charge. Other times management determines to create only the appearance of compliance. Nevertheless, hidden just below the surface are ongoing costs.

- Whatever factors eventually required one security audit will likely lead to a future security audit, and the next audit will likely find the same flaws if real improvement has not occurred.
- If a company operates in a market in which one contract required specific security guarantees, then it is likely that multiple future contracts will include similar stipulations. Across virtually every business sector, information security is becoming mandatory.
- Some organizations that are already engaged in ongoing efforts to 'plug leaks' in the information system maintain a mentality that individual incidents are isolated and treat the issue as a procession of one-time 'patches'. This approach is often accompanied by willful ignorance of the cost of ineffective mitigation techniques and the true damages from information losses.

Long-term, pervasive security plans are usually driven by either a core business plan that necessitates success in a market that demands secure handling of information or by loss events that threaten the viability of some business unit. Change is motivated by first identifying structural need for effective information security. Common examples are given below.

- Contract requirements for non-disclosure are standard within the defense supply chain.
- Regulatory compliance places requirements on the handling of many types of private information.
- Long-term viability in almost any industry requires non-disclosure. If manufacturing drawings, customer information, bid documents, etc. are leaked by a vendor, the customer will tend to look elsewhere.

Another point of contention when allocating security resources is compliance versus real security. Unfortunately, most government and industry standards pertain to handling and reporting controls that do not actually improve security. Reporting requirements notably arise out of consideration for the greater good of transparency and accountability in personal data handling and do not directly improve security but do increase visibility of failure and therefore rational level of security investment.

A more nuanced case is opportunity costs and poor returns from security investment. A chief example is slavish adherence to paper-based standards. For just one example, many healthcare organizations that are subject to FERPA spend the majority of their security budget on paper-based controls—even when the majority of the sensitive information they hold has already transitioned to electronic form.

When allocating resources, day-to-day operations and regulatory pressures often favor compliance over security. Compliance is also easier to assess and the target more straightforward than when defending against an evolving threat landscape. Unfortunately, if a breech occurs, and during the aftermath, compliance is overshadowed by accusations of lacking security practice. Compliance is little mitigation for the damage to organizational reputation.

Ultimately, compliance is usually a 'must have'. In this sense, compliance must trump real security in budgetary matters. However, when allocating total security budget, it should be remembered that compliance alone is not adequate, and should not equate to complacency.

With budget scarcity and tensions between compliance, contractual obligations, audits and proactive security in mind, the top-level business goal should be summarized in a sentence or two. This goal should act as the ground truth when discussing must-haves, cannot-haves, and benefits of particular security strategies.

Step 2: Identify the Stakeholders

With a business goal in hand, funding and support must be procured. Stakeholders must also be 'in the loop' or else they will become adversaries instead of champions of the project. This is all standard for any project, so only a few security-specific factors are discussed below.

- Security is a relatively new overhead at most organizations. The managerial class has almost universally internalized the positive cost-benefit of other overheads: accounting, resource planning and many actuarial activities. However, the business value of security remains foreign to many managers, and the concept of security as risk management must be established. Business value must often be established within several budgetary units before interest and participation are won.
- Security upgrades often require formalization of IT roles and external oversight in personnel decisions. Together with differences of opinions on technical aspects, all of this can lead to friction with IT administrators. Existing IT domains should be included in the discussion of any redistribution of authority and changes to infrastructure.
- New security procedures impose immediate time costs on third-party departments. Often, changes are pushed out without warning, communication of business need, or consideration for budgetary compensation. In addition, the core decision makers for a security upgrade inevitably fail to communicate adequately the thought process that leads to these changes, and immediate resentment and friction result.

  Every affected business unit should have a representative who is fully informed of the process and who can serve as a contact and communication channel into decision-making discussions. This representative will also inevitably communicate the process to their department more effectively than will the core decision makers.

Step 3: Assess Operational Feasibility

Enacting real improvement to information security requires a coordinated effort and examined allocation of resources. Security is about risk management. After realistically assessing the true costs of information losses, most basic security measures will be justified. More intensive security measures tend to be nontrivial to implement and maintain, and the true cost of information losses is often found to be acceptable in the balance.

This series of documents provides guidance that can be used for implementing a discrete project to harden an information system. However, it should be understood that an effective upgrade to information security is an ongoing effort that requires monitoring, response, and upkeep. Any such project will entail two components.

- Immediate outlay for upgrades to both infrastructure (fences, doors, servers, firewalls) and culture (training time).

- Maintenance in the form of both labor for regular training of employees, front desk staff or security guards, and facilities costs for maintenance of lawns, fences, network infrastructure, subscription services, etc.

Key questions must be answered to establish the operational feasibility of a security upgrade:

- What is actually possible? For example, in an urban setting or leased office space, a security perimeter might not be possible. However, care should be taken not to dismiss non-obvious cases before open discussion.
- What is feasible? For example, at a company expecting losses during this fiscal year, a facility upgrade or other large new budget item might be out of the question. Feasibility should be assessed only after true costs and business objective have been identified. For example, lost contract opportunities due to inability to meet security stipulations could be the cause of the current poor financial performance.
- What can we actually implement? Especially for a company that does not have a history of information security, in-house expertise can be lacking. The capabilities of the organization, or lack thereof, will feed back into costs for outside vendors, consultants, and one-time prototypes. Similarly, controlling physical entry is a straightforward concept, but implementing this within the current layout at a heretofore wide-open facility might not be possible. This scenario can feed back into large costs to reconfigure easements, parking lots and loading areas, for example. Implementation costs that are uncovered in turn feed back into feasibility.

Step 4: Security Inventory

Finally, the real security work can begin. First, an organization must take stock of what is to be protected.

A list should be created of any information that should not be disclosed to the public. This list usually grows beyond initial expectation.

- Databases
- Credit card numbers
- Personal information
- Manufacturing drawings
- Bid documents

The locations of all data, both hard copy and electronic should be cataloged.

- Backup tapes
- File cabinets
- Servers
- Workstations
- Mobile devices

In addition, network infrastructure that is used to access and protect this information should be cataloged.

- Routers and switches
- Workstations
- All installed software

Physical access is prerequisite to any other security. Luckily, the details of facilities change more slowly than details of information systems. Nevertheless, written records of access points and other physical details tend to fall behind changes.

- Loading points
- Inventory areas
- Inspection areas
- Fences
- Cameras
- Dumpsters
- External doors
- Internal controlled doors
- Fire alarms and fire suppression systems
- Air conditioners for IT equipment

Existing written policies, if any, should be collected. Informal policies should be condensed into forms that can be examined.

- Front desk and waiting areas
- Vendor access
- Computer access
- Key duplication and other credential management

Many companies are aware of the worst security vulnerabilities, but these have been inconvenient to mitigate. Knowledge of vulnerabilities might also be compartmentalized and known only to proximate groups. A security upgrade is the best time to put known issues on the table and allow them to enter the conversation on how to allocate resources.

- Procedural failures: unlocked computers, unrecorded information sharing, etc.
- Weaknesses of facilities: broken fences, inoperable door sensors, etc.
- Known information losses

Once this process begins, the escalating number of classes of asset to be recorded can be daunting. To assist, Volume 1: Current Asset Inventory provides a starting checklist of assets that should be recorded.

Step 5: Security Review

With assets and known issues in hand, the best practices in security should be reviewed. Volume 2: Policies and Training and Volume 3: Tools and Configurations introduce attacks and defenses for information systems. These volumes should be skimmed to identify relevant issues, and then the relevant issues reviewed in committee.

Once concerns have been identified, mitigation techniques must be selected. Feedback should be invited from stakeholders on what is required to implement these changes.

Step 6: Rollout Training and Upgrades

The last steps require a security upgrade to come into relations with the operations of the organization. Training and hardware must be brought online.

Training

Identify affected groups.

- Administrators
- Managers
- Office staff
- Floor workers

Each group should receive a custom training packet.

- Training plan
- Evaluation/enforcement expectations

To ensure the core security procedures are understood and retained, tri-fold cards or 'cheat sheets' make a good reminder. These can be precisely targeted at each role in the organization. Designing a training program is outside the scope of this document. An excellent guide is provided in [7].

Upgrades

Infrastructure upgrades can be integrated into the normal maintenance pipeline of the IT department. One caveat is to give upgrades sufficient priority so that momentum is not lost in completing the infrastructure upgrades under the umbrella timeframe of the security upgrade. Of course, at medium-sized organizations where a separate budget must be allocated, the upgrade must be a distinct task.

Ongoing: Monitoring, Enforcement and Self-Assessment

Monitoring

To demonstrate return on investment, a security project must be able to observe and report improvement. This will require measurement of security behaviors. Most organizations do not retain detailed evidence of internal network intrusions or phishing emails. Therefore, follow-up monitoring requires some pre-upgrade preparation. Simple comparative surveys of awareness, violations, or ease of compromise can establish concrete improvement in critical areas. Some ideas:

- A controlled mock-phishing campaign can provide good, cross-organizational numbers for the ease of compromising employee computers.
- Tests at building entry points for unlocked doors and the rate of tailgating success can verify if basic access controls have improved.
- Cracking password databases can indicate if passwords have improved. This can be done by saving a copy of the password database both before training and after training has completed and passwords for all accounts have expired. Running the same cracker on both databases will give a strong indication of the comparative quality of passwords in the two databases.

Enforcement

Security is only effective once a culture of security is the norm. Especially for an organization that is beginning with very little security, it is expected that many new policies will not be readily adopted, consistently implemented or followed at all. Procedures that preempt extant workflow or add time or cost to processes will be the most maligned and ignored.

Enforcement is perhaps the most critical component of the post-implementation phase. Failure to enforce security policy will result in perceived lack of efficacy of the training program, and likely reduction in funding. Likewise, heavy-handed enforcement will degrade morale, and often will erode support.

Incentives are therefore required to motivate new behaviors. Positive reinforcement can take the form of whatever reward seems appropriate for the departments that demonstrate adoption of new policies. The criteria for reinforcement can be a low rate of clicking on a link in a mock phishing email, or improvement in this measure, or an analogous measured improvement for any security behavior.

Self-Assessment

Value must also be demonstrated for the training program itself. This requires evaluation of the efficacy of the training program, compared to other approaches. Direct comparison of multiple experimental programs is likely impossible, so the key is introspection. Again, the best-known treatment of training programs is [7].

Applied Research Laboratory

The Pennsylvania State University

Understanding Security

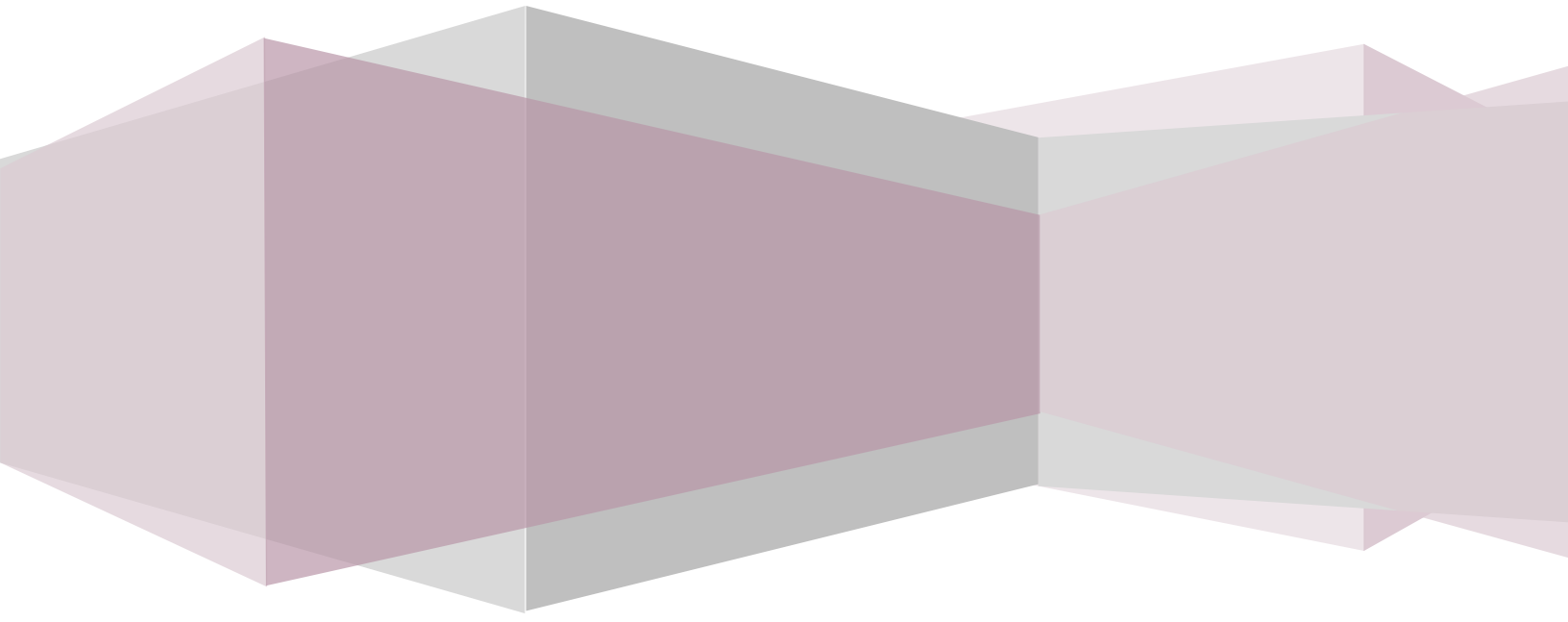
Volume 1

ASSET INVENTORY CHECKLIST

Brice A. Toth

Caleb J. Severn

Jonathan Hoerr



Introduction

The purpose of this volume is to help SMBs self-assess what assets they possess—what is at risk. One point about targeting behavior is that it arises from not just direct possession of some asset that is valuable to an adversary but also association or proximity to organizations that are valuable targets and occasionally purely due to high visibility. In some cases, a company is targeted simply for supplying commodities or services to other companies that supply a critical industry or following the release of a whitepaper or booth a conference. Accordingly, some questions below ask about associations and public releases. While not strictly 'inventory', enumerating important contacts and associations can spur appreciation of why even a small company can be a high-priority target.

Several asset types are included: intellectual property, computer systems, services and applications, network devices, and uniquely experienced employees. Each type of asset can be valuable for day-to-day operations or long-term strategy. An asset thereby entails some impact if it is compromised. Compromise can include disclosure of confidential information, unintended modification of information, or unavailability of an asset when it is needed. In addition to enumerations of common assets in tables below, a few questions can help to gauge more accurately the impact of compromise.

- How do employees in your organization perform their jobs?
- What data does your organization need to function daily?
- Where is organizational data stored and in what form?
- What applications depend on access to organizational data?
- What channels must remain open to allow these applications to connect to stored data?

Only when assets are enumerated and impact of compromise is acknowledged can an argument for return on investment for security spending be made. When progressing through this document, templates for inventory tables are provided, similar to the one below.

Brand	Model	Location	IP Address	MAC Address	Hostname
Dell	Inspiron 15	Lobby	192.168.1.115	00:B0:D0:BB:F7	lobby_563

The fields in each table are commonly needed during an asset inventory, but the necessary information can vary by company. Typically, the columns are organized from more general and universal information on the left to more specific and perhaps more specialized information on the right. For each table, an example will be shown in the first row of the table.

Human Assets

Employees that have unique skills, knowledge, or experience are assets to the company. Each Employee performs some roles within an organization, and minimally must have access to the information they need to perform their job. An accurate accounting of roles and responsibilities can expose holes in training and skill sets. Actual duties can also be used to establish need-to-know when assigning role-based permissions to each employee. Establishing need-to-know and compartmentalizing data is the key to reducing exposure to damage due to naïve, confused or actively mischievous employees.

Name	Location	Category	Type	Skills/Knowledge
John Smith	Back Office	IT Administrator	Contractor	Knows DB Systems, Internal Network, System Admin

Common and useful categories for employees are given below. Many SMBs outsource IT, accounting and other overhead services. The employee in this case can be the name of the company. Employees frequently wear multiple hats at SMBs, and these can be listed separately to mirror the multiple role permission the employee needs to have.

Employee Category
Management
IT Administrator
IT Security
Physical Security
Incident Response
Office (by department)
Floor/Non-office

Outsourcing Assets

While not assets in the traditional sense, outsourcing is increasingly important to SMBs. Service vendors not only fulfill the functions of employees, but also have similar access to facilities, networks and information. It is important to know who has access to what so that questions can be asked about how secure or trustworthy vendors need to be. In many cases, SMBs do not know what the security practices of their vendors are, or even what information is made available. Nevertheless, vendors frequently have physical and network access that is surprising and unexamined.

Category	Service	Vendor	Percentage of Operations
Network Infrastructure	Web Hosting	Alice's Hosting	100

Commonly outsourced services and categories are given below.

Category	Services
Network Infrastructure	Web Hosting, Cloud Storage, Webmail
IT Administration	Help Desk, Database, Intrusion Monitoring
Physical Security	Guards
Accounting	Payroll, Account Balance
Human Resources	Retirement, Benefits
Facilities, Internal	Maintenance, HVAC
Facilities, External	Landscaping, Snow Removal

Information Assets

Information assets are all documents, paper or electronic, that include data, intellectual property or any information that is sensitive or has value. Impact of compromise is a measure of the damage to the business if an asset is compromised. A common scale for impact that can be assigned easily yet proves useful is 1 (minimal, small monetary loss) to 5 (extreme, existential threat to business).

Asset Type	Location	Impact
Company Logo	N/A	1

Some information is required for daily operations; other information is key to competitive advantage. Many types of information are listed below. These categories typically follow ISO 27001.

ISO Category	Asset type
Organization	
6.1	Customer Credit Cards
6.2	Customer Medical Records
6.3	Supplier Finance Data
6.4	Supplier Contact Data
6.5	Supplier Credit Reports
6.6	Press Releases
6.7	White Papers
6.8	Partner Contact Data
6.9	Risk Assessments - Assets
Asset Management	
7.1	Asset Register
Human Resources	
8.1	Social Security Details
8.2	Employees Driving License Details
8.3	Employee Business Contacts
8.4	Employee Personal Contacts
8.5	Employee Ethnographic Details
8.6	Partner Contract Data
8.7	Partner Finance Data
8.9	Partner Credit Reports
8.10	Partner Purchase Order Data
8.11	Key Workers
8.12	Data Protection Register
---	Payroll Data
---	Retirement and Beneficiary Data
---	Employee Assessment Data
Communications and Operations	
10.1, 10.9	Tapes/Discs/DVDs/Portable Drives/PC Cards/USB Storage
10.3	Data Centers
10.10	Network Design
10.11	Intranet Data
10.12	Supplier Contact Data
10.13	Supplier Collaboration Details
10.14	Supplier Cryptographic Keys
10.15	Supplier Purchase Order Data

ISO Category	Asset type
10.17	Customer Credit Card Data
10.18	Customer Marketing Data
10.19	Customer Contact Data
10.20	Service Delivery Agreements
10.21	Capacity Planning Data
10.22	Contractor Transport Data
Access Control	
11.1	Employee Biometrics
11.2	Email (Stored or on Server)
11.3	Instant Messages
11.13	Employee Passwords
11.14	User Register
11.15	Access Rights Register
11.16	Remote User Register
Acquisition, Development & Maintenance	
12.1	Sales & Marketing Data
12.2	File Sharing
12.3	File Storage
12.4	System & Operations Logs
12.5	Source Code
12.6	Employee Private Cryptographic Keys
12.7	Computer Cryptographic Keys
12.8	Purchase Order Data
12.9	Partner Cryptographic Keys
12.10	Public Cryptographic Keys
12.11	Software Register
---	Basic Research Records
---	Engineering Data
---	Recipes/Process Data
---	Manufacturing Data
---	Quality Data
Incident Management	
13.1	Human Resource Data
13.2	Incident Register
Business Continuity	
14.1	Strategic Plans
14.2	Business Continuity Plans
14.3	Risk Assessment
Compliance	
28	Intellectual Property
62	Product Documentation
63	Training Materials
22	Financial Data
98	Compliance Register

Computing Assets

Computing assets, either software or hardware, are systems that process and store information needed by a business. This can include client workstations, servers, databases, and, more recently, mobile devices. These endpoint systems are a large portion of business IT assets and are the most likely to be used on a daily basis.

In the sections below, each system is defined and a table template is shown to demonstrate important information about each system. The important questions for this section are:

- How do employees in your organization perform their jobs?
- What data does your organization need to function daily?
- Where is organizational data stored and in what form?
- What applications depend on access to organizational data?

Workstations

Client workstations include any workstation or laptop used by an employee. These can be owned by the company or employee, but if a machine stores company data, it becomes an asset to the company. Workstations fall under ISO 27001 category 10.5.

Brand	Model	Location	IP Address	MAC Address	Hostname
Dell	Inspiron 15	Lobby	192.168.1.115	00:B0:D0:BB:F7	lobby_536

Servers

Company servers can be physical servers or virtual servers hosted on a physical machine. These systems host and store important information the availability of which affects operations. Many times, they are also the host to applications used by employees and clients, but these applications themselves are captured in the next section. Servers fall under ISO 27001 category 10.4.

Brand	Type	Model	Location	IP Address	MAC Address	Hostname
Dell	PowerEdge	2650	Server Room	192.168.1.1	00:B0:D0:BB:F7	db-server

Database Systems

A database system refers to the actual database that stores company information, not the database applications that manipulate this data. Database systems can store any company records, client information, or company data used by employees and clients alike.

Database	Type	Location	Tables	Users
Client Info	MySQL	On Dell Server (db-server)	Client, Address	Admin, John, Rick

Embedded Devices

Many devices in an office are not thought of as computers but are in fact general-purpose machines that are packaged to serve a dedicated function. In particular, these devices can store lots of information for temporary usage and a surprising amount of information is recoverable by an adversary that gains possession or control of the device. Hackers can use these devices to attack a network just like a workstation. Unfortunately, embedded systems are infrequently patched and frequently neglected.

Category	Brand	Model	Location	IP Address	MAC Address
Printer	HP	LaserJet 405	2nd Floor	192.168.1.23	00:B0:D0:BB:F7

To aid in identifying all embedded systems, several are listed below.

ISO 27001 Category	Device Category
---	Printer
---	Scanner
10.7	Fax machine
---	VoIP Telephone

Mobile and Removable Devices

Increasingly, employees use personal devices in the workplace. Because these devices access company data, they become an asset to the company just like personal computers. Mobile devices include cell phones, tablet devices, advanced personal music players, or any other handheld device that accesses or stores company data.

Category	Brand	Model	Owner	IP Address	MAC Address
Cell Phone	Apple	iPhone 4S	John Smith	192.168.1.210	00:B0:D0:BB:F7

There are many types of mobile and removable device, and several are listed below.

ISO 27001 Category	Device Category
10.2	Smart Card
---	Tablet
---	Smart Phone
---	External (USB) Drive

Service and Application Assets

Service and application assets include any application that is used to process, store, or transmit information. These differ from computing assets above in that services and applications run on computing systems. The designation is blurry, and some computing systems are dedicated to a single service and may be sold as a dedicated appliance. In other cases, a single application can be running on a multitude of computing systems, or a single computer can run many services.

In the sections below, different types of services and systems are listed. The important questions for this section are:

- How do employees in your organization perform their jobs?
- What applications depend on access to organizational data?

Operating Systems

Operating systems provide the foundation on which applications run. These include all operating systems running on employee devices and company servers.

Brand	Version	Systems Installed On
MS Windows	Windows 7	db-server, lobby_536

Database Applications

Database applications include any application, used by clients or employees, which connect to a company database with the specific purpose of accessing or modifying company data. This can range from online web applications to database input applications.

Application	Host System	Location	Accessible Information
Excel	lobby_536	Main Lobby	Client information, addresses

Support Services

Support services include applications that employees log into and software that is not typically used by people directly, but can account for most of the traffic on a network.

Service	Programming Language	Host System	Location
DNS	N/A	blade_4s	Main Computer Room

There are many support services running in a typical medium office space. Below is a starter list. Custom applications are any applications written in-house that the company needs to operate.

ISO 27001 Category	Service
11.2	MS Exchange Server
11.5	Active Directory
11.6	DNS Server
11.7	DHC Server
11.9	Dialup Remote Access
11.11	VPN
---	System Daemons (Custom)

Web and User Services

Web and user services include applications that employees log into and with which employees interact. The need for user input creates possibility for malicious input and web applications have become one of the prime sources of hacking vulnerabilities.

Service	Programming Language	Host System	Location
Intranet Website	Perl, PHP	web2s	Main Computer Room

Many companies run proprietary applications, but the list below provides a starting set of user services.

ISO 27001 Category	Device Category
10.16	Web Site Sales Application
11.4	MS Outlook Web Access
11.8	Enterprise Management Tools
11.12	Telework Work Stations
11.11	VPN
---	Web Applications (Custom)

Office Applications

Office applications include any application bought from an outside source that company employees use to complete daily functions. Common examples include office suites, email clients, web browsers, browser plugins (Flash, Silverlight), PDF readers and the many applications used for accounting, engineering, designing, logistics and resource planning, etc.

Brand	Version	Host System	Purpose
MS Office	2010	lobby_536	Create reports, retrieve db information

Network Infrastructure Assets

Network infrastructure devices, mostly switches and routers, provide the gateways to the internal company network and define its internal topology. Each network device might be identified with a name, address, tag number, or some other designation. Whatever information is used to identify a device uniquely should be included. Important questions to keep in mind for this section are:

- Where is organizational data stored and in what form?
- What channels must remain open to allow applications to connect to stored data?

These devices rarely appear on the list of what a company does or how it functions, but the invisibly of these devices depends on their continued dependable operation.

Routers/Switches

A typical entry in a network asset inventory is given below.

Category	Brand	Model	Location	IP Address	MAC Address
Wired Router	Cisco	AIR-CT2504-15-K9	Server Room	192.168.1.5	00:B0:D0:BB:F7

Although there are relatively few types of network infrastructure and these typically number fewer than endpoint systems, infrastructure is often tucked away, forgotten and unpatched. Inventory is a good time to identify and date all of these devices. A list of common network infrastructure devices is given below.

ISO 27001 Category	Device Category
10.6	Network Switch
---	Wired Router
---	Wireless Access Point
---	Wireless Router
10.8	Private Branch Exchange (PBX)
---	Firewall
---	Proxy Server/Port Forwarding
---	IDS/IDPS Appliance

Network Map

On this map, include information such as the following: external internet connection points, internal router/switch connectivity, workstation connectivity, and server connectivity. A discussion of network maps is given in the ‘Secure Networks’ section on page 148.

Applied Research Laboratory

The Pennsylvania State University

Understanding Security

Volume 2

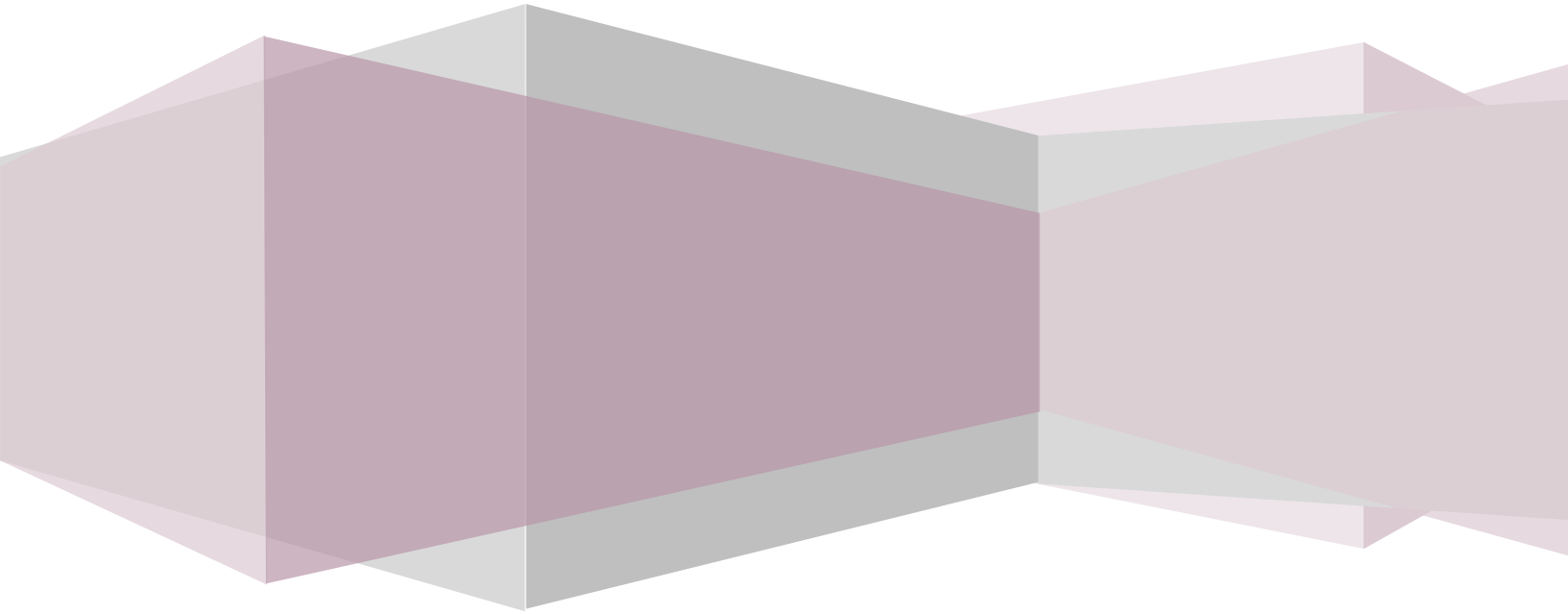
TRAINING AND POLICY TEMPLATES

For a Secure Workplace

Brice A. Toth

Caleb J. Severn

Jonathan Hoerr



Small-Tier Security Tips

Small-Tier security tips are the easiest to implement and apply at nearly all organizations. In addition to minimal implementation and training costs, the vulnerabilities addressed are frequently some of the first that are exploited when organizational assets are breached. Therefore, these tips can be thought of as the 'first line of defense' against a potential attack.

Employee Buy-In

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.BUY.1	Awareness Training	Motivates investment and self-monitoring; reduces costs of enforcement	All	High	High	Low	Medium	Medium
PT.BUY.2	Procedural Training	Increases conformance, reduces frequency of incidents; reduces damages from information loss	All	High	Medium	Medium	Medium	High

Motivation

Training is the most critical aspect of security because employees naturally resist policies they perceive as hindering their productivity. Employees who do not buy into the company security plan will fail to follow security protocol or attempt to circumvent protections. Even well-meaning but naïve employees will tend to circumvent security policy, possibly to the benefit of malicious adversaries. [7]

Prevention

Awareness and Personal Investment in Information Security

Sufficient training begins by explaining the reality of abundant threats, what is at risk, and the direct consequences of not adhering to security policy. Some points to cover in a security orientation:

- Competitive edge. Does the company store bid, procurement or other information that affect competitive proposals? These data are frequently targeted for espionage.
- Contract requirements. Does the company have contractual stipulations for containment of information? Leaking of client data can affect future sales and contracts, especially defense contracts.
- Customer satisfaction. Does the company store customer information? Leaking customer information is minimally a black spot on a company's reputation and can have high costs for customers and incur customer backlash.
- Privacy and liability. Does the company store personal information? Many industries and jurisdictions have standards and liability laws governing the prudent handling of personal information.

- Residual sales. Does the company store engineering information? Designs, drawings and manufacturing knowledge are in high demand, especially in developing industrial centers with weak intellectual property protections.

Clear Procedural Guidance

The task of creating procedures that do not compromise information, protect an organization against attacks, and do all of this across many employees and facilities is certainly not trivial. Even well intentioned employees and departments will fail to address the bigger picture if they are forced to create ad hoc security procedures. Employees also should not have to spend effort to discover best practice. If more effort is required to find the proper procedure than to create a reasonable-seeming plan of their own, the number of conformant employees will plummet.

All of this points to clear, plain, concise procedures for handling of information. Because the entire catalogue of security procedures for an organization will not fit this description, targeted information should be available for every role. A small card of procedures for common office tasks will suffice at each desk. A poster of procedures for tracking controlled documents will suffice at a copy machine, etc. Roles are discussed further in the 'Security Roles and Documentation' section on page 108.

Secure Passwords

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.PAS.1	Password Training	Increases conformance, reduces frequency of intrusion; reduces costs of monitoring and enforcement	All	High	Medium	Low	Medium	Low
PT.PAS.2	Composition Rules	Increases hardness of the entire information system; reduces damages from exfiltration of hashes	All	High	High	Medium	Low	Low
PT.PAS.3	Password Expiration	Mitigates costs of account compromise; reduces damages from account compromise	All	High	Medium	Medium	Low	Medium
PT.PAS.4	Account Lockout	Eliminates trivial password cracking attacks from frontend interfaces; reduce damages from compromised accounts	Admin	High	Medium	Medium	Low	Low

Motivation

Passwords are the overwhelming factor used for authenticating users, and by extension access to computer systems. Strong passwords are therefore critical to the security of an entire computer system.

Prevention

Training

Paramount to improving the quality of passwords is to motivate users. Employees should be educated about the consequent information losses and the true costs of the losses that result from a compromised password—and how their own strong password helps. As discussed in the 'Labeling and Confining Information' section on page 96, at most SMBs the computer system is configured so that every account has access to most of the system. Therefore, every password is a 'key to the kingdom'.

When employees realize the level of trust and authority they possess by virtue of their position, they are more likely to guard this privilege jealously. Once users understand why their passwords have a policy, they are more likely to comply and will be more amenable to a few more characters in their passwords.

Composition Rules

Users need to understand how to create passwords that are hard to crack. Password strength is measured in bits of entropy. Effective password composition rules are paramount in this. Unfortunately, the standard password composition rules have been passed down from the bad old days when passwords were constrained by hardware and algorithmic details. For example, in UNIX, only the first 8 characters of a password were even hashed; the rest were ignored. This choice was made because the DES encryption algorithm only handles 56 bits in one block. Today, computers can handle long passwords, so such computer-centric thinking is anachronistic.

Computers and people handle passwords in very different ways. The ideal password from a computer's perspective lacks any structure—holding the length of a string constant, random bits

provide maximum entropy. Given an extended alphabet of around 80 printable characters, 7 random characters provide around 44 bits of entropy. People consider such a memorization task to be hard and more characters will lead to many forgotten passwords, reused passwords and written passwords—unless the organization has a strict, engrained security culture. Maximizing entropy of a short string is done by ensuring the full alphabet of characters is used. This is the origin of recipe rules like 'complex 8': *At least 8 characters, including all of upper case, lower case, digit and special character*.

The fact that a password must be held in human memory creates specialized constraints and optimizations. Humans do not remember verbatim copies of strings; humans remember by creating associations between structures. The constraint on human cognition is that a person can remember only 5-9 unrelated structures. Holding number of structures constant, the largest vocabulary maximizes entropy—binary is the worst possible choice, followed by individual characters.

Ultimately, humans are poor at remembering character strings because humans are hardwired to form words. Natural language is oral, and, in oral language, individual sounds blend into words that symbolize specific concepts. Symbols readily yield relationships. Written text is a learned extension to natural human language. Even when reading an alphabetic language, humans do not perceive individual characters but words.

Because password complexity is constrained only by the human capacity to remember 5-9 unrelated structures, this constraint needs to be optimized. Because human memory is based on associations, a word is actually easier for a human to remember than a special character. A word is far more difficult for a computer to guess than a character. This is why 2000-word vocabularies beat 80-character alphabets as a constructive basis for passwords. The contrast is quite stark. Humans struggle to remember 10 characters but can more easily remember 10 words, equivalent to more than 100 bits of entropy.

Human cognition is manifest in the fact that the passwords people create are not random strings, but exhibit substructure. Complex character sets and 'recipe' rules give rise to predictable patterns as people struggle to create memorable structure within their passwords. Perhaps half of passwords created according to 'complex 8' will begin with a capital, continue with a word in all lower case and end with the number and character, in either order. This predictable structure reduces the randomness of 'complex 8' to around 36 bits of entropy – 8 bits less than 'random 7'. Longer 'complex' passwords will often include two dictionary words split in the middle by one or both of the digit or special character.

Passwords are broken using password crackers. A password cracker uses 'brute force' only in that many attempts are made. This term is misleading: the state-of-the-art in password cracking is a sophisticated generator that finesses predictable structures within passwords. The worst effect of complex recipe rules is that they contraindicate long passwords. Complex recipes also make structures more predictable and thereby decrease the entropy of password databases and make passwords easier to crack.

Consider a modern approach, 'simple 16'. This recipe simply requires a password of at least 16 characters. Almost everyone will choose dictionary words. Given a vocabulary of around 2000 short and common English words (20,000 words is a typical vocabulary for a college graduate), and assuming 4 simple dictionary words are chosen, this gives around 44 bits of entropy – equal

to ‘random 7’ and significantly better than ‘complex 8’. Users also consider 4 short words to be a much easier memorization task than 7 random characters. Twenty characters, 5 common words, provide more entropy than can be attained through random characters without forcing users to cheat to remember. [8]

Some simple rules can augment ‘simple 16’ to prevent grossly bad passwords: prohibit name, user name, or previous passwords. Grammatically correct phrases are also easier to guess, for example, “MyPasswordIsBad”. Additional password precautions are given in ‘Advanced Password Handling’ on page 86.

Comparing for exact matches to older passwords can be done easily by retaining hashes of old passwords. Comparing for similarity is more difficult. Typically, the only plaintext password that is known is the single previous password that must be entered when changing password, because retaining plaintext passwords would leave the entire system vulnerable. Attempting to generate variations on a new password and then comparing hashes of those variations to hashes of previous passwords tends to be expensive and to produce poor coverage.

As for comparison of plaintext passwords, some guidance recommends comparing the number of changed characters. The algorithm for comparison is typically unspecified but the metric suggests something like longest substring matching. However, any single criterion will have pathological cases; for example, longest substring matching will fail to identify palindromes (mypass to ssapym). In practice, standard libraries are used, as with pam_cracklib for Linux. These libraries perform several checks, for example number of changed characters, rotations, and monotonic sequences (123456).

Expiration

To limit the damage from a single compromised password, all passwords should expire. This can be configured as deemed appropriate, but for general office accounts, a password lifetime of six months to a year is a good balance between security and irritating employees with frequent password changes. For an administrator of a critical network, or a similarly privileged account, the password should expire quarterly.

Password expiration is applicable only to domain passwords; BYOD passwords are up to individual discretion. Issues surrounding BYOD are discussed in the ‘Removable Media and Personal Devices’ section on page 91.

Lockout

One basic principle of authentication is to limit the number of attempts that can be made by an adversary. If an adversary can make an unlimited number of rapid attempts, then passwords can be attacked by brute force without needing to compromise a computer. A wait of several seconds between login attempts is acceptable to humans, and will prevent a program from attempting to login thousands of times per second. After several failed attempts, an account can be locked out. Lockout can entail a longer wait of tens of minutes, or can require an administrator to reset the account manually. One caveat is that availability must be considered when choosing a lockout scheme. For local access, a lockout with manual reset is the most secure. For an internet facing application, webmail for example, lockout creates a trivial denial of service vulnerability: simply attempt to login with many user names and a large number of

employees will be unable to access the network. If significant labor is required to reset an account, as with manual reset, an enterprise can be shut down by an account lockout attack.

When an account is locked out, or for new accounts, a temporary password can be assigned by an administrator, if the authentication system requires that the password be changed the first time the employee logs in.

Other problems

Passwords tend to suffer from choice of a weak phrase. However, any single factor suffers from the threat of exposure. Especially reusable credentials like passwords are vulnerable to replay, phishing and other attacks. Better approaches are discussed in the 'Two Factor Authentication' section on page 45.

Example Passwords

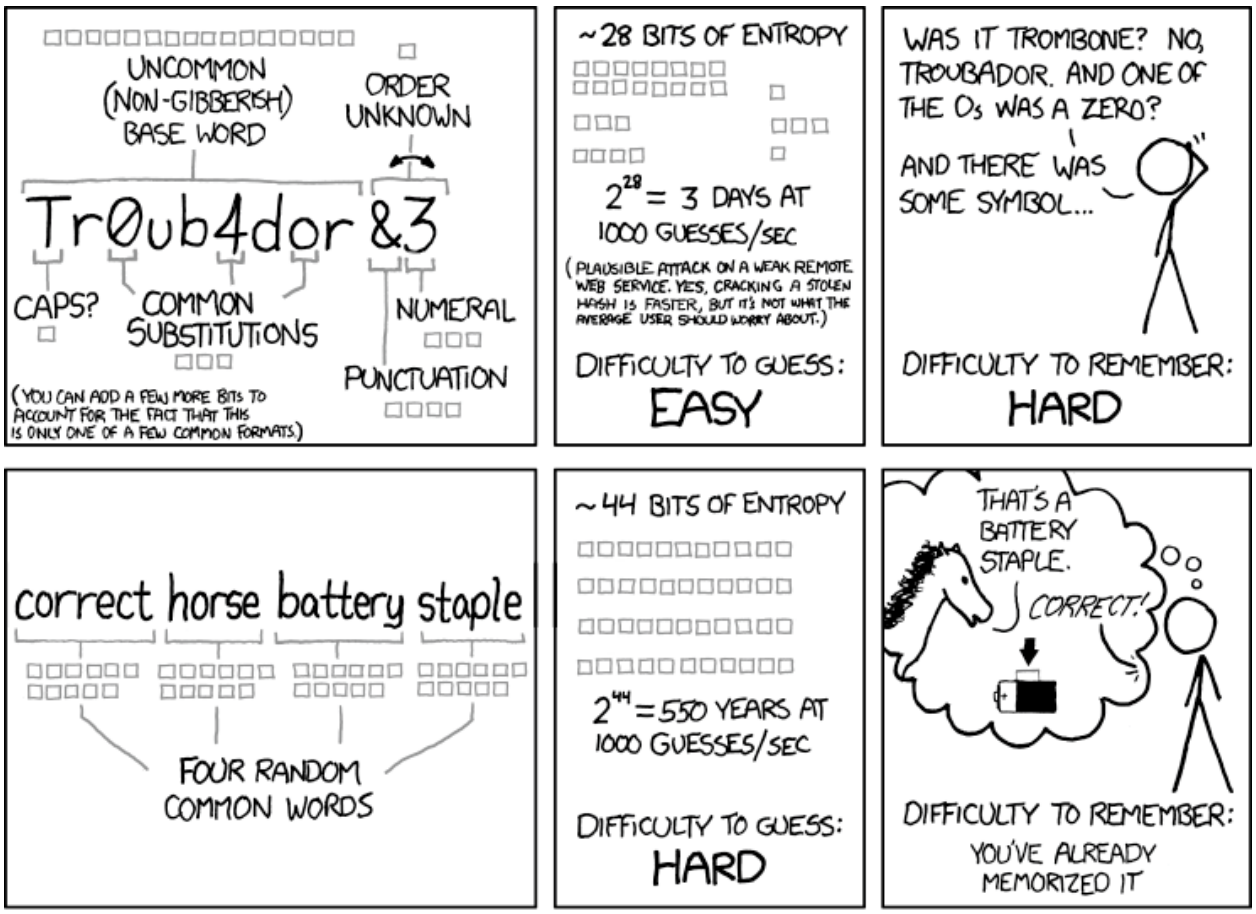
Some specific examples of passwords that achieve 44-bit complexity:

- AceHandleRugPlane
- 45HairPanPlumber
- 4n#}h$q

The last example is a 'random 7' password that is more difficult to remember but equally easy to guess as the first two. The 'random 7' password is included to demonstrate the incongruence between difficulty for human memorization and computational difficulty. Some complex passwords that attain less than 44 bits of entropy:

- Clower1!
- Why!1This

These poor passwords exemplify the popular approach for employees to satisfy recipe rules while minimizing memorization effort. A popular web comic helps to explain the concept behind longer passwords that are easy to remember:



Comic from xkcd.com [9]

Access Control

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.ACC.1	Controlled Access	Prerequisite to most other security measures; reduces damages from physical and informational losses	All	High	High	Low	Medium	Low
PT.ACC.2	ID Badges	Prerequisite to controlled access at larger organizations	All	Low-High	High	Medium	Medium	Low
PT.ACC.3	Computer Locking	Prevents momentary access vulnerability; reduces damages from physical intrusion	All	Medium	Medium	Medium	Medium	Low
PT.ACC.4	Computer Timeout	Fail-safe for computer access control; reduces costs of enforcement	All	High	High	Low	Low	Low
PT.ACC.5	Visitor Sign In	Increases visitor conformity, valuable for investigation; reduces costs of enforcement	All	High	Medium	Low	Low	Low
PT.ACC.6	Visitor Escort	Reduces physical exfiltration and unapproved information release; reduces damages from physical intrusion	All	Medium	High	Medium	Low	High
PT.ACC.7	Visitor Badges	Increases visitor conformity; reduces costs of enforcement	All	Medium	Medium	Low	Low	Low
PT.ACC.8	Visitor Phones	Reduces unapproved release and detailed reconnaissance; reduces damages from unapproved release and loss of intellectual information	All	Medium	Medium	Low	Low	Medium
PT.ACC.9	Employee Cameras	Reduces unapproved release; reduces damages from competitive and intellectual information losses	All	Medium	Low	Medium	Medium	Medium
PT.ACC.10	Access Audits	Prevents decay in access security over time; enables assessment of security measures	Admin.	Medium	Medium	Low	Low	Low

Motivation

Many of the other tips in this document become irrelevant if an adversary attains unsupervised physical access to a facility. Therefore, physical access remains the primary concern of information security, even in a computer age.

This section provides policies that help ensure guarded access to an organization and mediated release of information. The next section addresses measures to repulse individuals who are acting in disregard of policy.

Prevention

Controlled Areas

Some basic guidelines for physical access apply in all scenarios.

- Webservers, fileservers and backup disks should be kept in restricted areas, to guard against both accidental damage (unplugged cable) and intrusion.
- All areas that include workstations or laptops should have controlled access.
- Printers, copiers, fax machines, desks and other sources of hardcopies should have controlled access. Secure copiers and printers are available that require a keycard to access

hardcopies, and these maintain logs that can provide attribution for who accessed the device.

- If visual or audio presentations are given on sensitive topics, then access should be restricted to those. Presentations and meetings can be difficult to protect, as often space is limited and groups are difficult to control.
- All restricted areas should be protected by automatic locking (momentary unlock) doors, to prevent accidental violations.
- Locked doors should be supplemented minimally with cameras, and guards when deemed appropriate. Physical perimeters are further discussed in the 'Physical Espionage' section on page 48.
- Controlling access to an entire building is the easiest approach, but lack of access control at a smaller granularity creates a catastrophic failure mode and prevents role-based permissions or activity logging.
- Because internal access controls are not observable without some exposure, they are more resistant to preparatory reconnaissance and more robust to determined intruders.

Access Lists and Badges

The list of all individuals who are authorized to enter a controlled area should be centralized. Better, the list should be integrated with the access control system so that keycard access, etc. is updated automatically whenever the list changes.

Upon change of employment status or reduction in access privilege a review by an administrator should be performed to ensure that access has been removed. Logs should be maintained of changes, to aid investigation and auditing.

Locking Computers and Timeouts

Passwords become irrelevant if employees log in for the adversary. Unfortunately, many small businesses do not enforce basic access control to the computer system. All computers should be locked when unattended. To aid in preventing the worst violations, a timeout should be set to lock any computer after tens of minutes of inactivity. Modern operating systems display a picture or screen that obscures what is open on the computer once the computer is locked. On recent operating systems, the default setting is to require a key sequence to display the login dialog. On older operating systems, this option should be enabled to prevent password capture by programs that spoof the login dialog. For a discussion of spoofing and deceptive user interfaces, see the 'Phishing Websites' section on page 59.

Visitor Sign In

All visitors should register before entering a facility, and sign out before departure. This provides a count and list of all visitors currently inside a facility, or during a time window. A logbook is acceptable in many instances. However, a logbook itself can be a vector for information loss, for example if leakage of supplier or visitor identities to other visitors is undesirable. Registration cards reduce this information loss through public sign in.

Guests and Escorts

An organization inevitably requires outside people to come on site. Because guests are trusted only to perform certain duties, and access a limited set of objects, it is necessary to restrict all activities of guests. For day visits in an office setting, guests can be escorted at all times. The host of the guest can handle the brunt of the escort task.

For longer-term on-site work, arrangements that are more permanent might be required, including purging the affected area of sensitive information. In-house subcontractors should sign an agreement to abide by security policy.

By requiring guest to wear guest badges or other identification, the gravity of the organization's commitment to security will be more evident and this will encourage compliance.

Visitors and Cell Phones

Cell phones have become an ever-present issue. Consider if a no-phone or no-picture policy is needed for guests. If a no-phone policy is adopted, have provisions to stow cell phones in lockers or another secure manner at a welcome desk to avoid violation due to laziness or legitimate worry about the guest's own security.

Personal cameras

If the organization's secrecy or other security needs require that employees do not take pictures, consider a no-phone or no-camera policy for employees. Any requirement for approval of all public releases will likely necessitate a no-camera policy. Typically, a no-phone policy will be required only in highly secure areas. A no-camera policy can be enforced by granting the right to carry a personal cell phone to employees only after having signed an agreement to forfeit any camera used on site. A template policy for cell phones and camera usage is included in the 'Policy Templates' section on page 112.

Access Control Audits

The physical access controls for a facility should be audited on a regular interval and at any significant reconfiguration of the facility. Like most security systems, weak links determine the strength of the protections. Newly formed holes in access control weaken the entire security of a facility. Outdated and irrelevant controls will undermine the mandate of an access control scheme and lead to employee violations.

An up-to-date inventory of physical access passes, keys and combinations should be part of a physical access audit. Updates to the inventory should be made upon loss of any access credential, as well as mitigating the threat of intrusion by disabling digital cards and replacing physical locks. Employment termination or a change in status that eliminates need for access should also involve repossession of access credentials and return of those credentials to inventory.

Two Factor Authentication

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.AUT.1	Two-Factor Entry	Reduces instances of physical infiltration; reduces unwanted visitors, reduces labor cost for monitoring	All	Medium	High	Medium	High	Low
PT.AUT.2	Two-Factor Login	Increases hardness of the entire information system; reduces damages from credential compromise	All	Medium	Medium	Medium	Medium	Medium

Motivation

Keycards can be lost. Someone will write down or otherwise divulge a password. Looking across every employee in an organization, and over a long timeframe, the number of secrets that must be maintained is huge. Given the number of secrets, and number of modes of failure, it is unthinkable that at least one of these authentication credentials will not be compromised.

Nevertheless, it is very unlikely that any given two security credentials will be compromised concurrently. This is the basic motivation for second-factor authentication. To prevent a single point of failure of the access control scheme, a second factor should be required to access all restricted areas and restricted information.

Prevention

Second Factor for Authentication

Two-factor authentication requires two of the three authentication factors: something the user knows (password); something the user has (keycard, token display); something the user is (fingerprint). For physical access, a keycard and a short PIN code can serve as two factors. A four-digit PIN and a three-strike rule, to disable the keycard, is a sufficient second factor.

For local authentication, biometric data has gained some usage as a primary or secondary factor. The strength of biometrics is that the key thereby generated can, in theory, be much stronger than a password. Biometrics also do not need to be carried, cannot be lost, and are effectively immune to the password cheats that people use, like writing them down . As with other factors, it is important to have biometric keys in escrow to prevent problems due to changes in the metric, for example a wound on the finger used for fingerprint identification.

A token display is a popular choice as a second factor for remote login. A token display calculates a series of quasi-random numbers by hashing a random seed thousands of times and storing the hashes in a stack, such that the first tokens that are seen are hashes of future tokens. Given a token, it can be verified that the token is legitimate by hashing the token repeatedly and comparing each result to a previous token. Future tokens are very difficult to predict because hashes are one-way functions.

Biometrics traditionally required dedicated hardware, but image and voice recognition software has made biometrics less expensive at the cost of being hacked more easily. Token displays are available free from platform vendors, for example, Google Authenticator can be used to generate tokens using a cellphone. Escrow for token displays can involve out-of-band

information, for example a few ‘offline tokens’ that can be used to bootstrap a replacement phone as a replacement token display.

For a second factor, entropy is perhaps less important than unpredictability: a token is commonly only six digits. Reusable passwords are the weak chain in authentication because they are reused for months. Once in possession of a password, an adversary has continual access until the password expires or their nefarious activities are detected by other means. This is the motivation for imploring companies to enforce short password lifetimes and one of the reasons to deploy intrusion detection.

A token is valid for only a short window—maybe a minute or two—so tokens are much more resistant to stealing and reuse than passwords or biometrics. In fact, even if a password is stolen it is feasible that the token factor alone will prevent account compromise because it is much more involved to steal a token display than to extract a password either electronically or by social engineering.

Second factor can be supplement with out of band communication. For example, a server can require one, or two, factors to be entered from a computer, followed by a short PIN from a text message. The text message is sent to a separate device (possibly the same device as the token generator) over a separate network. Knowledge of the text message indicates physical control over two devices and successful communication over two networks, so the only single points of failure are then the person and server, as discussed next.

Limitations of Second Factors

Ultimately, biometrics and token displays are superior credentials compared to passwords, but are breakable. For elucidation of what biometrics or a token display actually offers, the attacks on these can be compared to the attacks on passwords. Biometrics are effectively immune to cracking and token displays are effectively immune to reuse, while password cracking works great on password databases and reuse works great on passwords. However, the differential in security that is offered is not as great as the differential in entropy or unpredictability suggests.

Password cracking works well because in a database there are usually some weak passwords that can be broken quickly. Nevertheless, modern password hashes and decent password composition rules can ensure that the majority of passwords in a database will remain unbroken during an online attack. The result is that when a specific password must be broken, cracking the password is usually not method of choice.

As with other cryptographic methods, it easier to attack a protocol than a password hash. Conceptually, a password is eventually represented as a digital key. This key is passed to authentication programs. This key is also subject to the usual thievery and tricks. Generic and effective techniques can extract any information in computer memory. An authentication key can remain in memory for hours after logging in.

Once a security key has been stolen, security protocols are easier to attack. For example, a common technique is ‘pass the hash’ where an adversary can simply send a stolen digital key to an authentication program, without knowing the password that generated it.

A biometric or token is eventually reduced to exactly the same key representation as a password, and so can be attacked in memory in the same ways. A pass-the-hash attack is an

example of reusing a credential that was calculated legitimately—a reuse attack. This attack operates much the same as with a stolen password but occurs later and internally. Pass-the-hash applies primarily to an adversary that has gained access to a machine already, and is attempting to escalate privilege, but can be used to attack vulnerable network protocols.

Physical Espionage

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.PHY.1	Shredding	Reduces information loss through refuse; decreases the labor cost to categorize all obsolete paper documents	All	High	High	Medium	High	Medium
PT.PHY.2	Camera Surveillance	Reduces initial reconnaissance and physical infiltration; lowest-cost security monitoring	Admin.	Medium	Medium	Low	High	Low
PT.PHY.3	Physical Perimeter	Reduces frequency of physical infiltration; decreases labor cost to manually monitor premises	Admin.	High	Medium	Low	High	Low
PT.PHY.4	Security Perimeter	Reduces physical infiltration and surveillance; decreases costs of training entire employee population for situational awareness	Admin.	Medium	High	Low	High	Medium
PT.PHY.5	Alarm System	Reduces exfiltration during physical intrusion, valuable for investigation; reduces damages from each physical intrusion	Admin.	High	Medium	Low	High	Low
PT.PHY.6	Physical Penetration Testing	Identifies threats to physical security; increases return for spending on physical security	Admin.	High	Medium	Low	Medium	Medium

Motivation

Most public attention with regard to security has shifted to cyber security. On a macroscopic level, internet fraud has become big business. While each email reflects little exertion, when many such emails are sent, each to tens of thousands of potential victims, the expected number of victims is greater than can be expected from old-fashioned fraud. The damages from internet fraud are now billions of dollars per year. On a microscopic level, computer users have come to encounter frauds and espionage in their daily lives in a way that average people simply did not in times past.

Changes in the economics of accessing victims have changed the way swindlers do business. The internet has allowed scammers to access huge communities of potential victims. Worse, the cost to send a malicious email is infinitesimal compared to the cost of an onsite visit or even a phone call. The concomitant change in the techniques of internet-based fraud is emphasis in quantity over quality. Often phishing emails are poorly formatted or translated. Phishing websites rarely accomplish the feel of a legitimate website. Awareness is often sufficient to avoid these attacks.

When the goal is not to cast a wide net and catch many unsuspecting victims, but to penetrate a specific organization by duping specific individuals, old-fashioned espionage remains the tool of choice. The methods of personal manipulation are known as social engineering, and are discussed below. These methods are more refined and better executed than other internet fraud. Rates of success for phishing emails are one in a thousand, or worse. A good social engineer will have a much higher success rate.

This section discusses the preliminary information gathering that a social engineer will perform before ever contacting an employee. The training and attention needed to resist social

engineering dependably are extensive. Luckily, the tools for stopping physical espionage are more straightforward.

Prevention

The security measures in this section are common knowledge. More so, a small business owner likely already knows that these protections should be in place. Nevertheless, motivations for these measures are detailed here to encourage their adoption.

Dumpster Diving

The office dumpster is a goldmine for espionage. Employees tend to see something they are throwing away as having little value to someone else. This makes waste a primary vector for information to escape a company, in both electronic and paper format.

Any document that contains confidential, private, or identifying information should be destroyed. Even documents that are ostensibly benign can be used to identify a target and are a great asset to a social engineer. For example, a flyer for an industry conference or a trade journal addressed to a specific person can be used together with other evidence to ascertain the name of the manager of a specific department. Such contact information aids social engineering and phishing attacks, as discussed in the next few sections.

A shred-everything policy can ease the burden of categorizing documents and catch the leaks that are not obvious. In addition, an on-site shredder and the observation of other employees shredding documents will help make the culture of information security at an organization more concrete. Shredding services are also available. To combat laziness, shredding bins should be at least as easily accessible as garbage cans.

Obsolete electronics are another vector whereby information tends to escape. Any hard drive should be wiped clean or destroyed before it leaves the controls of the information security system. Sanitization of drives is discussed in the 'Data Controls' section on page 71. Products to aid in hard drive destruction are discussed in the 'Hard Drive Destruction' section on page 152.

Camera Surveillance

Cameras alone can discourage opportunistic robberies and other attacks. For this effect, cameras need to be visible. One limit to the security provided by a camera is that rarely is a camera monitored. This makes a camera more of a forensic tool for investigating an attack that is detected by other means than a security barrier. Worse, often tapes are not even inserted, or the recorder is stored in a location that is both obvious and accessible to an adversary.

As part of a comprehensive physical security plan, a camera can be useful for stopping even determined adversaries. Before security can be circumvented by a social engineer, the adversary must know what security is in place. Therefore, most attacks are preluded by 'casing the joint' to discover what security measures are in place. The best defense against such reconnaissance is to observe the observer. Therefore, cameras should observe dumpsters, entryways, and other penetration points.

Security Perimeter

A security perimeter includes exposure, physical perimeter, and surveillance. Exposure requires an observable space with good visibility. A flat, well-mowed, well-lit ground is ideal. A physical perimeter must require time to circumvent. Fences are the overwhelming choice for a physical perimeter. Surveillance can be a guard, but more likely a camera. For a good example of a security perimeter, observe any prison.

The failure of most fence installations and other physical perimeters is to incorporate the fence into a comprehensive security perimeter. A lone fence provides outstanding protection from vandalism, petty robbery and other opportunistic attacks. However, the physical integrity of a fence is limited, and most jurisdictions do not allow razor wire and other fittings that present a real physical barrier to a determined adversary. Guard dogs are an extreme measure that most facilities cannot allow. Many fences also traverse the backsides of a facility with little or no lighting, heavy vegetation, no surveillance, and almost no chance of catching an adversary breaching the fence.

The key to a fence or other physical perimeter is to make the time needed to breach the barrier as costly as possible. If a physical perimeter is part of a comprehensive security perimeter, this time is spent: openly exposed and visible; doing something that is obviously malicious to any observer; and clearly being observed. The detection of a damaged fence also provides clear indication that a breach has occurred, so minimally, the breach of well-maintained perimeter will trigger forensic inspection of cameras and other evidence from surveillance. Even for determined adversaries, the combination of a fence, light, and camera is a substantial deterrent.

Ideally, a security perimeter will demarcate an excluded area large enough to prevent detailed observation of a facility from outside the perimeter. This perimeter should encompass any employee parking, to prevent exploitation of 'weak links' when employees fail to lock their cars and thereby expose security badges, personal computing devices, removable media, etc. Parking lots and other non-controlled areas are also good places to prime employees for social engineering attacks, discussed below. Once such a perimeter is in place, preliminary fact gathering by a social engineer is severely restricted.

Alarm System

An alarm system is a last line of defense and, like other measures used in isolation, really only discourages an opportunistic adversary. A well-researched break in will account for an alarm. A brazen thief might simply not care.

The greatest value of an alarm for stopping a determined adversary is to bring law enforcement on site within a few minutes and thereby mitigate bulk material removal from a facility. This effect is reduced if physical access is unrestricted, so that proper planning or fast action will allow an adversary to drive away before enforcement arrives. Proper perimeter security makes such a timely exit difficult. Only then does an alarm system become a real deterrent to a determined adversary.

Penetration Testing

Physical penetration testing involves attempting to access a facility to test access control. Rules of engagement may include social engineering, but typically not breakage. The testing can be performed by outside consultants, but to attain the best value for such services it is best to fix known issues beforehand. Interviews and requests for suggestions can identify many areas for improvement, and in the early steps of testing penetration testers often simply ask employees about ways to get in. Many times, mangers will find that tradespeople and guards that work with buildings and facilities daily are aware of trivial entry methods.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.SEN.1	Social Engineering Awareness	Reduces frequency of information loss; reduces damages from information loss	All	Medium	Low	Low	Medium	High
PT.SEN.2	Access Control Awareness	Increases the veracity of employee enforcement of access control, reduces the rate of success of tailgating and other infiltration behaviors; reduces damages from physical intrusion	All	High	Medium	Low	Medium	Medium
PT.SEN.3	Vendor Vetting	Reduces the frequency of physical intrusion by impostors; reduces damages due to physical intrusion	All	High	Medium	Medium	Medium	Medium
PT.SEN.4	Pre-Interview Screening	Reduces information loss through sentinels; reduces damages from information loss	All	Low	Medium	High	Medium	Low
PT.SEN.5	Employment Screening	Reduces frequency of inside adversaries; reduces damages from insider theft	All	High	Medium	Low	Low	Medium

Motivation

The motivations for guarding against social engineering were discussed under 'Physical Espionage' above. This section discusses the tactics and defenses for social engineering during direct human communication. Defenses against social engineering over the internet are discussed in the next few sections.

The risks of human interaction are of two kinds. First, employees will divulge much more information than they realize during casual conversation. Second, well-meaning employees will bypass security measures for an adversary, often out of politeness.

Prevention

Preventing information loss in casual conversation requires more extensive training and awareness than any other security measure. Preventing employees from being tricked into bypassing access controls is easier. This section provides a bare primer by way of a list of techniques to look for.

Engineering Conversations

Fraud and espionage have used the same basic manipulations since before computers. Employees must understand the tactics used by frauds if they are to expose them. The first step is to keep the context of interactions clearly in mind. A classic tactic among swindlers is to use habituated elements of legitimate social protocols within interactions that violate the contextual assumptions of those protocols. The systematic manipulation of culturally rooted social protocol gives rise to idea of 'engineering' social interactions.

- For example, the tone and vocabulary of an imperative is an expected imposition on the *initiator* of a phone call until he authenticates himself, but not an expected imposition on the *receiver*. By reversing roles and imposing an imperative on the receiver, demanding that the receiver authenticate himself, the interaction and context become inconsistent.

- Perceived authority aids the social engineer. This authority is gained by adopting a persona to whom the victim is socialized to acquiesce. An example is a 'doctor' calling, and needing to verify personal information to ensure he is talking to the patient. The most common tactic over email is to send an 'administrative' ultimatum to resolve a security or payment offense quickly.
- Background information lends believability to a fabricated context, a tactic called pretexting. For example, a stolen client database can allow a 'doctor' to contact patients with pretext to specific appointments. Pretexting is particularly effective because it uses the victim's own expectations against them.

One general method to combat misdirection and impersonation is to independently verify all contacts. This can be done by calling the supposed contact back. The phone number or email of the contact should be found independently.

Engineering Gestures

The norms of civil behavior dictate certain gestures. A social engineer anticipates these gestures, and uses them to manipulate people and security protocol. The tactics presented here could be included above, but are highlighted because they are used to bypass the basic access controls of a facility.

- The most dependable way to manipulate an employee is to make the employee familiar and even friendly. Once an employee recognizes someone, that employee will be inclined to stop asking if that person should be there, or doing what they are doing. In many cases, other employees will take a cue from an employee who welcomes a guest and assume that the guest has been vetted. A social engineer might build familiarity on site by frequenting non-secure areas, or by following employees to bars, restaurants, and other places they frequent. The following tactics are all supercharged when an employee actually recognizes and welcomes the adversary.
- The quintessential tactic to bypass human security is to feign some exceptional or uncomfortable social situation in which an employee is willing to make an exception. These methods rely on the social tendency to avoid a person displaying anger, hurry or sadness—even if this person would otherwise be scrutinized. Examples include an argument between people at a security desk, walking quickly while talking assertively on a cell phone, or crying.
- The common tactic to bypass automatic security is to manipulate human politeness. A social engineer can 'tailgate' through most locked doors by waiting for a polite employee to hold the door. 'Camping' at a locked door is usually not as obvious as standing in front of it. Instead, the situation can be made to seem coincidental by timing arrival. The act can begin minutes before, setting up the encounter by chatting on the way to the building, talking about company business on a cell phone in an elevator, or by merging with a group of employees. Entry is the final stage of physical infiltration and a social engineer might prepare by learning names and even faces beforehand.

Prevention depends on culture. The security culture within an organization must become ingrained so that employees understand and even appreciate the danger of holding a door for a stranger. Only then will employees cease to hold doors, scrutinize everyone, and not anger when others do the same to them.

Vendors

All guests should be vetted before entering a facility. While this may cause some friction, ultimately anyone wanting to do legitimate business should be willing to pay a small inconvenience. Some examples include deliveries or service people. Obviously, the service should actually be scheduled. Even when *someone* is expected, the identity of any outside contractor should be independently verified by looking up and calling a local office. Badges, other credentials, and verifying contact information presented by a visitor have no merit, as the appearance of a legitimate credential or identity of the contact is not independently verified.

To reduce the frequency of confrontations, any employee scheduling an outside service should preemptively establish the identity of the person who will be coming on site.

Fellow Employees

Employees often act as adversaries. This is especially true when an employee is leaving the organization. To mitigate the liability from inside adversaries, information should be compartmentalized and access rights should enforce explicit roles. Compartmentalization is discussed in the 'Labeling and Confining Information' section on page 96.

Screening of employees in sensitive positions can be continuous. Administrators are always sensitive positions. Many situations can increase the risk of an employee stealing information. It is mandatory in classified positions to undergo a regular review of legal issues, personal relationships, financial status and job performance.

Potential employees can also be adversaries, especially because knowledge of company operations is usually viewed as a positive factor during an interview. A pebble of information from an interviewee about a company can start an avalanche of information as interviewers talk about themselves:

> "I bet you are interviewing a lot of people right now."
>
> "Oh yeah, with the new factory going in and the new widget line in the works…"

An ambitious social engineer might even accept a job to gain inside access. Therefore, all employees should be subject to security screening, discussed in the 'Account Management and Employment Review' section on page 100. Screening can be conducted before performing an interview, but interviewees are understandably resistant to divulging personal information upfront for all but the most security-sensitive positions. Two forms of identification should be required as part of the screening process to deter impersonation and establishment of false identities.

After employment, a probationary period can be imposed. During this period, the new employee can have limited access and administrative privileges. At small companies where a single employee can be a significant fraction of the workforce, this can be a prohibitive expense. However, the inability to monitor employees also increases the risk from an insider threat at a small company.

Phishing Messages

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.PSH.1	Email Conversation Awareness	Reduces frequency of machine compromise; reduces damages from IT effort and information loss, overhead can overlap with social engineering training	All	Medium	Medium	Low	Medium	Medium
PT.PSH.2	Email Technology Awareness		All	Low	Medium	Medium	Medium	Medium
PT.PSH.3	Phishing Examples		All	Medium	Low	Low	Low	Medium
PT.PSH.4	Mock Phishing	Reduces frequency of machine compromise, provides memorable reinforcement experiences; facilitates assessment of the value of security spending	All	Medium	Medium	Medium	Medium	Medium
PT.PSH.5	Email Filtering	Removes the bulk of malicious email; reduces the labor cost to manually delete spam	Admin.	High	Medium	Low	Low	Low
PT.PSH.6	Late Filtering	Mitigates waterholing risk; small marginal cost-benefit ration for reduced damages from host compromise	Admin.	High	Medium	Low	Low	Low
PT.PSH.7	Client Filtering	Most dynamic defense against compromised websites; small marginal cost if running any host security	Admin.	High	Medium	Medium	Low	Medium
PT.PSH.8	Attachment Whitelisting	Reduces machine compromise by preventing most malware formats; small marginal cost if running any host security	Admin.	Medium	Medium	Medium	Low	Medium
PT.PSH.9	Fraud Reporting	Allows combating fraud on the internet scale; benefits everyone although it is a dominant strategy to abstain	All	Medium	Medium	Medium	Low	Medium

MOTIVATION

Most of the large-scale hacking attacks that grab news headlines do not begin with software vulnerabilities, but rather unwary employees. These attacks are called (spear) phishing, and target specific employees with some desirable access within an organization. Phishing is now the most popular form of cyberattack, and the dominant tactic for the initial penetration of an organization.

These attacks aim to steal vital security information for use in later phases—by tricking an employee into volunteering the information or by installing malware that extracts the information surreptitiously. Often phishing is used to extract user names, passwords or financial information. Phishing attacks also tend to persist and widen over time, as information gained is used to both find new targets and increase perceived legitimacy in future interactions. A common scheme is to use extracted names and email addresses of other employees as senders for future emails.

The problem arises in part because modern software is designed for speed and functionality, with an afterthought for security. One consequence is that malicious code can be executed from almost anywhere. A single click on an attachment or link in a malicious email can infect

the local machine. An infected machine can easily infect most networks. Once compromised, it requires expensive, expert mediation to purge a network.

Prevention

Conversational Training

Phishing is nothing new or specific to computer security. The tactics of mail fraud, spoof phone calls, etc. have simply migrated to email, messaging and browsing. The best defense against phishing remains well-trained, alert employees. In short, employees must think about security during daily interactions.

- All of the same tactics from the 'Social Engineering' section above apply to emails.
- Pretext does not have to be created: all organizations have enough public records to hook employees. Taxes, earnings, charities, legal cases, etc. all make available pre-packaged expectations. For example, immediately after an expensive lawsuit, an email from the opposing law firm with an attachment indicating another lawsuit will probably be opened eagerly by an executive.
- People will fall for standard parlor tricks. A resume, social media profile, or other personal information will divulge the activities, interests, and ambitions of employees. Like a fortuneteller, a social engineer will tell employees what they want to hear. An administrator with a desire for flexible hours, for example, will be more likely to open an email containing such an offer.
- Swindlers look for easy targets. Many phishing emails are mass spam that contain obvious visual or logical flaws, but people still fall victim. Studies have also shown that the inclusion of personal information does not greatly increase the success of spam emails. Victims simply are not alert.

Technical Training

Unfortunately, much of their software works to obscure the context of interactions from employees. Some details of the technology help explain why.

- Email is an ancient technology, built on plain text and naïve protocols. The sender name, email address can be set arbitrarily. Therefore, the sender of an email is always unauthenticated, and the interaction therein should be scrutinized and make sense within extant social context.
- Further, contact information, ID photo, shared calendar, status indicator, social media links, etc. are all superimposed by an email client to dress up the text of an email, based purely on the unauthenticated sender field. Therefore, almost all of the visual evidence presented to a user serves to legitimize a forged email.
- Spoofing is made easier because there is no connection between the appearance of a link and the target of the link. Therefore, text links, buttons and pictures in an email can link to anything.
- Common sense diligence is punished by current software because there is no contextual distinction between trusting and investigating an email. Email clients are getting better, but it remains safer to assume that a client will follow any link that is clicked, and execute any code found there—without asking. Older clients sometimes execute code when simply

opening an email. Even new clients can make it difficult to discern the destination or even existence of a link. The result is that it is not safe to check manually if a suspect email is legitimate.

Mock Phishing Campaigns

Training tools also include mock phishing emails. These emails attempt to trick employees into clicking on a link that leads to a webpage explaining the deception in the email. A less intrusive method is to sanitize and distribute real phishing emails together with explanation of the tactics and flaws contained in the email. Mock phishing campaigns have the advantage of doubling as one of the few quantitative self-assessment tools for a security-training program.

Late Email Filtering

Email servers often filter messages and links. Unfortunately, waterholing and other techniques have been devised to bypass server-side filtering. These techniques are discussed below. One common strategy is to send phishing emails on Friday that link to a legitimate website, allow time for the emails to pass server-side filters, and then compromise the website over the weekend. A waterholing attack is then ready for Monday morning when employees will actually open their email. To help prevent this, email should be scanned when downloaded from the server. This introduces noticeable delay for email retrieval.

Client Scanning

Avoiding phishing attacks is sufficiently difficult that prudent training should be supplemented with filtering and intrusion detection. Host security suites often include client-side email scanning, link checking, website blocking, and other protections against phishing attacks. This checking is done when opening an email, so several attacks that bypass server filtering can be detected. Host security products are discussed in the 'Host Based Security' section on page 124. Virtualized browsing is more effective, and is discussed later in the in the 'Virtualized Browsing' section.

Attachment Whitelisting

Malicious links gain a lot of attention because newer web-based attacks are very effective. Nevertheless, the most common entry vector for malware continues to be attachments. A simple mitigation is to allow only business-relevant attachment types. Application whitelisting can block most types of malware, but cannot block most instances of malware because ubiquitous attachments types are the most frequently used for malware, for example a PDF. Awareness training therefore remains critical.

Reporting

Suspicious email or other communication should be reported to law enforcement and the misrepresented company, if any. For example, a suspicious email associating itself with ABC Bank should be reported to ABC Bank, so that organization can warn its associates.

In the USA, suspicious email should be reported to the United States Computer Emergency Readiness Team (US-CERT). This is a quick, automated process. Simply attach the suspicious email and send to phishing-report@us-cert.gov. These incidents are not too trivial to report; investigators are aided when they can associate details of many attacks with a piece of malware.

Do not expect feedback following an automated report, but be assured these reports are valued.

Any specific information regarding a particular attack, fraud or group perpetrating these acts should be reported to the Federal Bureau of Investigation (FBI). Defense contractors have the additional requirement to report potential attacks to the Defense Security Service (DSS), and should consult their contract documents. To make reporting easier for employees, these emails can be forwarded to an administrator or help desk.

Phishing Websites

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
---	Email Filtering	See previous section for details	Admin.	High	Medium	Low	Low	Low
PT.PWS.1	Training - Awareness	Reduces link clicking behaviors; reduces damages from web browsing without further cost for monitoring and enforcement	All	Medium	Medium	Low	Medium	Medium
PT.PWS.2	Training - Technical	Reduces promiscuous browsing behaviors; reduces damages from web browsing without further cost for monitoring and enforcement	All	Low	Medium	Medium	Medium	Medium

Motivation

Phishing websites share the same goals as phishing emails: extract information that provides access to something of value. Phishing emails often work in tandem with phishing websites. The motivations to prevent phishing websites are then the same as given above for phishing messages. This section details technical aspects specific to websites.

Prevention

Awareness is the first and best defense against phishing. Below are several points that illuminate how phishing works so that it can be more readily identified when it is encountered.

Attack Tactics

Phishing websites attempt to mimic legitimate websites. Websites do this by spoofing and waterholing.

- Spoofing involves creating the appearance of a legitimate, authoritative contact. An example would be an impostor actually dressing up as a doctor, or a malicious webpage replicating the look and feel of a legitimate website.
- Waterholing involves compromise of third-party websites that are frequented by intended victims. Users are manipulated after reaching the correct webservers, so all links in emails are legitimate. When a victim visits these websites, either a compromised server collects data, or the victim is redirected to a spoof site.
- Waterholing adds a level of indirection to phishing, and provides an avenue to attack secure organizations by compromising less-secure websites.
- Waterholing can be used to cast a wide net and identify high-value targets within a community during the run up to a targeted phishing campaign.
- Because waterholing can involve little more than passive data collection, these attacks can be hard to detect, large scale, and persist for months.
- Common defenses can be bypassed by waterholing. A common tactic is to send phishing emails over the weekend, allowing these emails to pass email filters days before an attack commences at the websites linked by the phishing emails.

Visual Deceptions

Phishing websites also exploit complexities in how users perceive a webpage. Graphical rendering creates an arms race between spoofing and security, such that the user cannot trust what is displayed.

- Tactics include embedding pictures of text to avoid phishing scanners, or to obscure the existence of a link.
- Linked pictures can mimic popup windows, even display an 'X' to mimic the button to close a popup.
- Images can be placed over the address bar or link preview pane to display a legitimate URL.
- An entire legitimate webpage can be loaded beneath a transparent page with malicious links placed over legitimate links.
- The appearance of a URL itself is complicated. Most clients and browsers now display the actual destination URL at the bottom of the window when the cursor hovers on a link, but even when this is checked, internationalization and translation can be used to create legitimate-appearing URLs. Even simple misspellings of popular websites are effective: *bigbank.com* becomes *biqbank.com*.
- A phishing attack is often unnoticed by the victim. For example, a phishing attack can use the above tactics to lead a user to a spoof website, collect user name and password, and then forward the user to the login page of the real website. The user will likely assume they have mistyped their login information.

Defense Techniques

Some easy techniques to avoid attacks are:

- Do not follow links in emails. Always type URLs into the browser's address bar manually.
- Never click on a picture on a dubious website.
- Only use the 'X' or 'close' button on a window provided by the operating system, and be cognizant of whether a window is actually a photo rendered within the browser.
- When conducting ecommerce, check the address bar for *https://* or the lock, color or other security indicator in the address bar of the browser.

Social Media

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.SME.1	Usage Policy	Reduces social engineering reconnaissance and account correlation; reduces off-task activities, reduces damages from phishing attacks	All	Medium	Medium	Medium	Low	Medium
PT.SME.2	Pre-Post Review	Reduces unintended release by unmediated posts; protects the brand image	Admin.	Medium	Medium	Medium	Low	Medium
PT.SME.3	Password Management	Reduces frequency of site hijacking; reduces image degradation from hacker posts	Admin.	High	High	Medium	Low	Low
PT.SME.4	Safety Awareness	Reduces personal vulnerability due to social media presence; reduces damages from employee personal trauma	All	Medium	Medium	Medium	Medium	Medium

Motivation

Social media exposes three nearly independent risks. The first is that personal social media usage greatly aids fact finding for a social engineer or phishing attack. The second is that corporate social media can easily lead to unintended release of information if not properly controlled. Finally, social media exposes individuals to increased risk of ordinary crime.

Targeted espionage involves correlating disparate facts gathered from many places. One of the most powerful tools for correlating intelligence gathered from network data is to be able to associate a computer or network address with a person. Associating multiple computers and accounts with a single person can provide many new attack vectors. Simply logging into a social media site from work can provide such a connection. By correlating work computers with personal computers, the identity and personal details of an employee can provide powerful fuel for phishing attacks.

Informal interactions, such as Twitter, have become popular targets for phishing. The danger lies partly in the fact that, unlike in formal correspondence, users expect ill-formed messages that lack any context on social media sites. An example is a personal message, "*You did??:)*", linking to a spoof login website (discussed above). Fundamentally, users are at risk of waterholing or similar attacks anytime they enter authentication credentials or personal information on the internet. Unlike public webpages, this is nearly always the case on social media sites.

Concerns about phishing complement traditional concerns about release of information. Social media tends to disseminate information quickly, and people tend to post information, personal or otherwise, impulsively. This can lead to unintended disclosure of sensitive information, or damage to a company's image if employees or account hijackers express personal opinions that become associated with the organization.

Finally, social media can be used to track the activities of people. Unfortunately, this makes the prep work for robbery and other crime easy. Criminals increasingly use social media to identify unattended houses and other easy targets.

Prevention

Personal Social Media Usage

Every organization should consider a social media usage policy. If the organization deems that social media prohibition is appropriate, several levers can be used to enforce the policy. The simplest approach is to ask employees to abstain from social media while at work. Other tools include content filtering and website blocking. Almost the only protection from disclosure of information when employees are at home is to ask employees to refrain from sharing any specific information about the company while online.

Corporate Release Review

Ultimately, corporate social media is self-advertising for an organization, and this information source should have oversight similar to that for other advertising avenues. Namely, employees must understand the purpose of corporate social media and operate within these bounds.

To provide checks on the rapid release of information, a minimal release procedure should be in place. This process can entail anything from a two-person review rule to formal submittal and managerial review.

In addition to information that is contrary to the corporate brand image, personally identifiable information can also be problematic in social media posts. Any post to a corporate site should be made as an anonymous corporate contributor. Advertising the identities and daily activities of employees can provide much information for a social engineer.

Password Handling

The same rules for secure passwords within the organization's network apply to corporate social media sites. A different password should be used for every role, and certainly for every website. Once a password is broken, a good thief will try this password on many popular websites.

To control the image of a brand on social media sites, access to managerial functions should be tightly controlled. Most sites offer multiple user roles for corporate accounts. For accounts with many access rights, passwords should be very carefully controlled. This is especially true for accounts with rights to remove other administrators. To avoid the most sensitive accounts being compromised through side attacks during non-administrator activities, it is advisable to remove normal editing rights from administrator accounts.

Personal Safety

Some things should not be posted on social media sites. In other cases, the timing of a post is important. Addresses, detailed directions, and other identifying information for one's private residence should never be posted. Even pictures of one's house increase risk: most home robberies are perpetrated by local thieves who might recognize the house. Posting vacation plans ahead of time or vacation details while on vacation both provide thieves with tantalizing leads for empty houses. Instead, vacation photos can be posted after arriving home—once the window of opportunity has passed.

Posting personal information can enable identity theft and phishing. Most people know not to disclose their social security number, but birthdate can also be used by ID impersonators.

Posting an email address not only invites spam, but also aids in phishing friends. Social media is a goldmine for understanding the connections between people. With known connections and a valid source email, one's friends can be tricked into opening a malicious email.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.SUP.1	Manual Update	Reduces frequency of compromise of industrial controls and network infrastructure; reduces damages from network infiltration	Admin.	High	High	Low	Low	Low
PT.SUP.2	Automatic Update	Reduces frequency of malware infection on hosts; reduces costs of manual update and employee waiting	Admin.	High	High	Low	Low	Low
PT.SUP.3	Domain Update	Reduces effort to manage patch versioning across a network; reduces all administrative security costs	Admin.	High	High	Low	Medium	Low
PT.SUP.4	Update Management	Improves patch regularity and response; reduces the risks following patch releases	Admin.	High	Medium	Low	Medium	Low

Motivation

Apart from human error, malware infects a computer by exploiting some vulnerability in the software running on the computer. New vulnerabilities within computer programs and operating systems are discovered on a daily basis. Luckily, patches are also distributed aggressively, especially after an exploit of a particular vulnerability becomes known.

The penetrate-and-patch cycle makes vulnerabilities sufficiently valuable to malware makers that rarely are more than one entry exploit used. A 'zero day' vulnerability that has not been patched is extremely valuable. Given this scarcity, most malware makes use of known vulnerabilities that have already been patched. Therefore, prompt patching off all software is a critical step that will stop the majority of malware [1].

Prevention

Automatic Updates

For small networks, setting each host to download and install updates automatically each night will likely be a workable solution. All common operating systems offer this service. It is up to the individual user to accept these updates and possibly restart the computer, so employees must be trained and understand the need to do so. Automatic updating should extend to operating system, antivirus definitions, and application programs.

For larger networks, pushing updates to all machines is much easier using a group policy. In Windows, Windows Server Update Services (WSUS) is the standard tool for centralized administration of update policy. In Linux, no standard method exists. Puppet (https://puppetlabs.com/puppet/puppet-enterprise/) is perhaps the best known, and Vagrant (http://www.vagrantup.com/) can manage virtual machines as well.

For specialized software, patches will typically not be registered, so updates must be done manually. Many vendors offer security advisories for their products, and will send notices to anyone who subscribes.

One problem with updates alone is that some software is designed to allow multiple versions to be installed. Often development software of target platforms (Java, for example) retain old

versions when new versions are installed. Automated inventory (Network Inventory, page 145) should be configured to flag older versions for uninstallation. Exceptions might be needed for development machines, but these exceptions should be approved and documented to prevent a loophole in version control.

Patch management should also be integrated with malware and intrusion detection. If one machine is compromised then machines running similar software are likely susceptible. If possible, the entry point for infection can be used to focus efforts to mitigate the same vulnerability on other machines. In some cases, a patch is not yet available and software or specific settings must be temporarily disabled to prevent further infection.

Manual Updates

Malware also increasingly targets infrastructure, so administrators should patch routers, switches, computers, and even phones. Each of these devices should be updated to the latest firmware and available software to ensure the latest security updates have been applied.

Many industrial or infrastructure products do not have any automatic patching service. These products are managed through version updates or security advisories. Therefore, it is critical to subscribe to vendor notifications for these devices and to update any affected system manually.

Update Management

Automated updates with domain enforcement can ensure patches are eventually applied. Vulnerability scanning can identify unpatched software. However, only actual measurement of the performance of the patching system can ensure the result is within acceptable bounds. Many times administrators are surprised at the number of unpatched systems that remain after vulnerability identification and despite mandatory patching.

To ensure return of investment, a goal should be set for the window to patch software. This can be several days, but should not fall far behind patch notes because hackers begin developing exploits as soon as patch notes are released. With a goal set, initial measurements will typically fall short of the goal.

Root cause analysis can identify why some systems are not being patched. Typically, administrators avoid heavy-handed or disruptive policies but sometime employees will go to extraordinary lengths, delaying automatic updates for months. Mandatory restarts might be needed. Infrastructure tends to be forgotten in the busy schedule of IT administrators, but a log should be kept of when patches were applied, when those patches were published, and when any vulnerabilities were first discovered by scans (Penetration Testing, page 157). Administrators often find they too delay patches for weeks or months. With measurable performance in hand, the case can better be made to management for more resources to implement and maintain patch controls.

Software Installations

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.SWI.1	Newest OS Version	Increases hardness of installations; reduces configuration and management costs	All	High	Medium	Low	Medium	Medium
PT.SWI.2	Newest Browser	Reduces frequency of infection when browsing; reduces damages from compromise and costs of incident response	All	High	Medium	Low	Low	Low
PT.SWI.3	Baseline Installation	Reduces nonconformance by establishing secure settings for use by most employees; reduces effort to install new machines	Admin.	High	Medium	Medium	Low	Low
PT.SWI.4	Minimal Installation	Reduces vulnerability surface for all computers; reduces management effort and frequency of infection	Admin.	High	High	Medium	Low	Low

Motivation

One of the basic functions of a computer security administrator is checking installed versions and updating. In addition, settings must be tweaked to disable unsecure and unused features. Much of this standard practice accumulates as default settings for newer versions of software. Newer versions are also architected with security as an increasing priority.

Prevention

Use the Newest Version

There is a common misconception that newer versions of operating systems, applications and browsers are not as mature as older versions. Over time, security has become more important and, from a security perspective, newer is better. For example, each newer version of Windows is more secure than the last.

This happens in many dimensions. Many default settings are tightened. In newer versions of Windows and Linux, fewer services are 'on' by default. This greatly reduces vulnerability surface for any organization that does not pay close attention to default settings. It would take a great deal of expertise and time to tweak the settings of Windows XP to be as locked down as the default settings for Windows 8, even when equivalent settings are available. Linux distributions tend to be nominally more locked down than Windows, and these operating systems similarly tighten settings over time.

Newer architectures are inherently designed for better isolation and security. Older browsers allowed a website to access almost anything on a machine, including cookies and scripts from other sites. Render systems especially could be easily bypassed to access other open pages and many unintended areas. Unfortunately, security has been typified by the reactive penetrate-and-patch cycle. These problems persist, but the race between penetrate and patch in certainly lost when using dated versions of software.

This phenomenon occurs for several reasons. One of the most important is that unsecure features cannot be blocked because people would complain if, for example, popular websites

stopped working. As pressure is put on application developers, practices improve. When an unsecure feature becomes marginalized, it can finally be blocked. Those who follow web trends and browsers can watch as the usage of an unsecure feature declines to a few percent, and wait to see what browser takes the initiative to block that feature first.

This phenomenon is especially true for the World Wide Web because it is relatively new and technology has changed quickly. For demonstration, imagine one could jump in a time machine and go back ten years carrying a computer with the latest version of Windows and the newest versions of Internet Explorer and Google Chrome. Upon arrival, most websites simply would not work with the newer browsers. Standard practices have moved away from some very unsecure practices.

Baseline Installation

It is best practice to maintain a baseline installation of each operating system that is used within an organization. This installation then carries with it the best security practices of the organization by way of registry settings, installed applications, application settings, etc. Typically, this installation will have many security settings tightened compared to the default operating system configuration.

Newer versions have fewer services enabled by default but the number of installed applications has not similarly reduced. It is common during audits to find unpatched versions of software that is not used because it is forgotten. In general, the principle of least vulnerability surface applies equally to application settings, installed applications, operating system settings, and overall network capabilities.

The baseline image should be reviewed and updated on a regular schedule as well as when changes or security events dictate. Reconfigurations of the network are also a good time to revisit baseline installations. For auditing, forensics, and to mitigate the risk of regressions in new installations, a previous baseline should be retained for at least as long as any system on a network is running an operating system installation that originated from that baseline.

Data Integrity

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.DIN.1	Automatic Backup	Reduces frequency of accidental data loss; reduces damages from lost data	Admin.	High	High	Low	Medium	Low
PT.DIN.2	Offsite Backup	Reduces probability of massive data loss; Increases operational resilience to catastrophic events	Admin.	Medium	High	Low	Medium	Low
PT.DIN.3	Device Backup	Mitigates the risk if accidental data loss; decreases damages from mundane data loss events	All	Medium	High	Medium	Low	Low
PT.DIN.4	Integrity Monitoring	Reduces frequency of malicious data loss; reduces damages from compromised data	Admin.	Medium	Medium	Low	Medium	Low
PT.DIN.5	Backup Encryption	Reduces frequency of data leakage to third party storage vendors; reduces costs of vendor vetting, reduces damages from information leakage	Admin.	High	Medium	Low	Medium	Low

MOTIVATION

Most businesses are concerned primarily with data integrity. Data integrity involves preventing data from being unintentionally modified. This encompasses accidental modification and malicious actions, so there is need for data redundancy even without consideration for security: disk failures, power outages and fires plagued information storage well before hackers. Data loss due to computer failure or disaster is a more likely threat than espionage.

The determining factor in the need to backup data is the cost to reproduce that data. Many companies will find their data irreplaceable. If so, the backup strategy for this data must survive the company itself.

Data confidentiality and data integrity together are coverage concepts, meaning every piece of information within an organization need be retained forever and so its integrity must be ensured, or retained for limited time and destroyed to prevent leakage. Often both integrity and confidentiality apply to a piece of data. Unfortunately, there is an inherent conflict between integrity (making multiple copies) and confidentiality (keeping inventory and ensuring secrecy of all copies).

Integrity measures are usually supplemented with confidentiality measures, such as encrypting backups and minimizing the amount of cached data that is exposed on mobile devices when traveling. Creating a document management system is out of the scope of this document. However, the considerations here and the discussion of encryption products in the 'Data Confidentiality' section on page 130 aid in establishing integrity and confidentiality requirements for such controls. Considerations for mobile devices and travel are discussed in the 'Travel and Laptops' section on page 94.

Prevention

Automatic Backup

The events that might destroy data range in scope from a cubicle to a city, and have corresponding frequencies ranging from regular occurrence to being of historical significance. Data backups to counteract data destruction should have both correspondent costs to activate and dependability.

A comprehensive backup solution then necessitates a hierarchy of controlled redundancy to make common cases fast and uncommon cases failsafe. Proximate copies should be used to guard against common losses like hard drive failure or accidental deletion, and should be updated very often, maybe constantly. In addition, the cost in time and effort to recover this data should be low. This can be accomplished with disk mirroring, as provided by RAID hard disk arrays.

Distant copies should be secure from regional catastrophes but can be considerably difficult to activate, taking up to days to bring online. On the far end, shipping quarterly images of the organization's core database to offices in other regions by mail might be acceptable. Between these extremes, network backups provide a nice compromise that scales from nightly backups onsite to offsite cloud synchronization.

It is up to the organization to determine the depth of defense needed. A small business might simply disband if their sole facility is flooded; geographically remote backups would be superfluous. A global financial corporation might require backups on every continent.

Laptops and local copies

Data cached on laptops and workstations should always be backed up to a network device so that two copies exist. Integrity can be ensured during network storage backups. Many businesses that are too small to have established backup procedures are moving to cloud storage solutions. Cloud storage ordinarily has the added benefit of redundant backups, but a company should consider the issues in the 'Cloud Security' section on page 82 before moving to cloud storage.

If anywhere/anytime data access is not needed, but employees do need to cache their current work on their mobile devices, employees can mirror folders between local machines and network storage using an application such as FreeFileSync (http://www.freefilesync.org/). One caveat is that mirroring folders tends to increase exposure to loss and theft while traveling because more data than needed tends to be mirrored onto mobile devices.

Integrity Monitoring

Besides physical destruction, data can be modified maliciously. Often this is done by malware in an attempt to infect applications, elevate its capabilities, or hide its activities. Online file monitoring is a facet of intrusion detection, and is provided by some of the same tools: host-based security is discussed in the 'Host Based Security' section on page 124 and some of these products provide monitoring of files.

Monitoring of offline backups is necessary to assure that the backups serve their purpose. Aside from malicious action, media can degrade. Often neglect renders backups less secure than the data they are supposed to assure.

Encryption Requirements

Offsite backups will usually need to carry some confidentiality designation. In most cases, backups will need to be encrypted. Certainly, any backups stored with third-party vendors will need to be encrypted. A further discussion of vetting datacenter providers is included in the 'Cloud Security' section on page 82.

Data Controls

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.DCT.1	Location Tracking	Reduces frequency of data loss; reduces damages from information loss, overhead can overlap with inventory controls	Admin.	Medium	Medium	Medium	Medium	Medium
PT.DCT.2	Access Control	Reduces frequency of data leakage; reduces damages from infiltration and insider theft	Admin.	Medium	Medium	Medium	High	Low
PT.DCT.3	Encryption Policy	Reduces frequency of data theft; reduces costs of physical controls and monitoring	Admin.	Medium	Medium	Low	Medium	Low
PT.DCT.4	Key Management	Reduces probability of massive data loss; necessary for operational integrity of the organization	Admin.	High	High	Low	Medium	Medium
PT.DCT.5	Device Sanitization	Mitigates the vector for information loss through discarded, resold or transferred devices; increases the residual value of electronics without increasing risk of information loss	All	High	High	Low	Low	Medium

Motivation

The first task in handling data is to know where the data is. Unfortunately, losing track of the location of data is a common reality in organizations. Once location is documented, data are still at risk of being accessed by unintended parties.

As discussed in the 'Data Confidentiality' section on page 130, encryption is critical to securing data when it is not in use. In short, data on a hard drive, tape or flash drive can be read by anyone with access to that media. This applies to backups, databases and workstations, but especially laptops and removable media. Encryption is straightforward to use, but creates new vectors for information loss due to lost encryption keys.

Prevention

Physical location

The physical location of data should be documented. Data are typically not forgotten in place, but lost during a series of moves of which no person or department has complete knowledge. Therefore, a written procedure should exist for the checkout, check-in and relocation of data. These procedures follow direct analogy for control of any physical inventory.

Also like physical inventory, access to data must be controlled. Secure locations, encryption standards, and access control lists for most data should be documented at division or department level. Corporate databases should be handled centrally.

Key Management

Several risks are associated with encryption. First, passwords or keys might be forgotten. Second, an employee might hold data hostage. To avoid loss, key management should mandate an escrow plan for all keys used to encrypt data within an organization. Keys used to secure data under the purview of fulfilling a contract should be escrowed by the contractor. Similar to keys, encryption algorithms should be standardized and documented.

Implementing key escrow is non-trivial. The following controls should be observed.

- To prevent compromise of escrowed keys, all key extraction should require multiple parties. Typically, at least two people must be present and authenticated to allow key disclosure. Two-factor authentication should be required of each authorizing party.
- The software and other resources that are used to generate and store keys should be measured periodically to ensure that no tampering or replacement has occurred. Likewise, every key should accompany an associated certificate to ensure tamper proofing.
- Communication channels for key distribution must be well thought out and documented. Ad hoc key dissemination will dependably undermine an encryption system.
- Like passwords, encryption keys should have defined lifetimes and the lifetime should decrease for keys that are more sensitive.
- Key storage should be backed up and the protection and retention policy should meet or exceed the most stringent requirement for any encrypted data.
- Signing keys should never be held in escrow. Second-party control logically undermines the salient characteristics of verifiability and non-repudiation. If a private signing key is lost, a new key should supersede the lost key.
- All private signing keys should be retained for the full period of possible legal action. Some jurisdictions now enforce legal liability for cryptographic signatures.

Key escrow, spillage and changeover of public signature keys should be integrated into the reporting requirement detailed in the 'Labeling and Confining Information' section on page 96.

Device Cleaning

Residual information remains after a copy of a digital file is placed on a device. Some cases are obvious, as with a file on a computer hard drive or a USB drive. Additionally, almost every device that processes digital information contains non-volatile storage and makes copies of the data that it processes. The number of devices that store copies of temporary files is surprisingly large: printers, copiers, fax machines, projectors. Even phones store account credentials. This data remains even after deleting a file or a job is completed.

Any device with persistent memory should be decommissioned before leaving an information control system. Decommissioning should include destroying or shredding hard drives and removable media—details of tools to do this are given in the 'Hard Drive Destruction' section on page 152.

Collaboration and Confidentiality

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.CAC.1	Collaboration Awareness Training	Reduces frequency of information leakage by unsecure communication; reduces damages from information loss	All	High	Medium	Medium	Medium	Medium
PT.CAC.2	Secure Channels	Increases conformance with information controls; reduces costs of enforcement for information release	All	Medium	Medium	Medium	Medium	Low

Motivation

Employees collaborate throughout the day using phone, email, messaging and other tools. Therefore, it can be an automatic response to communicate with vendors, customers, or remote coworkers using these same tools.

Unfortunately, common communication tools like email and messaging are not designed for secure communication. Emails are, by default, sent in plain text. This means that when an email is sent, anybody on the internet can intercept it and look directly at the contents of the email. Any data transmitted across a public communication utility is not only visible, but is sometimes recorded and stored by third parties. This stored data is not owned or controllable by the originator of the message.

Prevention

Awareness Training

Training and tools are both essential to engrain the habit of secure communication within an organization. It is important for employees to understand that sending confidential information via email is a very large security risk and should be avoided. Points to include in collaboration awareness training include internet routing and email technology.

Traffic on the internet does not go directly to its destination, but bounces through many switches that are operated by many companies. The routes a message can take can be surprising. It is common for email sent within one country to leave that country at some point. When malicious actors taint Border Gateway Protocol (BGP) tables, much of the traffic in a region can be routed through a different continent. Any organization on the route can inspect and store an email.

Email technology itself is not secure for confidentiality or integrity. Email can be spoofed y setting the sender to whatever one desires. Email can also be modified in any way because the base email protocol has no checks on content. The text in an email is just that, plain text. Any of the organizations that see an email on its route can easily read that email.

Collaboration Tools

If sensitive information must be passed over the internet, proper tools should be used. One of the most popular is VPN. Details of secure collaboration tools can be found in the 'Confidential Collaboration Tools' section on page 134. One point about encrypted communication is that keys and passwords must be transmitted by different channels than those used for the data

thereby encrypted. Once a more secure but costly transfer of credentials has taken place, information can be sent encrypted over ordinary channels.

As important as the availability of secure channels is the habit of using them. Employees by default use the easiest and most familiar methods of communication. If employees do not gain the habit of using VPN or other secure channels, they will send sensitive information by email without thinking.

Remote Sessions

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.REM.1	Encrypted Connections	Mitigates threat of eavesdropping on credentials and data even locally; reduces damages due to compromise of machines	Admin.	High	High	Low	Low	Low
PT.REM.2	Remote Authentication	Reduces frequency of remote intrusion and mitigates risks from third-party management of credentials; reduces administration costs for outside accounts and damages from remote attacks	Admin.	High	Medium	Low	Low	Low
PT.REM.3	Remote Roles	Reduce attack surface and slow penetration during attacks from outside accounts; mitigates damages due to intrusion by third party and external accounts	Admin.	High	Medium	Low	Low	Low

Motivation

Remote sessions occur when a process on one machine logs in on another machine. This can be done within a facility or across the internet, as with VPN or webmail.

Prevention

Encrypted Connections

Any service that requires login should use encrypted connections, especially if it is hosted on the public internet. Services include webmail, file hosting, intranet, etc. Encrypted connections are needed even if remote sessions do not have write access to anything, as passwords can otherwise be sent in plaintext and reconnaissance and network mapping alone can be damaging. Vendors, customers and affiliates should also use encrypted connections for any services they offer. Specific technologies and safety checks that can be performed by a user are discussed in the 'Web Encryption Technologies' section below.

Major cloud and search vendors have had to implement encryption of the pipeline between their facilities due to government surveillance. Smaller companies that are involved in support, even indirect, for critical industries should expect similar eavesdropping from state actors and possibly competitors at this time. In all cases, an adversary who is resident on a network will eavesdrop on packets sent over the local network, so remote login, administration, and data transfer should be encrypted even on wired networks within a single room. Luckily, the effort to use secure services like SSH, SFTP and HTTPS has become standard and expected by employees, so there should be little resistance to closing the gaps that remain.

Remote Authentication and Privilege

Affiliates have become a major vector for attacks. Several major breaches have originated with remote sessions from affiliates and insufficient isolation of these sessions. It is difficult to gauge secure practices among customers, and difficult to enforce contractual security stipulations placed on vendors.

Better account management within an information system can mitigate damages from an attack through a third party. At least as much as for employee accounts, outside access should have stringent controls for credentials, account reclamation, and privilege. Two-factor authentication (page 45) is critical for outside access because it can mitigate the threat of poor credential management by an affiliate. All of the considerations for local accounts apply as well, including logoff after inactivity, only logging on to one role concurrently, and disallowing reuse of an identifier for a period to prevent replay attacks.

Similarly, remote sessions should be isolated and given the least needed privilege. Even if role-based, fine-grained access control is not implemented for employee accounts, for third-party accounts the accessible systems and data should constitute as narrow an attack surface as possible. Creating a standard for creating and managing remote accounts helps ensure this is done consistently.

Audits should be conducted to ensure need-to-know for the access that is granted. Penetration testing should be conducted to ensure the session controls actually enforce the intended access policy.

Web Encryption Technologies

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.REM.4	Web Encryption Awareness	Reduces frequency of compromised credentials and leakage of personal information; costs overlap with training for secure communication	All	Low	Medium	Low	Medium	Medium

Motivation

The internet is designed for simplicity in the core of the network. One outcome of this is that users on the edge of the internet have little control over where or through what networks their packets are routed. The result is that a surprising number of entities have access to web traffic originating at a given organization. Added to this, standard web technologies transmit data in a form readable by anyone. As a result, basic web technologies are adequate only when browsing public, non-modifiable web pages.

When communicating over the public internet, confidentiality can arise only from agreeing on some end-to-end encryption protocol. Two technologies are used to secure most of the sensitive traffic on the internet. It is therefore prudent that all employees receive training and become aware of both the capabilities of these technologies and the limitations of TLS/SSL and HTTPS.

This section and the 'Man in the Middle Attacks' section below serve largely as prerequisite material before the 'Cloud Security' section on page 82.

Prevention

TLS/SSL

Transport Layer Security (TLS) provides an encrypted tunnel between endpoints. TLS is perhaps less commonly known than its preceding standard, Secure Sockets Layer (SSL).

TLS makes use of prior knowledge of key certificates that are vetted inside browsers, email clients, etc. to negotiate the details of a secure connection between hosts. A key certificate contains the public key for some server. What is important here is that a public key and private key form an inversion pair, so that encryption by either inverts encryption by the other. Thereby, a public key can be used to verify that a party on the other end knows the corresponding private key.

A key certificate certifies that a public/private key pair is associated with some named entity. A key certificate is in turn signed by some other private key. Thereby a chain of certification is created that leads to a self-signed 'root certificate' associated with a Certificate Authority (CA). It is these root certificates that are built into a browser and that the browser ultimately uses to verify other certificates.

HTTPS

Often, TLS/SSL must be configured explicitly for secure email connections. However, the power of TLS is in its use to build higher-level protocols. Hypertext Transfer Protocol Secure (HTTPS) is built on top of TLS/SSL. For secure web browsing and ecommerce, HTTPS is the most common security method.

HTTPS is usually invoked automatically between the server and client browser when a secure area is reached. Therefore, the only concern for an end user is to be mindful of checking that HTTPS is activated before viewing or sending sensitive information across the internet. Most modern browsers provide some visual feedback when a secure connection has been established, often an icon or color inside the address bar. The address of a secure website also begins with *https://*.

Browsing Pitfalls

Unfortunately, there are pitfalls to encryption that can undermine its efficacy. Some of these are not within the control of a user. Poor web design can leak authentication information or cookies that allow a session to be hijacked. Other vulnerabilities can allow one site to be polluted by malicious content from another site. A web browser can attempt to mitigate some of these vulnerabilities, with mixed results.

Regardless, a user is always more secure when all sensitive information is encrypted. As discussed in the 'Phishing Websites' section on page 59, it can be difficult for a user to verify that web communication is actually encrypted, so some attention is needed. Many popular websites, including email and social media, are beginning to encrypt all traffic by default. Other sites still require a setting to be changed. It is a good idea to check the encryption setting for any websites that are used to access personal information.

Unfortunately, many websites continue irresponsible security practices, such as mixing secure and unsecure content, or unexpectedly switching back to HTTP after a HTTPS session has begun. For better security, some third-party applications can force all browser connections to use TLS/SSL.

Security Limitations of Encryption

One important point about public key certificates in general is that the weak link in the security chain is associating a name with an entity. The encryption used by the newest TLS standard can be considered impenetrable for the time being (see the 'Man in the Middle Attacks' section below for attacks on protocols). However, the semantic association of a name with an entity is much less clear-cut.

CAs vary in the depth of their vetting process, one telling case being a certificate for the name 'Microsoft' being issued to an individual not associated with Microsoft. Even for a legitimate webpage, the association between the certificate and the URL is often murky, with webpages often using a certificate issued to a person, or even a third-party hosting company.

A secure tunnel does not guarantee the entity on the other end can be trusted, only that the communication is private. Accordingly, HTTPS only verifies that the website on the other end holds a valid certificate, and that any data sent can be read only at the computers on either end.

This certificate could be stolen, issued to a malicious entity, or the otherwise legitimate website on the other end could be compromised.

Fundamentally, the mere presence of a valid certificate does not indicate that the certificate holder is not an adversary in the current context. Analogously, the 'secure' indicator within a browser does not vouch for the trustworthiness of a webpage. In light of malicious webpages with valid certificates and waterhole attacks that use legitimate webpages for indirect attacks, this semantic gap remains to be filled by a vigilant user.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.REM.5	Training - Awareness	Reduces frequency of compromised credentials and leakage of personal information; costs overlap with training for secure communication	All	Low	Medium	Low	Medium	Medium
PT.REM.6	Protocol Enforcement	Reduces attack vectors by forcing usage of newer protocols; reduces damages from network compromise	Admin.	High	Medium	Low	Medium	Low
PT.REM.7	Layered Encryption	Mitigates the threat of many attacks on encrypted connections; reduces risk associated with using cloud services	All	Medium	High	Medium	Low	Low

Motivation

Several attacks exist even on encrypted connections. To highlight the risk, some lower-level details of networks are described below.

The creation of functioning low-level routing protocols has required much research. In addition, most common protocols were created before the global internet was a reality. As a result, these low-level network protocols have no provision for authentication or other security. For example, several times a malfunctioning or malicious router has corrupted the routing tables used by the border gateway protocol (BGP) to route internetwork traffic on the internet. This has sometimes disrupted large regions of the global internet.

On local networks, routing makes use of address resolution protocol (ARP) to make routing decisions. ARP is used to resolve network-layer addresses, usually IP, to link-layer addresses, often Ethernet MAC. The first time a packet is sent to a network address, the link-layer address of the destination must be resolved by a switch broadcasting the destination and waiting for a reply from the destination. Once found, the address is cached so that future packets can be immediately directed to the appropriate link.

ARP can be hijacked by several methods. The usual goal is to associate a network address with a malicious host. By waiting for a resolution request, an adversary can reply from a different machine. The ARP protocol will also cache unsolicited replies. Operating systems attempt to secure ARP in different ways, but these efforts attempt to build castles on sand. ARP cache poisoning can be done with 100% rate of success.

Once associated with an address, all packets destined for that address will be sent to a malicious machine. By associating two target addresses with a malicious machine, an adversary inserts itself in the middle of any communications between those addresses. Once in the middle, many higher-level protocols can be attacked. A common tactic is to intercept traffic between a host and the external gateway. This way, every packet between this host and the internet will be intercepted.

One powerful attack is to act as a transparent proxy. A man in the middle (MIM) waits for a TLS connection to be attempted. Then separate TLS connections are created between the MIM and each endpoint. Each incoming packet is simply unencrypted and then re-encrypted before sending to the final destination. Tools like ettercap (http://ettercap.github.io/ettercap/) and

stunnel (https://www.stunnel.org/index.html) can do this automatically. sslstrip (http://www.thoughtcrime.org/software/sslstrip/) is a very popular tool to perform a similar attack that simply forces an unencrypted connection to the client.

Prevention

Several attacks are possible only on older versions of protocols, for example SSL version 2. This standard has been obsolete for nearly a decade, but lingers in networks for backward compatibility. By disabling fallback to older protocols, many attacks can be prevented. This should be done for an entire domain.

As discussed in the 'Web Encryption Technologies' section above, a certificate only demonstrates that the party on the other end owns a valid certificate. The transparent proxy attack works because the both endpoints accept a valid certificate for the wrong party. This is one of the more difficult vulnerabilities to address, because it takes advantage of an exploit in a very common activity, web browsing. The low base rate of attack means it is very hard to remain vigilant for a valid certificate for an unintended party. Web browser warnings are no help because the connection is secure. It is somewhat easier to protect against ssltrip, because the connection at the browser will not be secure.

Defense in depth is the best approach. If sensitive files need to be transferred, these should be encrypted before sending through a secure connection. That way, if the secure connection is compromised, another password will remain to be compromised to access the sensitive information.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.CLO.1	Provider Vetting	Necessary before a vendor can be trusted	Admin.	High	Medium	Low	High	Low
PT.CLO.2	Geolocation Guarantees	Necessary for government data	Admin.	Medium	High	Low	Low	Low
PT.CLO.3	Attestation Framework	Reduces dependence on vendor integrity; reduces costs of vendor monitoring	Admin.	Medium	High	Low	Medium	Low
PT.CLO.4	Appliance Auditing	Mitigates vulnerabilities in cloud instances; reduces damages from information leakage in the cloud	Admin.	High	Medium	Low	Medium	Medium
PT.CLO.5	Appliance Encryption	Mitigates threats to communication with the cloud; reduces damages from data loss in the cloud	Admin.	High	Medium	Low	Low	Low
PT.CLO.6	Uplink Auditing	Increases the hardness of communication with the cloud; reduces costs of developing ad-hoc departmental procedures for uplinks	Admin.	High	Medium	Medium	Medium	Low

Motivation

Many small and large companies are contemplating migration of their computing infrastructure from in-house datacenters to cloud services. This move is usually driven by economies of scale, lowered risk, or fast ramp-up time. Unfortunately, a recent survey by Voltage Security indicates that a majority of senior-level IT managers have halted at least one cloud project due to security concerns. There are four areas of concern when pushing data to the cloud.

- Uploading data to a computing service entails trusting the cloud provider to handle the data securely and with integrity.
- Cloud providers face more frequent attacks than enterprise datacenters, and sophisticated versions of the same network-based attacks.
- Public datacenters execute many jobs concurrently, from diverse and possibly mutually antagonistic organizations. Attacks between virtual machines that share physical hardware are a relatively new threat vector and the defenses are not as mature as for outward-facing network security.
- Interoperating with a cloud provider requires uplinking to the provider over the internet.

Prevention

Trust in the Cloud

Many concerns for security in the cloud surround the unknown: cloud service providers have yet to be vetted by the test of time for their security practices. For now, these concerns have not been borne out. The business model of a cloud provider is far more invested in information security than that of the typical small to medium businesses that are outsourcing infrastructure or services to the cloud. This motivation, together with economies of scale, means cloud datacenters afford fulltime security personnel and comparatively tight security controls.

The key to prudent use of the cloud is to minimize the unknown by asking questions. Minimally, a cloud provider should disclose reasonably detailed security plans. Perhaps principal among security practices are personnel, quality control, location, and certification.

- Privileged access to the cloud infrastructure should entail a vetting process. This applies to architects, administrators, programmers, and operators. Privileged credentials should be tightly controlled.
- Testing standards should be clear and comprehensive for the software and other components of the cloud infrastructure.
- Geolocation is important in two dimensions. Although one of the selling points for cloud services is that low-level details can be ignored, disaster recovery dictates that a cloud provider guarantee that data are replicated at two different facilities. For government information especially, nation of residence for these replications might be restricted.
- Lastly, a cloud provider should comply with any standards that are relevant to the application that is being run on the cloud, and the provider should allow third party auditing of this compliance.

Data Ownership and Confidentiality in the Cloud

The legality of data ownership in broad strokes is that the owner of the hardware on which the data are located owns the data. This is why companies can read employee email. This also means telecommunication companies, cloud providers and others who store customer-originated data are ultimately not liable to the customer for the use of that data. So, for example, this data can be disclosed in response to judicial or government inquiries without substantial threat of civil action against the provider.

Therefore, the onus for data confidentiality ultimately lies on the cloud customer. If confidentiality from the cloud provider is desired, then remote attestation is the best option. Remote attestation takes advantage of a trusted platform module. These modules work by recording system state in immutable form. This is done by measuring the software that is loaded. For demonstration, a small, read-only program can hash the firmware of a computer, and record the measurement. Only after is the firmware run. Likewise, the firmware can hash the bootloader, and only after run the bootloader. The chain can continue up to the hypervisor, and virtual machine image. A check can be done by a bootloader at the head of the image by transmitting a signed record of the machine measurement stack to the owner of the image, and the operating system and remainder of the virtual machine image decrypted only if the owner is satisfied with the state of the platform. Thereby hardware, software versions, time of day, etc. can be guaranteed before exposing data.

Attacks on Cloud Providers

The security of cloud providers against outward attacks tends to be better than the security of enterprise datacenters. Cloud providers tend to be subject to the same attacks as enterprise networks but at the same time to be better prepared, with the caveat that the attacks are sometimes more technically sophisticated and have a greater emphasis on web applications. In turn, cloud providers suffer a much less frequent incidence of spear phishing and sophisticated attacks on humans. This can be attributed to the layer of separation and anonymization between employees and the data processed at cloud datacenters.

One focal point for attacks on Cloud infrastructure is the management tools. Cloud management tends to be highly automated. This state arises because cloud platforms tend to have many operating system instances running. Short-lived jobs and variable load also mean provisioning must be done more aggressively than for dedicated servers. The effect on security is that relatively few administrative actions each affect a much larger number of instances. This makes each manual management operation more critical.

Little can be done to directly influence the security of a cloud provider. The key is to choose a vendor with effective and well-documented security practices.

Attacks between Cloud Clients

Cloud security is a hot topic for both researchers and security companies. The novel challenges of cloud computing revolve around collocated appliances, shared networks, and other 'inside attacks', in contrast to external attacks on cloud providers.

Cloud instances run as virtual appliances on virtual machine monitors (VMMs). Like operating systems, VMMs are designed to enforce protections for the resources used by client processes. VMMs themselves are smaller, less general, and more secure than general-purpose operating systems. Notably, a VMM does not run client software or third party modules and is much less extensible compared to an operating system.

Unfortunately, as with operating systems, effective security against actively malicious users has been given significant priority only recently in the timeline of the development of virtualization. Notably, the hardware and software often have gaping holes in security. As an example, direct memory access (DMA) has been the bane of VMM security since the introduction of DMA. Only recently has hardware added support for higher-level IOMMU interfaces that allow a VMM to mediate DMA and interrupt handlers for guest operating systems. These cautions apply to circumventing the protections provided by a VMM, not compromising the VMM itself.

Virtualization aside, many cloud instances can be compromised easily because the images that are uploaded to cloud providers contain obvious vulnerabilities; for example, SSH keys pairs are present. Gartner found that 60% of virtualized servers are more vulnerable than the servers they replaced due to unsecure deployment [10]. For appliances that will be run on a public cloud, security controls should be given the same scrutiny as for a server on a local network.

Additional considerations for virtualized appliances are similar to those for secure processes running on an operating system. Storage is always a vector for leakage, so any physical memory or local storage that is allocated for sensitive data should be shredded before the appliance exits. Encryption of data at rest remains important, as it is in any scenario where physical access to storage cannot be controlled.

Security of Uplinks

Unfortunately, the weak link in cloud services is often the uplink to the cloud platform. This uplink typically uses a web-based front end. The link itself is prone to ARP-cache poisoning and SSL-stripping vulnerabilities. In addition, compared to system-level daemons that have been patched to reasonable levels of dependability over two decades, web applications tend to be more vulnerable. SQL injection and scripting vulnerabilities have surpassed buffer overflows in popularity for direct frontal assault on a server.

A VPN link will be more secure, but is less common. Even with a secure link, any tunnel remains vulnerable to unsecure endpoints, and so the terminal machines that are used to access a cloud service remain a good entry point for hackers. Any data in the cloud that is accessed from a company can also be accessed by anyone who hacks that company. This means that outsourcing to the cloud cannot serve as a substitute for reasonable security in house.

Outlook for Cloud Security

The consequence of the current state of the art is that most organizations keep their most sensitive data in house, and this will likely continue in the near future. However, secure computing is slowly transitioning to the cloud. Cloud providers have begun to offer non-collocated hardware options for a premium charge over usual cloud processing. Even governments have begun to publish standards for processing sensitive information in the cloud, and some agencies have already made the move.

Mid-Tier Security Tips

Mid-Tier tips are targeted for larger organizations. Most deal with administrative and managerial functions that are not directly visible to end users or policies that will be deliberated by managers before being rolled out to the entire organization. The issues here are irrelevant if Small-Tier tips are not implemented; a travel laptop policy is difficult to justify if the office door is frequently left unlocked. Without deployment of these or similar policies, it is difficult to attain a high level of security, or to be able to receive high marks from a security audit.

Advanced Password Handling

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.PAS.5	Password Cracking	Reduces the instances of weak passwords; provides quantitative feedback of the value of security spending	All	Medium	Medium	Low	Low	Low
PT.PAS.6	Role-Based Accounts	Increase the security of sensitive operations and critical accounts; reduces the damages from a single compromised password	Admin.	High	Medium	Medium	Medium	Low

Motivation

Password databases follow a regular pattern: when cracking the database, the rate at which passwords are broken has two phases. First, the ration of cracked passwords to guesses is high, indicating that some of the passwords in the database are weak. Eventually, the rate of cracked passwords decreases and reaches a steady state, indicating that the bulk of passwords are reasonably strong.

Prudent password composition rules can decrease the long-term rate at which passwords are cracked. This is important in cases like customer databases, where each password might protect a financial account. However, the long-term rate becomes irrelevant for proprietary information, because typically a handful of passwords will suffice to access an organization's entire information store. In this case, a password file behaves something like a chain, and we must worry about weakest links.

Prevention

Run a password cracker

Password crackers are used to guess passwords. One of the first methods an adversary will use once inside a network will be to exfiltrate any password database and try to crack passwords. Because of this, access to networks tends to depend on 'weakest links' in a password file.

To prevent the weakest passwords, and thereby make the entire password file much more robust, a password cracker can be run on the organization's own password file. The 'worst' passwords will depend on what cracker is used: as new patterns are added to a cracker, new

passwords will be broken. When a password is broken it provides a good training opportunity and will motivate a better password next time.

Longitudinal studies of rates of password cracking within an organization also provide a rare quantitative measure of the efficacy of a security-training program.

Compartmentalize passwords

It is admittedly inconvenient for any employee to login multiple times to conduct their job. However, given the catastrophic mode of failure when an all-access password is compromised, it is prudent to adopt role-specific passwords as bulkheads for sensitive assets. An administrator can answer emails, etc. with a general password, but should have a role-specific account for configuring servers or classified networks, for example.

Internet Whitelisting

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.NET.1	Internet Whitelisting	Greatly restricts possible attack sources; reduces damages from infected machines	All	Medium	Medium	High	High	Medium
PT.NET.2	Automated Extensibility	Reduces employee resistance, increases conformance; reduces costs of lost productivity	All	High	Medium	Low	Medium	Low

Motivation

Many malicious websites operate on the internet. Some of these sites attempt to infiltrate a computer that visits that site. These sites are discussed in the 'Phishing Websites' section on page 59. Once infected, a computer can be used to infiltrate an organization, or the wider internet.

One of the common uses for an infected machine is to send phishing or spam email or exfiltration of passwords. Computers under the control of an adversary are known as bots. Bots take their orders from bot controllers. The important point here is that most malicious activity requires a command and control link with an external contact.

One promising approach to protecting an organization is to prevent communication with malicious addresses on the internet. Notably, preventing infection by malware is sufficiently difficult that restricting command and control to bot controllers is sometimes recommended by researchers as a more feasible defense.

The first approach to filtering the internet is usually to create a list of malicious addresses, and block all traffic to these addresses. This technique is called blacklisting, and is used frequently. Several communities maintain large blacklists.

Unfortunately, blacklisting is complicated by the sheer scale of the internet. Bot controllers change addresses frequently to evade blacklists. Most bot traffic is also between infected machines and potential victims, so most machines involved are owned by well-intentioned organizations. Blacklisting also works only for outbound traffic because source addresses can be spoofed.

Prevention

The opposite approach

Rather than maintaining a blacklist of blocked sites, it is also possible to maintain a whitelist of allowed websites. Whitelisting provides inherently tighter control than blacklisting because an address is blocked unless explicitly allowed.

In sheer numbers, whitelisting does a far better job of filtering the internet. A large blacklist might contain a million addresses. There are billions of websites on the internet, so blacklisting can block on the order of 0.1% of the internet and leaves the other 99.9% open. A large whitelist might contain ten thousand websites. Therefore, whitelisting allows on the order of 0.001% of the internet to get through.

Whitelisting is also very effective at stopping command and control. This is because only specific ports at specific hosts can be allowed. In this way, whitelisting rules are similar to firewall rules.

In practice, organizations see most attacks stop when internet whitelisting is implemented.

Hurdles to Implementing Whitelisting

The critical advantage of whitelisting is that even the largest whitelist will admit a minuscule fraction of the internet that is allowed by a blacklist. This categorically superior result should not be forfeited in an attempt to do slightly better.

The primary hurdle to implementing internet whitelisting is that employees hate it. In general, security hinders the job functions of employees. Whitelisting in particular takes something as ubiquitous, frequent and useful as visiting a website and makes it a matter for anxiety. Every link, every vendor or customer contact becomes a potential sticking point. Productivity decreases when workflow is interrupted every time, for instance, a buyer must visit the website of a new vendor. Because of potential backlash and lost productivity, the choice faced by most organizations is between a loosely managed whitelist and no whitelist.

The critical point to a successful whitelist then is to be liberal and responsive with the list. The list should be liberal because the instances of websites being blocked should become small over time. The whitelist must be extendable, and employees will have to be involved regularly in extending it, because enumerating the websites that will be visited is impossible: 'A-Z Electric' might occur to somebody, but certainly not all of the one-hundred competing vendors in the same region. The list should be responsive because once a website is blocked an employee should not have to lose time on a formal review or other painful procedure to extend the whitelist. If these properties are missing, worn-down buyers will simply cultivate fewer contacts, for instance.

The process can easily be automated, and should be. Even sending a message and waiting several minutes for a website to be added manually is asking a lot from employees and IT. Instead, an automated popup from a web proxy can ask an employee if the site should be trusted. If the employee agrees, the site should be optimistically un-choked. A permission-based system is reasonably secure because permissions can be revoked upon review. In fact, all requests can be automatically filtered through the blacklist that would be used by itself otherwise, guaranteeing tighter security than with the blacklist alone. Simply associating an employee with a request in a permanent record will also reduce the number of safe but frivolous websites that are requested.

Virtualized Browsing

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.NET.3	Virtualized Browsing	Best mitigation for browsing- and email-based threats; reduces costs for host security and IT monitoring within the protected zones	All	Medium	High	High	High	Medium

Motivation

From the discussion of phishing messages and malicious websites above, it becomes clear that training employees to guard against phishing and malicious websites is difficult and expensive. Even with extensive training, when the entire computer-using workforce is viewed laterally, and the operations of an organization are viewed over time, it is certain that internet-based attacks will compromise a host at some point.

Added to this, host-based security is ill fit to defend against spear phishing. A popular piece of malware will eventually enter virus definition databases. However, off-the-shelf programs allow known malware to be mutated and masked from virus detectors. For targeted, one-time spear phishing attacks, a 'custom' mutated virus is a feasible business model, and host security can be reliably evaded.

Given that prevention is so problematic, what is needed is a way to mitigate the damage due to a compromised host. This can be done by making the host temporary, so that compromised software and operating system simply disappear after a user closes their internet connection. Unfortunately, reimaging everyone's computer every day is prohibitively expensive. Users also do not like thin clients because they need to work offline, want to work faster than network storage usually allows, and resent not being able to customize their workflow. For engineers and developers these solutions are not feasible.

Prevention

Non-persistent virtualized browsing uses a fixed virtual machine image (VM) to browse the internet and read email. Direct access to the internet is blocked to all office computers. Instead, users must create a remote desktop connection or otherwise login to a remote machine. The internet can then be accessed from this machine.

The remote machine is actually one of possibly many VMs that are instantiated exclusively for internet access. The image can be tightly controlled for secure settings and run minimal software to make it hard to compromise. Because of the limited usage, these images can be made much harder than can a thin client. Access to and from the VM can also be tightly restricted, so that few entry and exit ports are allowed. Most importantly, the VMs are non-persistent, so that if a VM is compromised a clean image will be reloaded before another client logs in.

Setup effort can be substantial, as servers must be setup and cluster management is required to manage the pool of virtual machines. Virtualized browsing is also one of the most-hated security provisions, albeit less than thin clients. Nevertheless, virtualized browsing is one of the only effective measures for mitigating phishing and web browsing threats.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.DEV.1	Training - Awareness	Reduces probability of infiltration by removable media; reduces damages from infection possibly without prohibiting removable media	All	Medium	Medium	Low	Medium	Medium
PT.DEV.2	Media Tracking	Reduces information loss through removable media and insider threats; reduces damages due to inside threats	All	Medium	Medium	Medium	Medium	Medium
PT.DEV.3	Device Access Policy	Increases inspection and approval of personal devices; reduces damages from infection of internal networks	All	Medium	Medium	Medium	Medium	Medium
PT.DEV.4	Media Encryption	Reduces information loss by lost devices; reduces damages from travel incidents	All	High	Medium	Medium	Low	Medium
PT.DEV.5	Remote Sanitation	Reduces the scope for physical attacks on misplaced devices; reduces the risk associated with mobile device usage	All	Medium	High	Low	Low	Low
PT.DEV.6	Remote Work Policy	Reduces exposure to unsafe networks and vulnerability at remote endpoints; reduces damages from remote intrusion	All	Medium	Medium	Medium	Low	Medium

Motivation

Removable media constitute one of the most popular means for targeted attacks on otherwise secure organizations. Removable media is a potent delivery method because employees are inclined to explore an unfamiliar device more so than an unfamiliar program or even email.

Both removable media and personal devices are prone to loss in uncontrolled environments. Once a device has been outside the control of any trusted entity, it can be compromised and act on behalf of an adversary.

Personal computing devices present a threat to an information security because a high proportion of personal devices are managed with little regard for security, used by multiple persons, and exposed to high-risk public networks. Because personal computing devices store information and programs and have a high exposure to infection, all of the same motivations for quarantining lost devices apply to personal devices.

Certainly, policy for placing sensitive data on personal computers at home should mirror policy for personal devices at work. Home offices additionally suffer from unsecured networks and lacking security practices, so even when bringing work laptops home information is at increased risk.

Prevention

Lost and Found Devices

Awareness training is critical for guarding against compromised removable media. Minimally, most untrained employees will insert a found USB drive in their computer to investigate the content or owner. Insertion of a device can be enough to install malware. Aside from naïve

concern or curiosity, many attacks leverage greed for a free device or mischief by labeling a malicious file as something scandalous, like layoff plans, salary reports, etc.

The same security protocol applies to both found devices and recovered lost devices. Any device should be quarantined until completion of both an antivirus scan and inspection for new files. For this purpose, a lost device includes a computer, smart phone, USB drive or other storage device. To enforce this policy automatically, computers can be configured to require removable media to be wiped prior to connecting them to the information system.

Information Flow Control

Removable devices have the capacity to transfer information at the same rate as an open network. Removable media are also large enough to hold a backup of a large data store. Accordingly, the use and movement of removable media should be subject to the same typed of controls as network access and data backups. Only authorized users should have physical access to connect a device into a network. Location of a device, removal of a device from a facility or migration of a device to a new location should be documented. Checkout and check-in should occur whenever removable media are used within a controlled environment.

Personal Computers and Smart Phones

An employee is prone to perceive their personal device as both more indispensable and less of a threat than a recovered device. Therefore, employees resist restrictions on personal devices more than restrictions on removable media. Executives tend to be the easiest hacking targets within organizations in large part because they frequently violate policy for personal devices.

If personal devices are allowed, employees and contractors should sign agreements to comply with security policy and submit to virus and other scans while on the enterprise network before bringing a device on site. Access should always be restricted to known devices, that is devices that have been registered. Without this restriction, it is impossible to distinguish between an employee's device and an intruder's device. This will require employees to register replacement devices.

An important distinction is between connecting to the enterprise network and connecting to external networks. The enterprise network connection can be used to connect to external computers, for example social media sites. Because the organization has limited ability to configure personal devices, external connections can be used to circumvent many workplace usage policies. Devices can also be used by hackers to relay information from computers that are otherwise well isolated from external networks. If personal devices are allowed, it is more secure to restrict all connections from these devices to third-party networks.

Encryption

Because mobile devices are small and easily lost, they have greater potential to violate physical access controls than laptops. Typically, mandatory encryption for removable media is advisable if employees will transfer data to removable media before travel or will otherwise remove such media from the premises. Mandatory encryption can be enforced in Windows by setting domain policy.

In addition to whole-device encryption, sensitive information should be encrypted by file or directory so that only data that is actually opened is exposed if an adversary compromises the

device. This same consideration for encrypted containers applies to all computers (see 'Data Confidentiality' on page 130) but mobile platforms are more susceptible to infection. Many phones offer the ability to sanitize the drive of the device if it is lost or stolen. Remote sanitization should be enabled for all organizationally owned mobile devices.

Working Remotely

A policy not to allow work at home is the easiest to enforce and for employees to understand. A more lenient policy can specify at what sensitivity level information can be transferred to personal devices, if such a multilevel document management system exists.

Remote work also presents a backdoor to allow protected communication, VPN for example, to be intercepted at an unsecured endpoint. Therefore, any computer that is used to gain unrestricted access the company network remotely should adhere to the same security policy as employee workstations.

Travel and Laptops

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.DEV.7	Training - Awareness	Reduces infection on hostile networks and loss while traveling; reduces damages from travel incidents	All	High	Medium	Low	Medium	Medium
PT.DEV.8	Travel Laptops	Reduces exposure of information; reduces costs to prepare for travel	All	Medium	High	Medium	Medium	Low
PT.DEV.9	Pre-Travel Purge	Reduces exposure of information; reduces damages from information loss	All	Medium	Medium	Medium	Medium	Medium
PT.DEV.10	Pre-Travel Image	Facilitates forensic analysis of loss incident; allows accounting of damages from travel incidents	Admin.	Medium	High	Low	Low	Low

MOTIVATION

Travel represents an especially susceptible time for information security. Simple lost computers and documents are one cause. Theft is another common information leak. Hotel rooms of defense contractors are common targets for theft. Some regions of the globe are also known for high rates of computer hacking.

Travel is also a time when employees depend on unfamiliar environments to conduct their jobs. These environments are dangerous precisely because ubiquitous utilities and infrastructure are usually taken for granted, but can be malicious in an uncontrolled environment. Even a charging station can be malicious.

Prevention

Minimize Exposure

Everyday work computers become laden with company data over time. To limit exposure, the amount of data that is at risk should be minimized. Typically, information on past jobs and general office documents are not needed when traveling for a specific purpose. Consider using designated travel laptops to limit the amount of sensitive data needlessly taken off site. Before travel, only the information that is actually needed can be loaded onto the computer or other media. After travel, these machines can be reformatted to prevent spread of malware.

If employees travel with everyday laptops, a review should occur before departure and unnecessary and sensitive information removed. Imaging the hard drive of a laptop before travel both backs up all data and provides a record of what might be lost or leaked.

Malicious Networks

When traveling, the lack of internet connectivity can be a hindrance to productivity. Unfortunately, however inconvenient, it is unsafe to connect to any public network and there is a realistic expectation to be attacked on a public network at some point during a trip. Unsecured Wi-Fi is the most obvious target for snooping and hacking, but other networks are also vulnerable. A common tactic is to spoof a legitimate Wi-Fi network, so even secured Wi-Fi can be completely visible to hackers. Wired networks are also vulnerable. Many connections

share the same local network, and any user on that network can poison the routing so that all traffic can be intercepted.

Malicious Infrastructure

Many cell phones use their charging port as their data port. This opens the way for malicious charging stations that hack cellphones and tablets. These do exist in the wild, so cell phones and other electronics should not be charged on public charging stations.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.ROL.1	Minimized Shares	Reduces frequency of spillage, unauthenticated sessions; reduces damages from exfiltrated information	Admin.	Medium	Medium	Medium	Low	Low
PT.ROL.2	Information Demarcation	Increases security of the most sensitive information; decreases costs of handling bulk, non-sensitive data	All	Medium	Medium	Medium	High	Medium
PT.ROL.3	Role-Based Permissions	Mitigates vulnerability to multi-vector attacks and reduces risks from breach of a system; reduces damages following infiltration of a network	Admin.	Medium	Medium	Medium	Medium	Low
PT.ROL.4	Specialized Roles	Mitigates threats due to uncommon and high-risk usage; reduce risk associated with remote workers and managerial functions	All	Medium	Medium	Medium	Medium	Low
PT.ROL.5	Role Awareness	Reduces nonconformance by unqualified or naïve employees; reduces damages from employee negligence	All	Medium	Medium	Medium	Medium	Medium

Motivation

Centralized network storage is a powerful tool for both employees and adversaries. Beyond the basic protections for confidentiality and integrity, information should be compartmentalized to reduce the consequence of a single breach. Reducing impact begins by exposing only what must be exposed, minimizing access to need to know, and reducing the granularity of roles so that not everyone needs access to everything.

Segregating data by secrecy level is only one dimension of compartmentalization. Most information within an organization is of low sensitivity individually, yet a wholesale exfiltration of the company data store would constitute a roadmap to putting most companies out of business. Therefore, the mode of failure when a computer is breached should not be all-or-nothing. To this end, data should be treated at a smaller granularity, with access rights granted to each employee as needed.

Prevention

Minimize Shares

Shared folders and drives should expose only what needs to be shared. System files should never be shared, as this exposes things like password hashes. Therefore, sharing the root of a physical drive is a critical vulnerability.

Directories can be shared safely by any machine. The simplest form of share is configured locally, and authentication configured at the host that is sharing the resource. Network shares can also be mounted and shared across an entire domain, as with an intranet or transparent drive mount. However, allowing diverse machines to share directories invites access creep.

It is preferable for IT administrators to create network shares, so they can back up all shared folders centrally, set permissions, password policy, etc. Knowledgeable administration reduces

the frequency of occurrence of vulnerabilities like anonymous sessions. These network shares can be mounted locally if desired.

Demarcate Sensitive Information

Data compartmentalization begins with designating roles at an organization. The simplest example of compartmentalized access is a one-dimensional secrecy level. By segregating company data and enforcing tighter security restrictions on who can access the most sensitive data, and how this data is accessed, a physical and procedural barrier is created between different types of company data. This barrier protects data that are more sensitive.

Unfortunately, assignment of strict security restrictions to all information will likely backfire. The US security classification system provides a case study in over-classification. If a large proportion of the information that is generated is classified top-secret, many people will need top-secret clearance to perform their job duties. In the US today, five million people have top-secret clearance. It is predictably difficult for five million people to keep a secret. To prevent default, lazy over classification an easy step is to ensure that it is easier to label information as non-sensitive than to label it as sensitive.

Scarcity of resources also dictates limiting the amount of information that is labeled as secret. If a vast amount of information is labeled as highly secret, then a vast number of data accesses will need to be made to this data. As the number of such accesses increases, extensive security protocols, like the two-person rule, become prohibitively expensive. Therefore, the amount of sensitive information is a counter indication to the ability to afford secure procedures to access this information.

Likewise, overly restrictive or frivolous security controls on non-sensitive information will be undermined by impatient employees, and regardless of policy, lax handling will eventually be used for bulk non-sensitive information. These lax procedures and nonconformance tend to bleed into the handling of sensitive data that are not clearly demarcated.

Therefore, data of different sensitivity level should have different handling procedures, and be stored and handled separately. A simple example of this separation is storing sensitive data on a dedicated server that has no web access and limited user access. When a program needs information on this server, an additional authentication can be performed, using a password specific to this server.

The prerequisite to compartmentalization is proper labeling of data. Hard copies of sensitive documents are traditionally marked on a cover page. Marking must occur at creation, printing or copying, to ensure lapses of attention do not lead to unlabeled data. Electronic documents can be more difficult, as employees must remember to create documents with the appropriate labels and assign them the appropriate permissions or place them in the appropriate locations. Management of electronic permissions is much easier and more reliable whe using role-based account permissions, discussed next.

Enforce Explicit Roles

The scope for loss resulting from one compromised account should be minimized by compartmentalizing data access by role. Roles should be of small enough granularity so that the resulting permissions are more restrictive than simply requiring network access (i.e. the 'employee' role).

Create an explicit trust model: who is trusted with what information? In a company, employees must work together, so groups will be needed. Often, appropriate groups at a small to medium business follow departmental units such as sales, accounting and engineering. For example, an engineer account would typically require write access to engineering data. An accountant should have write access to accounting data. Neither group has a need to know in the complementary case. By compartmentalizing this information by limiting the permissions assigned to a single account, a security breach in one department does not compromise the other.

Most companies exhibit some degree of matrix structure. Without reflecting this matrix structure in role assignment, many employees in many departments will have to be given access to other departments. This can be avoided by assigning both departmental and project roles. Examples of appropriate granularity for most companies are 'Mechanical Engineering Department' and 'Project X'. Actually organizing directories and permissions to reflect a matrix structure will often require substantial work at a company that has had an entirely open file structure.

One person can wear several hats, and it is common for higher-level employees to need access to multiple roles. It is possible to implement multiple roles by assigning users to groups that grant the permissions of each role. However, when tighter security is prudent, authentication should not be bound to a person, but rather a person acting within a specific role. If an employee needs to fulfill several roles, that employee should be given role-specific accounts with different credentials for each. Therefore, an engineer who also shares IT duty should have two accounts. This does require logging in separately to access the privileges of different roles.

This distinction between role and person is critical for administrator accounts, as administrator accounts can change permissions and therefore cut across many domains. All office functions should be disabled for administrator accounts, to prevent laziness or oversight leading to the use of administrator accounts for risky activities like email or web browsing. Only administrators roles should have permission to access system files (passwords, etc.), even for local access.

Enforcing roles for employees can also prevent employees from inventing complex, novel security risks. Evaluating security protocol is intractable when multiple, concurrent attack vectors are allowed. Accordingly, employees should typically not be allowed to log in as multiple roles concurrently.

One caution about group roles is that regardless of the role, the identity of the individual should always be known. For example, remote sessions and processes running with permissions of a group must still be associated with a specific user so that attribution is possible. This is one additional advantage of per-role accounts, as every login is associated with a single individual and a single role and tracking is easier.

Specialized Roles

Roles also extend the capabilities of a security system to include temporary roles for highly sensitive tasks. The same principle of using a temporary role applies when an employee occasionally needs access not required to complete daily tasks. An account can be created then deleted once the task is complete. This has the additional advantage of not requiring long-term memorization of a seldom-used password.

One caveat is that temporary roles require reasonably well administered account management, or temporary accounts can exacerbate problems with rogue accounts. Every temporary account should have an assigned lifetime, and possibly a global maximum lifetime for all temporary accounts. Minimally, temporary accounts should be deleted automatically upon expiration of the lifetime.

Another type of specialized role is a remote session. A remote session occurs when someone logs into a computer over a network, but the distinction is critical when employees or affiliates log in from outside a facility. Remote sessions should always be treated with suspicion, and the permissions for remote sessions should be tighter than for the same role locally. Root or super user access should usually be disabled for offsite users.

Even for local accounts, it can be advantageous to limit privilege to specific circumstances. For example, administrator access that allows medication of an inventory database without using the frontend application can be limited to a period when inventory is being audited. A frequent example is weekday or business hour limitations. For example, a large payment would typically not be initiated overnight on a weekend.

Ensure Role Awareness

Employees are typically inclined to seek additional privilege. It is therefore important to ensure every role has a minimum training requirement to ensure employees understand the responsibilities of that role. This is especially true for privileged roles and administrator accounts.

Especially for executives, it is important to emphasize the business impact of security responsibilities. Busy managers are known to do things like hand out root encryption keys for financial institutions or delegate maintenance of sensitive computer systems to unsupervised contractors. When executives understand that the uninterrupted operation of core business functions depends on a relatively small set of hard requirements, the worst violations are less likely to occur.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.ROL.6	Centralized Management	Mitigates risks from lost or compromised accounts; reduces costs of account maintenance	All	High	Medium	Medium	Medium	Low
---	Employment Screening	See 'Social Engineering' section on page 52	Admin.	High	Medium	Low	Low	Medium
PT.ROL.7	Documented Roles	Reduces access creep for employees, reduces instances of security liability due to unqualified employees; reduces damages from insider information theft	Admin.	Medium	Medium	Medium	Medium	Medium
PT.ROL.8	Account Reclamation	Mitigates threats from former employees; reduces damages linked to disgruntled employees	Admin.	High	High	Low	Low	Low
PT.ROL.9	Training Controls	Increases employee awareness and qualifications; reduces administrative costs due to non-conformance	Admin.	Medium	High	Medium	Medium	Medium

Motivation

Much information theft is insider theft, either by current, outgoing or former employees. Account management is important because it is one of the best ways to mitigate the threats of insider theft and unintentional damage.

Every employee has inside access to company information. The default, naïve architecture for information systems provides every employee access to a great deal of information, possibly most of the information at an organization. A more robust and scrutinized architecture can prevent every employee from having access to so much information.

Broad access to company systems also makes theft by intruders easy. A single compromised password, attained either by cracking or by phishing an employee, provides access to all of the information that employee is authorized to access with that account. Eventually a password will be compromised, so the exposure from a single password compromise should be reduced.

Prevention

Documented Roles

All accounts should be documented, and the state known. The simplest case is two states (active and disabled), and rules (checklist) to transition between them. Minimally, on hire, an account should be created and added to the account tracking system (as simple as a spreadsheet), and a temporary password chosen.

Especially important is that a controlled procedure exists for termination of an employee. Termination procedures should include disabling of account access and cleansing computers of confidential or personally identifiable information. Access can be terminated by changing the password or deleting the account. Many attacks have been aided by former employees with active accounts that have been forgotten by an organization.

Centralized Account Management

All role privileges within a computing administrative domain should be granted and recorded by a central administration. The administration of accounts should be have provisions to respond in a timely manner to several types of event.

- Account recovery upon loss of credentials
- Account lockout upon detection of malicious or high-risk behavior
- Immediate access if needed by management in response to an emergency or investigation
- Automated detection and removal of inactive accounts

This can be done by a dedicated security department, but at most SMBs the owner or IT personnel handle role creation. The creation and deletion of role permissions for current employees is typically tightly integrated with account creation and deletion.

At small organizations, an owner or other single contact may handle all administration. At medium businesses, effective coordination between employees or departments can require some effort. Automated, reliable notification of change of status is needed for example when an employee is terminated to ensure timely change to access privilege. Even at small organizations, where account management is handled by one person, automated notification can help identify compromised administrator accounts. Change of status includes daily operations like creation and modification of accounts, so notifications should be sent for these events also. The form of notification can be email, phone, etc. but reliability dictates that the form of notification and protocol be standardized.

One nuanced point is that distributed computing systems rely on caching of data at local machines. In the context of accounts, this is how, after logging into a machine that is on a domain once, it is possible to log in to that same machine even if it is disconnected from the domain network. For related reasons, in limited cases, reliably removing the privileges of a group from one account can require invalidating the entire group and recreating the accounts that were not deleted. Some provision for recreating accounts should therefore be included.

Employment Lifecycle

As discussed in the context of social engineering, adversaries sometimes attempt to gain access by actually gaining employment at an organization. Minimally, all new hires should be subject to security screening.

Beyond this, current roles, actual responsibilities and need-to-know of every employee should be tracked and documented. Access privileges should be reviewed when changing roles. Holding security access for multiple roles is natural during transitions. However, access creep often leads to senior employees having unrestricted access to nearly the entire organization. This is contrary to both compartmentalizing information and least privilege.

Training Schedule

Security depends on every employee conforming to security policy, but security is usually auxiliary to a job function. It is therefore easy for employees to fall behind the needed security training for their roles. To avoid drop-off in conformance or an employee ‘falling through the

cracks', training should be standardized and documented. Documentation should include all training that is scheduled, received and required.

The minimal security training for all employees is a thorough review of the organization's security policies and culture at hire. This should be supplemented with yearly company-wide reviews to maintain security awareness and to roll out any policy changes. Talking points for initial training are discussed in the 'Employee Buy-In' section on page 35. Role-specific training requires per-employee records to implement consistently.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.CRT.1	Training - Awareness	Increases rate of reporting, reduces nonconformance; reduces training costs for specialized incident personnel	All	High	Medium	Low	Medium	Medium
PT.CRT.2	Incident Team	Mitigates damages from information incidents	Admin.	High	Medium	Low	Medium	Low
PT.CRT.3	Reporting Plan	Required in many industries, reduces delay to conform to contractual requirements	Admin.	Medium-High	Medium	Low	Medium	Low

Motivation

Inevitably, an incident will occur where information, a facility or computer system will be at risk. It is infeasible for every employee to be knowledgeable of how to handle such security incidents. It is then left to a small incident response team to possess detailed knowledge of how to handle an information incident.

Prevention

Incident Detection

It is unlikely that every incident will be detected by security personnel. Therefore, the bulk employee population must be trained in what constitutes an incident and how to report an incident. Data spillage occurs when classified or controlled documents are found on a computer or other container not permitted to contain that data. Employees should know a clear and simple course of action for how to handle a spillage. Employees should also be aware of specific actions to take if they detect a phishing attack, physical security breach, or other intrusion.

The best tool to minimize the impact of security incidents is to have a clear procedure to report and respond to incidents. Minimally, every employee should know to whom to report an incident. A timeline to report is also needed to avoid employees putting off reporting to avoid inconvenience. Failure to create simple and easy procedures and disseminate this information will lead to nonconformance and unreported incidents.

On discovery of data spillage, employees should be trained to leave any computer and data as found and immediately contact appropriate security personnel. This will facilitate the best assessment of the causes and risks associated with the spillage, and afford the best opportunity to contain any information leakage.

Intrusion is more difficult to handle, as a time component might be involved. Employees must still report first, and the incident response team itself must be responsive enough to mitigate ongoing intrusion.

First Response

An incident response team and first response procedure should both be in place. These assets can range from a single contact person and the policy to lockout an affected computer until it can be analyzed, at a very small company, to a team of dedicated security specialists at a larger company.

A response plan should include provisions for communication, coordination and reporting. In addition, the significant risk events that are identified during system inventory should each have a corresponding plan of action. This plan should be audited and possibly exercises conducted to ensure the plan is feasible and reasonably effective.

Reporting and Data Analysis

A written plan to report a security incident should be in place. This plan must encompass each category of sensitive information that is stored; credit card numbers, customer lists, and proprietary information are common examples. Common stakeholders include management and administrators within the company, customers, vendors and regulators. In some industries, clear regulatory or contractual obligations will exist for reporting incidents. The Department of Defense, specifically, has requirement for reporting any leakage or compromise of a sensitive system. Other industries, financial and health care, for example, have strict reporting requirements for leakage of sensitive customer information.

Accurate reporting and ensuing forensic investigations and audits require establishing beforehand what records will be retained. This information must be sufficient to establish the facts that will be needed. Specific details that might be recorded in logs include when an event occurred, what assets or people were involved at both the source and destination of any data transfer or malicious messages, and the impact of the event. Some types of event might require retaining the full content of communication or files so that impact or leakage can be assessed, for example.

For the sake of both auditing and continuous improvement, any detection events that were associated with the event and the responses of relevant personnel to the alerts should be recorded. Using recorded alerts and events, criteria can be developed for identifying and forecasting scenarios. As a simple example of a correlation rule, rapid increase in incoming traffic at two or more external gateways can trigger a DDoS scenario response. Once identification and forecasting rules are established, the response to the triggers falls within the more general response and continuity plan of the organization.

Experience from incidents is also useful for continuous improvement of the response team, so post-eradication activities should include analysis of root cause and development of new response strategies that can be presented during upcoming training. Traces and timelines of events provide concrete scenarios that can help focus training and contingency planning.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.RAC.1	Response Scripting	Reduces response time and increases effectiveness of responses to events; reduces damages from a wide range of events	Admin.	Medium	Medium	Medium	High	Medium
PT.RAC.2	Identify Dependence	Increases the effectiveness and completeness of response plans; reduces damages due to unforeseen consequences	Admin.	Medium	Medium	Medium	Medium	Medium
PT.RAC.3	Reliability Engineering	Decreases the rate of failure and increases the availability of systems; decrease total cost of startup and operation	Admin.	High	Medium	Low	Medium	Medium
PT.RAC.4	Practice Response	Increases efficacy of recovery efforts and decreases recovery time; increases return from all preparation spending	Admin.	Medium	Medium	Medium	Medium	Low

Motivation

When disruptive events occur, the effects can be far wider ranging than an initial impression would suggest. In terms of both business operations and bottom line, planning can reduce the impact of such events.

Prevention

Incident Scripting

“Plans are worthless, but planning is everything.” —Dwight D. Eisenhower

When disruptive events occur, plans always fail to account for the full range of situational specifics. However, an effective and timely response to a disruptive event is composed of a number of simpler action-reaction situations. It is in these moments that similarity and analogy to existing plans is invaluable. This is especially true of secondary- and higher-order effects of an action that might not be obvious if these actions have not been analyzed previously. By identifying interactions and consequences of actions, planning can eliminate many grossly poor decisions.

Therefore, it is wise to construct a set of scripted reactions to disruptive events. An example scenario could be an electrical outage. The steps could be 1) Call operations managers on cell phones 3) move employees to the west lawn 2) seal and rope off the chemical storage area 3) start backup generators 4) divert power and restart exhaust fans 3) call the electric company 4) manually override the front gate. Considering details and unlikely contingencies is also valuable because it is much easier to identify an action that is not relevant in a specific situation than to identify the omission of a necessary action.

Action plans need to be distributed to responsible parties, likely across administrative divisions. Audits of plans are necessary to capture new requirements and cull any points that become irrelevant. Auditing must also ensure that the resources listed exist in fact. Regularly scheduled reviews also preserve awareness throughout employee changeover.

Identify Dependencies

Incident action scripts can be tedious to create, in part because it can be mentally arduous to brainstorm contingencies and requirements. The tendency is to analyze events to the point of plausible rationalization that the resources allocated to creating a plan are sufficient. What is needed is a more focused, systematic way to explore an event.

The various factors affected by an event are related by dependencies. The dependencies between factors are an invaluable tool for expanding the scope of a plan to include every likely contingency. When dependencies have not been considered, many barriers to overcome will appear at critical times.

For an example of a dependency chain, the uptime of a server might dictate installing a backup server. A backup server requires a serviced and operational air conditioner. This might require installing an additional A/C unit or changing to a portable unit. A portable unit might require buying a pushcart and installing a ramp in place of a stair, having three employees ready to push, etc.

The levers that are available to a response team include activating emergency systems, disabling affected or at-risk systems, and communication and reporting. Proper ordering of dependencies is more critical when disabling systems. Bringing systems back online can also be troublesome if those systems have never been tested, a common example being restoring backups in the case of a loss event. Therefore, disabling actions bear second examination before finalizing contingency plans, and contingency planning should be incorporate lessons learned when debugging systems during commissioning.

The dependencies between factors should, as closely as possible, form a closed set. By following dependencies until a point is reached that the next factor is out of the control of the organization, or considered an acceptable risk, the effects of an incident can reach surprising breadth. Some organization use the dependencies that are identified to build failure trees to better visualize root cause analysis or contingency planning.

Reliability Engineering

Reliability engineering provides several principles that should be considered when provisioning for recovery and continuity. The cost of reliability increases rapidly as reliability approaches perfect, so minimum total cost will dictate nonzero downtime. One specific dimension is the tradeoff between redundancy and reliability; redundant components have an obvious cost.

There is also a tradeoff between inventory and peak capacity. Provisioning for quick recovery will often require coordinating with suppliers and service vendors to ensure they possess a needed capacity. Two common examples of vendor dependencies are extended service hours for IT vendors and availability of spare parts from suppliers. A vendor's capacity for rapid response can be supplemented with a local inventory of spare parts or IT systems. Both inventory and peak capacity can be expensive, so the optimal operating point is peculiar to the organization and system.

The reliability of individual components is not constant, and there is a tradeoff between maintenance cost and downtime. A classic example is servicing industrial machines, but IT systems are also subject to preventative maintenance, both planned software upgrades and

hardware replacement. Minimum cost will usually dictate some preventative maintenance and the optimal level of maintenance increases as the cost of unplanned downtime increase. Many hardware components can be monitored automatically and alerts generated; automated monitoring can be incorporated into automated maintenance scheduling.

Uncertainty remains the enemy of low-cost reliability, as maintenance becomes preemptive as uncertainty increases. In some cases, like high temperatures due to fan failure, imminent failure can be obvious, whereas in other cases, like a hard drive with bad sectors, time to failure can be quite variable. Redundancy interacts with component reliability here, as preemptive replacement can reduce the service intervals for hard drives to a minor fraction of the interval for reactive maintenance. Given the relatively low cost of hard drives and high cost of IT labor, modern systems typically find redundant storage to be more cost effective than preemptive maintenance of hard drives. For other components and uncertainty levels, the balance will favor preemptive maintenance.

Practice Response

Unfortunately, when a loss event occurs the first thing many companies discover is that the plans they have in place are not actually implemented fully. Backups are made, but the procedure for restoring might be complex and not understood. Systems can be architected for online operations but the first time something needs to be replaced administrators might find there is no way to take parts of the system offline without the entire system becoming unavailable. Likewise, emergency response teams can have scripted responses and even documented responsibilities, but when a loss event happens, the team can take inordinate amount of time to mitigate the situation.

The failure of contingency plans when they are needed is not surprising because many contingency plans are never tested. Similar to software programs, daily operations of a company, or any other process, the first day a contingency plan is brought online will witness bugs. The only way to avoid crippling problems when operations are already hindered is to test contingency plans at least once. Drills can be small-scale recreations of actual events, but are best performed at least as often as the changeover of people and assets.

In concrete terms, every level of backup should be brought online at least once. At least one production server in every farm should be taken offline and brought back online anytime the configuration of the farm changes significantly. This can be done during off-peak hours, or the repercussions could be as bad as if the outage were not planned.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.SRD.1	Security Roles	Reduces the number of open issues, reduces frequency of oversights; increases return on investment for security spending	Admin.	High	Medium	Medium	Medium	Low
PT.SRD.2	Security Role Training	Increases competence of the security team; reduces damages from all types of attack	Admin.	Medium	Medium	Low	Medium	Low
PT.SRD.3	Security Chiefs	Necessary for implementation of key handling and other high-level security controls	Admin.	High	Medium	Low	Low	Low

Motivation

Often when IT staff or other professionals share responsibility for security holes develop in the information system. This is in part because known issues or known best practices are neglected because no single employee has ownership of the task and so several employees have it 'on the back burner'. These known issues are frequently the first to come out when the organization is faced with an audit or penetration test. Other times a lack of demarcation leads to overlap and oversight. This can be as simple as assuming someone else has performed a weekly scan.

Prevention

Explicit Roles

Organizations without dedicated computer security staff should still have clear, distinct security roles, including clear ownership of every security task. Assignment of ownership encourages accountability and continuous improvement. Roles should be assigned as part of a larger formal documentation of company security practices.

Training requirements should be one component of this documentation, to avoid responsibility creep for people not sufficiently knowledgeable to handle their tasks. Training requirement includes initial training when assigned to a role, training for changes to role requirements, training for changes to information system, and periodic refresher training/

At small companies where professionals in other disciplines share responsibility for IT, an accurate inventory of IT skills can also motivate management to allocate training budget to security. Sources for security training are discussed in the 'Security Training' section on page 165.

Minimal set of Roles

Minimally, an organization should appoint a chief training officer to oversee the design and funding of the training program and to oversee the training, qualification and vetting of individuals who have a noteworthy role in securing the organization's information.

A chief privacy officer should also be appointed, to oversee the compartmentalization of data, documentation of handling procedures and controls, and vetting of IT vendors throughout the organization.

Minimally, two distinct individuals must hold substantial mandate within the organization for enforcing security concerns. These two individuals will jointly authorize the top-level secure operations for key management and encryption policies, discussed in the 'Data Controls' section on page 71. Dual authorization should also be required for deletion of offline backups, discussed in the 'Data Integrity' section on page 68, either to gain approval or to carry out the task. Drive sanitization can also require dual authorization.

Affiliates and Audits

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
PT.AFF.1	Vendor Lockdown	Extends security assurances transitively to information sent outside; reduces damages from intellectual property theft	Admin.	High	Medium	Medium	Medium	Low
PT.AFF.2	Vendor Audit	Reduces retreat of security practices among outside vendors; reasserts continued conformance with contractual obligations	Admin.	High	Medium	Low	Medium	Low

Motivation

Suppliers, contractors, field service and customers all receive sensitive information. Information security therefore depends transitively on the security practices of affiliates. Third parties have become a common attack vector as lower-security affiliates serve as backdoors into sensitive systems. As just one example, a breach of millions of credit card numbers in the payment system at Target stores originated with compromise of an HVAC vendor. Similar attack sceneries have been observed for payroll, accounting, inventory management and anyone with access to a network.

In the not-distant future, defense contracts will mandate minimum security practices for all suppliers. These requirements will be transitive and apply to subcontractors. Aerospace and other industries have discussed similar measures.

Prevention

Vendor Lockdown

All vendors should be subject to a security vetting process commensurate with the vetting process required by the customer to win the jobs that are eventually pieced out to these vendors. In addition to screening, all contracts should lockdown the required security practices of a vendor. One critical provision is that security requirements apply transitively to all subcontractors.

A tiered vendor structure is possible, where only more secure vendors can service more secure contracts. In addition, all vendors should be subject to a non-disclosure agreement. An example agreement is given in the 'Policy Templates' section on page 112.

Vendor Audit

Yearly briefings should be conducted for all contract employees, vendors, and business partners to reaffirm the security demands placed on anyone in possession of sensitive data. The right to audit the security practices of a supplier should be built into all contracts, and exercised during the fulfillment of the first contract. Further audits can follow as needed to ensure the level of security required.

*Remote Protocols

As with any connection, a remote session has the potential to be intercepted. In fact, the uplink is probably the weakest link in most cloud computing usage. Of course, as discussed in the 'Collaboration and Confidentiality' section on page 73, unsecure protocols like FTP and plain email should not be used to exchange sensitive information with a vendor. As discussed in the 'Man in the Middle Attacks' section on page 80, not all 'secure' connection are equally secure. Some protocols and cyphers have older versions that have been cracked. Others protocols were never really secure. Recent operating systems should be used when making to remote connections, and legacy protocols should not be re-enabled on these operating systems.

Likewise, the need to isolate and contain remote connections indicates that the Demilitarized Zone (DMZ) architecture that is discussed in the 'Secure Networks' section on page 148 should be used for remote login, if anywhere. This information is reiterated here because it is critical that third-party connections receive keen attention and strict controls.

Authorization for Staff-Owned Telephone with Camera

Approved authorization allows a staff member (a person possessing a valid, non-visitor identification badge) to bring his or her own personal cellular telephone or smart phone containing a functional camera into company facilities with the following critical restrictions and responsibilities:

- Personal cellular telephones are not permitted in closed or other areas posting this restriction.

As is the case regarding all personal belongings within company facilities, telephones are subject to random inspections and must be surrendered to the security staff pursuant to either an official investigation or random inspection.

Use of a telephone or any other personal electronic device for any recording—including audio, photography, or videography, within company facilities, or for company material inside or outside company facilities—is strictly prohibited. Any device suspected of making such a recording or connection to any company information system will be inspected and/or confiscated; media and/or memory components may be permanently retained. Involved person(s) will become the subject of an official investigation into the device's use, and will be subject to disciplinary action reported to the Defense Security Service (DSS), as well as possible suspension or termination of employment.

No cellular telephone or smart-phone, except Blackberries meeting company procedures and configuration, may be connected or synchronized with a company computer or the company network.

Cellular telephones, whether powered on or off, continue to be prohibited from classified meetings, secure video-teleconferences (VTC's), secure telephone calls and other classified communications.

Staff should make efforts to ensure all cellular telephones are kept a safe distance from these and similar discussions and communications involving company proprietary, export-controlled, or other sensitive but unclassified material.

Please also remember:

No other cameras or personal electronics with a camera are permitted within company facilities.

Camera-phones owned/leased by or issued to visitors are not permitted inside any company facility. They must be stored upon entering a company facility, and should be powered off before doing so.

Remain cognizant of the field of vision to which a camera's lens is exposed. Minimize the possibility that any image of classified, sensitive or proprietary material could be unintentionally or remotely captured by covering or blocking the lens via clothing (i.e. a pocket) or appropriate holster.

When signed and approved by the company Security Office, the authorized staff member agrees to adhere to all rules and penalties imposed for any violation involving his/her cellular telephone.

Email _____ Work# _____ Cell# _____

Phone Make/Model/Serial# _____

Name _____ Signature _____ DATE_____

FOR SECURITY AND ADMINISTRATOR USE ONLY

Security Approval _____ Disapproval _____ DATE_____

Information System Access Authorization and Briefing Form

I understand that as an Information Systems (IS) user, it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I have read or will read all portions of the System Security Plan (SSP) pertaining to my level of responsibilities and agree to the following:

Protect and safeguard information in accordance with the SSP.

Sign all logs, forms and receipts as required.

Obtain permission from the Information System Security Manager (ISSM) or designee prior to adding/removing/or modifying any system hardware or software.

Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to an IS.

Escort non-authorized personnel in such a manner as to prevent their access to data they are not entitled to view.

I will comply with the following password requirements:

a) I will select a password that is a minimum of 14 non-blank characters. The password I select will contain at least one number or punctuation symbol and a combination of upper and lower alpha characters.

b) Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.

c) If I have access to a Generic or Group account, I will first login with my personal user id prior to accessing the Generic/Group account.

Protect all media used on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.

Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.

I understand I must be authorized in writing by the ISSM to perform a Trusted Download. If authorized, I will perform this in accordance with the Trusted Downloading Procedures.

Notify the ISSM or designee when I no longer have a need to access the system (i.e.: transfer, termination, leave of absence or for any period of extended non-use).

Use the system for performing assigned company duties, never personal business.

Comply with all software copyright laws and licensing agreements.

I understand that all of my activities on the IS are subject to monitoring and/or audit.

Printed Name: _____ Phone: _____

Signature _____ Date _____

FOR SECURITY AND ADMINISTRATOR USE ONLY

☐ Employee ☐ Visitor / Company: _____ Visit request expires on:_____

Account Name: _____ Date Added: _____

Type of Account: ☐ General ☐ Privileged

Date Account Disabled / Deleted: _____

Authorization for Foreign Communication

To: Security Office, Company

From:

Date:

Regarding approval to (select one or more):

☐ FAX outside the U.S.

☐ PHONE outside the U.S.

☐ MAIL outside the U.S.

☐ SHIP (including FedEx, UPS, DHL, etc.) outside the U.S.

☐ EMAIL outside the U.S.

☐ OTHER _____

Name, address (including country), and contact information of person/entity outside the U.S.:

Justification for the foreign communication/contact/shipment:

Will you disclose any work information or material items outside the public domain i.e., any items that have not been cleared for Distribution A (unlimited distribution) and published in professional journals or presented at professional meetings? If so, explain.

Is the subject matter sensitive, proprietary, classified or export-controlled? If so, please detail and explain.

Will you provide technical specifications or applications from company work? If so, please detail and explain.

FOR SECURITY AND ADMINISTRATOR USE ONLY

☐ APPROVED ☐ REJECTED Date: _____

Signature of Facility Security Officer or Designate: _____

Visitor Log

VISITOR LOG, _____ BUILDING

Admitted by:	Visitor Name:	Citizenship(s):		Host Name:	Time In:	Visitor Badge #:
Date:	Organization:	Classified Visit?		Visit Purpose:	Time Out:	Badge Issued?: ☐
		Y	N			Badge Issued?: ☐
Admitted by:	Visitor Name:	Citizenship(s):		Host Name:	Time In:	Visitor Badge #:
Date:	Organization:	Classified Visit?		Visit Purpose:	Time Out:	Badge Issued?: ☐
		Y	N			Badge Issued?: ☐

Applied Research Laboratory
The Pennsylvania State University

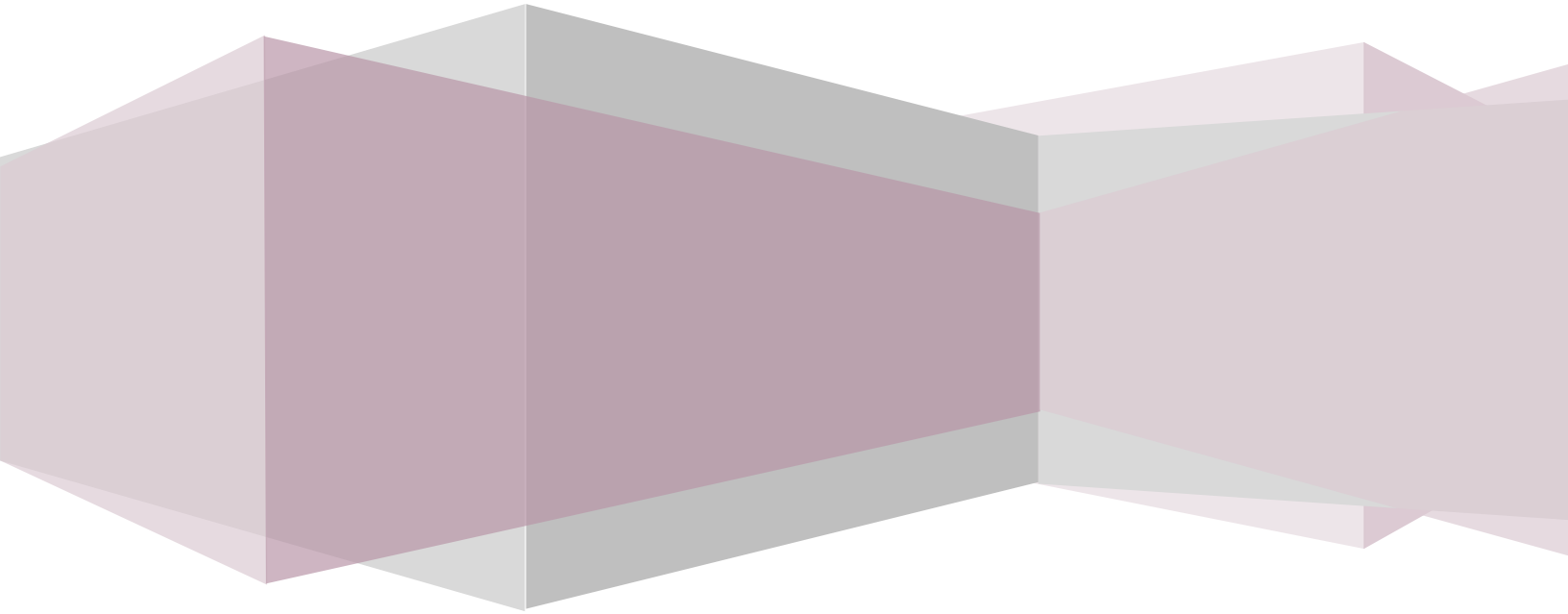
Understanding Security

Volume 3

TOOLS AND CONFIGURATIONS

For a Secure Computing Infrastructure

Brice A. Toth
Caleb J. Severn
Jonathan Hoerr



Small-Tier Security Tips

Small-Tier security tips are the easiest to implement and apply to nearly all organizations. In addition to minimal implementation and training costs, the vulnerabilities addressed are some of the first that are typically exploited when organizational assets are breached. Therefore, these tips can be thought of as the 'first line of defense' against a potential attack.

Device Commissioning

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.CSH.1	Infrastructure Password	Reduces unauthorized access by anonymous clients or by using default password; increases return on investment for intrusion detection	Admin.	High	High	Low	Low	Low
TC.CSH.2	SNMP Audit	Mitigates SNMP as an attack vector or minimally increases cost of malicious information gathering; increases return on investment for intrusion detection	Admin.	High	Medium	Low	Low	Low
TC.CSH.3	Minimal Embedded Servers	Mitigates unused services as attack vectors and vulnerabilities in embedded servers; reduces damages due to breaches	Admin.	High	Medium	Low	Low	Low
TC.CSH.4	Inventoried Ports	Increases efficacy of network scans; Reduces administrative costs for monitoring	Admin.	Medium	High	Low	Low	Low
TC.CSH.5	Disabled Legacy Services	Mitigates threat of eavesdropping; Reduces cost of password reset and damages due to spillage	Admin.	High	Medium	Low	Low	Low

Network infrastructure and embedded devices are the most frequent source of critical vulnerabilities at small companies. These devices can be small, hidden in dark corners and, when everything goes well, invisible. As a result, many of these devices are forgotten and evade IT oversight. Most security assessments at small companies find at least one critical vulnerability on a printer/scanner or consumer-grade router.

Unsecure infrastructure is often a beacon for opportunistic internet-facing attacks. Worse, many of these devices come with default settings and enable many 'features' that are critical vulnerabilities out of the box. Therefore, a secure network requires inspecting and configuring new devices before placing them on the network.

Device Configurations

Price: *Free*
Setup: *Easy*
Link: N/A

Infrastructure vulnerabilities are very common among small businesses with informal IT procedures. They key is to enforce a formal procedure for device commissioning so that nothing

is put on the network without thought. The process is similar to inspection and inventory controls for purchased materials, and is sometimes modeled after such controls.

A commissioning procedure should be supplemented with occasional vulnerability scanning to both detect undocumented inventory and identify vulnerable devices. Vulnerability scanning is discussed in the 'Penetration Testing' section on page 157. The following checks should be performed on every device.

- Web interfaces, embedded file servers, even administrator interfaces on consumer-grade infrastructure devices are often configured with anonymous access. Anonymous sessions allow anyone to enter a computer system without a password. Anonymous sessions are commonly found in file sharing and web administration applications for infrastructure devices. A strong password should be chosen that is unique to the device. This password will be seldom used and infrastructure is usually attacked first, so passwords for infrastructure should be stronger than for other accounts.
- Default (administrator) credentials are configured for many printers and routers. This is done to reduce support calls, but all default passwords must be changed to prevent trivial attacks on a network. Scanning for unsecure credentials on infrastructure is an automated and common attack on internet-exposed devices. Once inside, hackers will scan all devices. Default passwords are catalogued online by hackers (http://www.routerpasswords.com/).
- To minimize customer problems, device manufacturers often enable legacy protocols. Unfortunately, legacy protocols tend to be unsecure. SNMP is one common protocol for monitoring network infrastructure. Older versions check a 'community string' to authenticate access. This is a weak security protocol and made worse if default community strings are configured. In all cases, default community strings should be changed. From a security perspective, SNMP should be disabled if not needed. If SNMP is needed, only the latest version 3 should be enabled.
- Every service is an attack vector. To minimize attack vectors, the number of running services should be minimized. If a service is not used, this improvement comes at little cost. Printers and high-end consumer routers are notorious for having many services enabled by default. Most often, FTP and other services can be disabled. Web interfaces often cannot be disabled, but if a device is not accessed through the web interface, disabling the web interface is worth attempting.
- If auxiliary services on infrastructure devices are used, e.g. web interfaces and file sharing, it is preferable to migrate these services to accessible servers and disable the corresponding services on embedded devices. Printers and routers tend to use unpopular or even discontinued servers. These servers regularly have vulnerabilities and misconfigurations (FTP proxy connections, for example) that remain unpatched because 1) much infrastructure lacks auto update 2) firmware for embedded systems is infrequently updated by vendors. By running applications on dedicated servers or workstations the operating system and server are accessible, frequent patches are available, and both can be patched more readily.
- Any device should be subject to an inventory of all open ports. Even after disabling everything that can be found in a web interface, some surprising open ports can be found. Need or necessity for any active service should be documented, to make interpreting automated inventory scans easier.

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.WLK.1	Obsolete Machines	Mitigates the most frequently exploited vulnerabilities; reduces damages from network intrusion and reduces costs of administration	Admin.	High	Medium	Low	Medium	Low
TC.WLK.2	Obsolete Protocols	Reduces lingering vulnerabilities on largely updated networks; decreases damages from infection and reduces costs of administration	Admin.	High	Medium	Low	Medium	Low
TC.WLK.3	Rogue Machines	Eliminates the easiest targets on a network; Reduces damages due to physical infiltration	Admin.	High	Medium	Medium	Low	Low
TC.WLK.4	Temporary Setups	Eliminates the easiest targets on a network; forces a closed loop maintenance practice	Admin.	High	Medium	Medium	Medium	Low
TC.WLK.5	Isolated Development	Reduces the frequency of vulnerable testing systems appearing on visible networks; reduces costs of security administration and damages from buggy systems	Admin.	High	High	Medium	Low	Low
TC.WLK.6	Isolated Industrial Networks	Mitigates threats to the most vulnerable and critical systems; reduces losses from unreliable facility and manufacturing systems	Admin.	High	High	Low	Medium	Low

There are few clear victories in computer security. Luckily, software quality has improved over time and the days of throwing remote buffer overflows at network-facing daemons have largely past. As a demonstration, in the bad old days, most security patches addressed observed exploits; now, most exploits are generated from patch notes. Ultimately, this means zero-day vulnerabilities as a mainstay technique works as a business model only for advanced persistent threats (nation states).

Correspondingly, the nature of infiltrating networks has changed. Technical exploits remain, but application-level vulnerabilities have become more common. SQL injection has become the most common direct external exploit; cross-site scripting has also become popular. Attacks on employees, like spear phishing, have also become more advanced, see the 'Phishing Messages' section on page 55. When attacking from the network, hackers will usually recon the network looking for easy targets. These weak links are usually forthcoming unless an organization has invested in extensive audits or penetration testing. Below are some common findings.

Obsolete Computers

Price: *Varies*
Setup: *Easy*
Link: N/A

Most organizations have a standard for what operating systems and applications are installed. Unfortunately, the logistics of rolling out new versions and the cost of purchasing machines means that enterprise tends to be one or two versions behind the most recent. This leaves many enterprise networks vulnerable to off-the-shelf exploits like Metasploit, detailed below.

Most organizations also have known exceptions to IT standards. One common example is unique hardware, like a scanner, that supports only an obsolete version of Windows on the attached computer. A version of any operating system that is out of support will have known and unfixed vulnerabilities. Unfortunately, these vulnerable machines are usually connected to the network and configured to require domain login and thereby have access to the same network domains and credentials as conforming machines.

Obsolete Standards

Price: *Free*
Setup: *Moderate*
Link: N/A

An entire network will need to support weak standards and protocols for compatibility with a few obsolete machines. Well-known obsolete standards that have lingered on networks because of compatibility with old machines include LANMAN or NTLM authentication for Windows or SSL version 2.

If an organization cannot upgrade some decade-old hardware, then obsolete machines should be booted from frozen images and isolated from the network: there are no new updates coming anyway.

Other common vulnerabilities include use of legacy applications. RSH, Telnet and FTP are legacy applications that were originally developed for use when security was not prioritized. These applications send all data in plain text, including passwords during login. Even on local networks, administration and data transfer are vulnerable to snooping and should be done over encrypted connections. Telnet and RSH have been superseded by SSH, SCP and FTPS and others and should be replaced in all usage.

Rogue Computers

Price: *Varies*
Setup: *Moderate*
Link: N/A

In addition to vulnerabilities inherent in the activities of different business units, some machines on a network are exceptions to formal or intended security standards. Rogue machine is a common term for a machine that is an exception to security controls. Rogue machines are often not formally inventoried.

Some classes of rogue machine appear repeatedly. Shared computers or computers in public spaces are frequently given leeway for security. Common examples include a computer in a conference room, a training machine, or a guest kiosk. Personal devices and executive devices frequently evade enforcement. Development and IT departments also create many ‘temporary’ configurations. These setups outlive their intended lifetimes and are sometimes forgotten.

Other devices seem harmless or might not even appear to be computers. An isolated computer in an executive conference room that is used only for presentations will likely contain ‘temporary’ copies of PowerPoint presentations that contain sensitive information. Many offices now have web-enabled projectors, printers, and VOIP phones. These devices are often

built on top of full, general-purpose computers. Unfortunately, these devices are also frequently configured by their manufacturer to require no login. Similar to kiosks, these devices are often great entry points to begin an inside attack on a network. Vetting VOIP, printers and other devices can be difficult because security features are often omitted in product literature and almost never a selling point.

Among the first things that hackers look for, rogue machines are critical vulnerabilities. Worse, these hosts tend to be easy to find because of obvious host names such as 'conf3A' or 'hr_train'. Once found, these machines are often require no sign-in or use a well-known or guessable password. Once inside, these machines usually have network access and so make great bases to begin probing a network. Worse, despite a lack of authentication, these machines often have access to network drives that contain sensitive information.

Closely related are rogue wireless access points, discussed in the 'Wireless Networks' section on page 139. These are often observed in conference rooms, lobbies, obscure corners of a facility, and executive offices. Unsecured access points frequently connect to the network backbone.

All access to the organizational network should be restricted. If kiosks or other open machines are needed, these should use a dedicated network.

Temporary Configurations

Price: *Varies*
Setup: *Moderate*
Link: N/A

The above cases usually result because IT bends the rules for another department. Yet, IT itself often installs machines for maintenance or diagnostics that make easy entry points. Host names typically give these machines away. Often these machines are attached to a network during maintenance and left in place by busy or distracted administrators. In other cases, these are backdoors to make maintenance easier. All of the same security concerns carry over from above, with the addition that administrative credentials are frequently stored on these machines, for example SSH keys.

Closely related to this are weak passwords for network infrastructure. Routers, firewalls and other network infrastructure are too often left with default passwords. Ironically, network scanners and other security appliances tend to be some of the worst offenders.

Testing and Prototype systems

Price: *Varies*
Setup: *Moderate*
Link: N/A

Similar to IT maintenance setups, developers often create prototype or testing setups with the entire gamut of minimal authentication or empty root passwords, open ports, and loosely configured servers. This is done to ease transitional headaches and reduce iteration time.

Prototypes and work in progress configurations should be restricted to isolated networks whenever possible. In almost every case, a testing system does not need to be accessible by the

larger network, let alone the open internet. In most cases that a testing setup needs access to other machines, these can be replicated within a testing environment. Of course, actively malicious adversaries are only one motivation. Bugs in development systems are also a danger to network integrity.

One common driver for test systems appearing on production networks is the lack of a clear, defined release protocol. This can easily happen when 'hotfixes' and other urgent activities blur the distinction between testing and production. Development should always strive to enforce a formal rollout procedure, complete with safety controls and checks before any new system is taken online.

Industrial Systems

Price: *Varies*
Setup: *Moderate*
Link: N/A

There are factories around the globe where industrial controls are placed on shared subnets with office computers. This should never happen.

There has been a race between new, more secure designs and malware to reach the lowest levels of software. This trend is exemplified by BIOS-level rootkits and the threat of firmware-level rootkits. Industrial systems and network infrastructure are also increasingly targeted. Hacked internet backbone routers, and compromised weapons systems are just a few news stories to come from this.

One factor that makes industrial systems so vulnerable is that there was a longstanding conceptual separation between industrial controls and information systems. Industrial systems were seen as purpose-built and uniquely configured. So for example, a programmable logic controller (PLC) might support TCP/IP over Ethernet, but the network stack might not handle multiple TCP connections. This makes sense if the Ethernet is used as a dedicated point-to-point link. On a more complex network, and now under the purview of information security, a denial of service attack is trivial, as simply performing a port scan will crash the PLC.

Fragility is only one reason that industrial controls should always be on dedicated networks. These networks also often operate at higher loading than office networks. It is possible to find industrial applications configured on 10 mbps Ethernet with average load of 20% full bandwidth. Such a high loading is impossible for enterprise networks because usage peaks would drop throughput to nearly nothing. This loading is fine on dedicated and rigidly timed industrial networks that always operate at the average load. This thinking does not apply if the industrial network is connected to an enterprise network. Even if higher-bandwidth links are used, the bursty nature of enterprise traffic makes shared networks incongruent with low-latency, real-time controls.

A more fundamental problem is that industrial controls are simply designed without consideration for information security. The task of getting low-level communications going is eased by simplifying the network interfaces as far as possible. No authentication is done, and arbitrary data can be pumped into an interface so long as the frame format is correct. This lack of security typically also applies to the programming port, so anyone with physical access can

download or upload the PLC program. Industrial systems are also frequently one of a kind and custom-programmed on the spot, and so little sanitization of inputs or software testing is done.

If dataflow is needed from the machine level up to to the enterprise level, then control networks should be hidden behind DMZ networks, discussed in the 'Secure Networks' section on page 148.

Host Based Security

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.HST.1	Host Security Suite	Mitigates threats from most common malware and prevents most malware command connections; net cost savings compared to damages from infected machines	Admin.	Medium	Medium	Medium	Low	Medium
TC.HST.2	Intrusion Detection	Necessary to identify ongoing infection, slows infection progress; necessary for analysis of damages from infection	Admin.	Medium	Medium	Medium	Low	Medium
TC.HST.3	Automatic scanning	Maximizes probability of detecting malware before it embeds itself; maximizes return on investment for detection	Admin.	High	Medium	Low	Low	Low
TC.HST.4	Application Whitelisting	Mitigates threat due to abundant sources of executable files; reduces damages and administrative costs due to malware	Admin	High	High	High	Medium	Medium

Anti-virus software is probably the most widely known class of security software. These products scan a local host for known threats. Many of these tools also support email scanning. Free antivirus software is available, although these offerings are prone to change.

Several companies provide integrated security suites that can be installed on a host machine. These will often include antivirus, local intrusion detection, and some conformance monitoring to protect employees from malicious emails or websites. Advanced features can have a high performance overhead. We do not review common tools here, but instead simply list several of the best-known free offerings.

One caveat to host security is that ubiquitous antivirus and intrusion detection on Windows means most hackers and malware bypass such security as a matter of course. This is often done by testing to ensure that a piece of malware does not trigger common antivirus programs at the time it is released. Consequently, virus definitions should be updated frequently to catch newer threats.

Host security does make intrusion much more difficult, and without it, hackers can use fast, brazen tactics. This is one argument for Mac and Linux being easier to attack than Windows: many Mac/Linux users think they get a free pass on host security so hackers can spam them with attacks until one works.

Microsoft Security Essentials

Price: *Free (Windows only)*
Setup: *Easy*
Link: http://windows.microsoft.com/en-US/windows/security-essentials-download

Microsoft Security Essentials (MSE) is the baseline, minimum security software for the Windows operating system. It is not included in Windows by default but can be downloaded free. In addition to scanning the local file system, popular host security suites frequently plugin to email clients and web browsers to provide some boundary defense against email and internet attacks.

Most security suites bundle several services. Windows Defender is included in recent versions of Windows and provides host-based firewall and other services that complement MSE.

Unfortunately, traditional virus detection software has lost the battle against malware makers. The traditional method is to generate signatures for malware. Modern tools can rearrange binary executables using polymorphic and metamorphic transformations such that the function of the executable does not change, but the signature can be very different. These transformations are one-way, meaning that it is easy to create variants but very hard to discern if two programs are functionally equivalent.

To combat the failure of signature-based malware detection, modern malware detection uses indirect methods. These methods fall more under the purview of intrusion detection than antivirus. One method is to detect if some process is doing something it should not do, for example calling an operating system or virtual machine interface that it should not. Another method is to define invariants and detect if some state of the system violates rules for allowable states.

The most popular non-signature method takes advantage of the fact that malware serves some adversary. This adversary will eventually want to exfiltrate information or use an infected machine for some purpose. These actions require information exchange between the infected computer, sometimes called a 'bot', and the malware controller, or 'bot master'. These command and control exchanges require a connection to a server that is under control of the adversary. Worldwide efforts have culminated in a reputation system for domains and addresses on the internet. Once a server is identified as a bot master, any connection made to that server is an indicator that the machine making the connection is compromised.

OSSEC

Price: *Free*
Setup: *Easy*
Link: http://www.ossec.net/

OSSEC provides host-based intrusion detection. Host-based intrusion detection looks for artifacts like rootkits, phantom processes, and file modification. OSSEC will also analyze logs and detect configuration changes. As a file-monitoring tool, OSSEC also provides data integrity protection. With effort, hacker attacks can bypass host-based intrusion detection, but intrusion detection will dictate more time-consuming attack strategies.

Many of the indirect methods for detecting malware infection that are discussed above overlap with intrusion detection software. Some commercial suites bundle host based defenses and intrusion detection into one integrated product.

Scanning Configuration

Price: *Free*
Setup: *Easy*
Link: N/A

Host scans should be conducted at least once per week. Virus definitions should be updated prior to scanning. If signature files are used for integrity monitoring, these signatures should also be updated weekly. These settings should be enforced for an entire domain.

AppLocker

Price: *Free (existing Windows installation)*
Setup: *Moderate*
Link: N/A

The discussion of internet backlisting and whitelisting on page 88 covers the basic ideas of whitelisting including the motivations and pitfalls. The same principles apply to local execution. Most host security products include application blacklisting. A whitelist of programs that are allowed to run will vastly reduce the number of programs that threaten machines. Whitelisting uses signatures to approve programs, so protection extends to Trojan horses and modified programs.

AppLocker is free with Windows and can be configured from a domain controller. Modern Linux distributions include Integrity Measurement Architecture (IMA) and Linux Security Modules (LSM) that can be used to implement whitelisting, but there is no standard or easy way to configure whitelisting on Linux.

Secure Applications

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.APP.1	Secure Browser	Reduces the frequency of infection from websites; almost zero-cost mitigation for common vulnerabilities	All	High	Medium	Medium	Low	Low
TC.APP.2	Streamline Features	Mitigates the majority of vulnerabilities; reduces damages due to employee negligence	Admin.	High	Medium	Medium	Low	Low
TC.APP.3	Streamline Services	Mitigates vectors to access and move across a network; reduces early-stage damages from network infection	Admin.	High	Medium	Low	Low	Low
TC.APP.4	Disable Autoplay	Mitigates vulnerability due to removable media, especially for air-gapped networks; Reduces costs of awareness training	Admin.	High	Medium	Low	Low	Low

Most security breaches do not begin as technically sophisticated attacks—it is much easier to get an unwary employee to install malware by clicking on a link in an email or to give up their password through social engineering. While not security tools per-se, common applications are the most frequent vectors for attack. Securing the tools employees use every day is therefore a critical step to mitigating overall vulnerability.

Google Chrome

Price: *Free*
Setup: *Easy*
Link: https://www.google.com/chrome

Web browsers have been prone to many exploits. Newer browsers are increasingly built with security as a priority. Therefore, minimally, always run the newest version of Internet Explorer or Firefox. Better, in a browser security research paper released in December of 2011 [11], Google Chrome was found to have a superior implementation of 5 key security areas: Vulnerability patching, Safe Browsing API, Sandboxing, JIT Hardening, and Plug-In Architecture.

Disable Application Features

Price: *Free*
Setup: *Moderate*
Link: N/A

An exploit targets a specific vulnerability in software. Therefore, reducing the number of active applications, plugins, etc. reduces the number of vulnerabilities on a system. Even more, software at higher levels tends to have proportionally more bugs and vulnerabilities. Therefore, applications introduce more vulnerabilities than operating systems, plugins have more vulnerabilities than browsers, websites have more vulnerabilities than servers, etc.

Unfortunately, convenience and flexibility have always been prioritized over security. Therefore, the default settings for most applications have most features enabled by default, including rarely used features. Over time, this tendency has gotten slightly better. Notably,

several factors, including bad press about vulnerability, has forced web browsers to begin disabling by default many of the website features that were popular less than a decade ago.

One of the best ways to secure a computer remains disabling anything that is not used. In most cases, it is a minor inconvenience to disable even seldom-used features. For example, disabling all web browser plugins—except any auto-patch service—is a great way to improve browser performance, stability and security. If a specific, reputable website requires a plugin to view content, then this plugin can be enabled as needed. Other common applications to clean are Microsoft Office and PDF readers.

Disable Services

Price: *Free*
Setup: *Moderate*
Link: N/A

The arguments for disabling services on servers are largely the same as for applications. However, the information held by some network services can be more damaging to an entire network if the machine is compromised. Notably, intranet services are not needed for operation of externally visible servers. Internal network ports are common targets when servers are attacked. Two recurring attack vectors are NetBIOS and Server Message Block (SMB). When possible, these services should be disabled at all machines and blocked at firewalls.

NetBIOS is an outdated, inefficient protocol designed to provide name resolution and shared folders on non-routable LANs. NetBIOS is now routed over TCP/IP networks. DNS provides name resolution. Other protocols are better for file sharing. Therefore, NetBIOS should be disabled on all machines. One note is that NetBIOS was deprecated from Windows 2000 on, but is used by Windows Server 2003 to establish trust between forests. By default, neighborhood discovery is not done using NetBIOS from Windows 2000 on.

SMB provides folder and printer sharing. SMB is unnecessary, although disabling SMB can be inconvenient. SMB should always be disabled on gateways and externally visible servers. After disabling both NetBIOS and SMB, servers cannot be remotely managed in Active Directory's management console. Remote desktop can be used instead.

Disable Autoplay

Price: *Free*
Setup: *Moderate*
Link: N/A

There are cases where code is executed automatically, without approval or notification of the user. One of the important cases is autoplay in Windows. The default behavior is to run any autoplay code that is contained on removable media. This means that a malicious or infected device can infect any computer to which it is connected. This is one of the primary methods to attack air-gapped networks.

The easiest way to combat autoplay attacks is to disable autoplay. The presence of autoplay is evidenced by a popup asking what to do when removable media is inserted. When autoplay is

disabled, a device will simply be silently mounted and viewable like any other drive. Removable media restrictions are further discussed in the 'Virtualized Browsing' section on page 90.

Data Confidentiality

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.CAC.1	File Shredding	Reduces risks from residual copies on disk; increases residual value of electronics without increasing risk	All	Medium	High	Medium	Low	Medium
TC.CAC.2	File Encryption	Mitigates risk from of data at rest, necessary for effective segmentation of information; allows high-level control of risk	All	High	Medium	Medium	Medium	Medium
TC.CAC.3	Personal Information Scanning	Reduces the amount of personal data at risk; reduces cost relative to other controls for personally identifiable information	All	Medium	Medium	Medium	Low	Medium

Protecting sensitive information from disclosure requires handling the complete lifecycle of a file. Lifecycle considerations include whether or not a file needs to be reproduced, if a copy is still needed, and how to dispose of an unneeded copy. The tools here only aid in reducing the incidence of information leakage, but data confidentiality depends heavily on prudent data handling procedures.

Proper handling of confidential data begins with limiting reproduction. In the extreme, reproduction can be controlled, similar to control of hardcopies of classified documents. For most organizations, it is sufficient to remember more copies amounts to more chances to leak information. Consider a shared repository or database for commonly needed but confidential information, like client contact information.

File Shredder

Price: *Free*
Setup: *Easy*
Link: http://www.fileshredder.org/

Permanent storage on a computer can leak information long after a file has been forgotten or the computer decommissioned. Simply deleting a file only removes the location of that file from memory; deletion does not destroy data on the hard drive. This information can easily be recovered by an adversary with access to the hard drive. To limit the scope for forgotten and uncontrolled copies of sensitive data, this data should actually be destroyed if it is no longer needed.

A file shredding program will actually destroy information on disk. Shredding can be time consuming, so shredding should be used selectively on sensitive data. File Shredder offers a complete range of shredding options, from fastest to most unrecoverable. The methods range correspondingly from zero fill, to randomized fill, to multiple randomized overwrites. In Linux, $shred$ is a standard program for secure file deletion (http://www.linfo.org/shred.html).

File shredding programs can range in price based on their features. These features are usually interface conveniences, so from a security standpoint, free shredding programs will be sufficient for almost all organizations. If your organization has a need to worry about *very* sophisticated physical analysis of a disk, free shredding can be combined with physical access security while a

disk is in use and hard drive destruction after a drive is decommissioned to provide a nearly invulnerable data destruction solution. Hard drive destruction is discussed in the 'Hard Drive Destruction' section on page 152.

DBAN

Price: *Free*
Setup: *Easy*
Link: http://dban.org/

Darren's Boot and Nuke (DBAN) is a tool for whole-disk shredding. These tools are useful for cleaning a computer before it changes owners or users. These tools differ from file shredding applications in that the computer is booted into the disk shredding application. This allows the entire hard drive to be shredding, including protected partitions and boot sector. All data on a hard disk will be deleted, and the operating system must be reinstalled.

BitLocker

Price: *Free*
Setup: *Moderate*
Link: http://windows.microsoft.com/en-US/windows7/products/features/bitlocker

Login, authentication and session controls apply only to accessing a computer through software interfaces. Anyone with physical access to a hard drive can read the entire content. This can be especially important when computers are physically vulnerable as employees travel overseas.

Hard drive encryption ensures that the bits read from a hard drive do not divulge any sensitive information. All major operating systems allow for encrypting directories or entire hard drives. BitLocker is included in Windows, but must be downloaded separately. Linux also provides encryption, although there are many different options on different distributions. FileVault is available on Mac OS X.

Encryption can be used selectively on sensitive data because encryption does entail performance penalty as files must be decrypted with every access and encrypted with every modification. Encryption will also make legitimate data recovery difficult. A separate encrypted partition can be created for storage of all sensitive data. Many organizations use full disk encryption to avoid non-conformance by employees who would otherwise fail to encrypt sensitive files.

Unfortunately, disk encryption does not prevent all attacks. Notably, anyone who can subvert a computer can access an encrypted file while it is opened. For highly sensitive data, layered encryption can be used. Layered encryption places encrypted files inside encrypted partitions. Whole disk encryption casts a wide net to protect bulk data at rest. The individual encrypted directories or files ensure highly sensitive data are only exposed at a finer granularity to any adversary who is resident on a machine when that data is actually opened.

Memory vulnerabilities

Encryption is excellent for securing data at rest on hard drives, but does not eliminate the need for physical security for active computers. One caution about using encryption on a laptop, or any computer that enters a standby state, is that files are vulnerable while sleeping. When an

encrypted file is opened, it is transferred to RAM memory and unencrypted. To save power, the operating system may write the content of memory to the hard drive before entering a standby state. Then the content of memory is simply reloaded when the computer resumes. Therefore, any encrypted file that is open when a laptop saves its state will be stored on the hard drive in the clear. To protect sensitive data, all encrypted files should be closed before putting a computer to sleep. Some organizations disable sleep states entirely.

More generally, encryption keys are vulnerable when in memory. Unfortunately, an encryption key is in memory pretty much anytime encryption is being used. Any malicious device with direct memory access (DMA) can read the entire content of memory. Several tools are freely available to extract encryption keys through USB or FireWire ports. Ultimately, sensitive files should never be opened on an untrusted computer or when connected to an untrusted network.

Defeating cryptography

Often, encryption is treated as the end of the conversation about data confidentiality. However, data confidentiality depends on a complex chain of algorithms and procedures, and information is attacked at its most vulnerable moments. This means the mathematics of encryption is a small part of the bigger picture of information security. Usually, crypto systems fail because of protocol or human factors.

The first question to ask about a crypto system is where the keys are. Many encryption systems rely on a series of chicken and egg relationships. The key must be stored somewhere. If the key is encrypted with some other key, then this key must be stored somewhere. Ultimately, the final key must be stored in the clear or memorized by a human. If the key is ultimately derived from a passphrase, then all of the usual password attacks apply.

The second question to ask about a crypto system is when and where the data is unencrypted. Cryptography is irrelevant while information is in the clear—and all encrypted information will appear in the clear in some computer's memory. If it did not, the information could just be destroyed instead. This means the machines that are used to process sensitive information must be trusted. Unless the information was originally typed on the machine, and will never leave, the encrypted information reached the machine somehow, normally over a network or on a removable device. This means the sensitive machine is also accessible.

Cryptography is a powerful tool, but it is essential to remember that protecting sensitive data has no fixed or easy solutions. Security always depends on asking hard questions and adopting a whole-system perspective.

Identity Finder

Price: *less than $100/seat*
Setup: *Easy*
Link: http://www.identityfinder.com/

Identity Finder is a scanner for personally identifiable information (PII). PII is often targeted for information theft because it has high potential monetary value. Unfortunately, most identifiable information is stored as small files, and these often seem harmless individually. This complicates the task of tracking and protecting PII, and ensuring conformance to PII policies. PII

scanners run on host machines, search common locations for PII and report inventories. An organization should have a policy for scanning for personal information on all computer systems, in addition to handling of sensitive information.

Confidential Collaboration Tools

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.CAC.4	Virtual Networks	Mitigate vulnerability to eavesdropping on remote links; decreases risk due to remote work	All	High	Medium	Medium	Low	Low
TC.CAC.5	Encrypted Email	Reduces the frequency of sensitive information sent in the clear; reduces damages from leakage	All	Medium	Medium	Medium	Low	Low
TC.CAC.6	Secure Web Shares	Reduce the frequency of data exposure over email; can reduce cost compared to commercial VPN	All	Medium	Medium	Medium	Low	Low

Employees will inevitably need to share data remotely or with clients and vendors. Transfers of collaborative data constitute particularly vulnerable moments because information must breach organizational boundaries. Security tends to have corresponding gasps between both organizations and networks.

Employees are understandably inclined to transfer sensitive information using email and other common collaboration tools. Unfortunately, these tools are usually no more secure than talking in a public area. Emails are, by default, sent in plain text. This means that when an email is sent outside the local network anybody on the internet can intercept this email and look directly at the content.

Arrangements should be made to transfer sensitive information over secure channels so that it can cross physical networks securely and be integrated into the receiver's information management system when already on site. Encryption is available for email and attachments, but it is better to make a clear procedural distinction when transferring sensitive information by using task-specific tools.

VPN

Price: *Free*
Setup: *Moderate*
Link: http://openvpn.net/

A Virtual Private Network (VPN) allows secure browsing of a remote network. These tools extend a local network by binding two ends of a virtual connection with an encrypted tunnel. VPNs are easy to use because, once activated, a user can browse remote directories using either a web browser or the familiar file system interface of the local operating system. VPN products are numerous, and mature offerings are available free. OpenVPN is one of the best-known free software products. VPN hosting services can be purchased yearly for less than ten dollars per client.

VPNs come in two varieties, based on where in the protocol stack encryption occurs. SSL is the standard encryption protocol used for web commerce. SSL encrypts a data stream at the application level, and so vendors can have their own portable implementation. Because it operates above the network stack, a potential strength of SSL is that is can bridge protocols, although rarely is anything but TCP/IP used. In fact, one weakness of SSL-based VPN is that SSL

is strongly associated with web browsing. Many of the newer, one-click-install VPN services use SSL. These products can be very user-friendly, but many operate only over a web browser.

The other major VPN encryption scheme is IPSec. IPSec is more complex than SSL, but maybe more flexible. IPSec encrypts packets at the lower internet layer, and is actually part of the network stack inside the local operating system. Enterprise VPN services typically use IPSec. Many IPSec VPN services integrate with the local file system so that, once connected, a remote directory will appear within the local file system browser. While IPSec provides end-to-end security, one obscure weakness of IPSec is that, because it is implemented within the operating system, IPSec VPN cannot be used to tunnel through an untrusted operating system.

There is also PPTP-based VPN, although almost exclusively on Windows. PPTP is less secure than SSL or IPSec, but might be compatible with more systems.

One caution is that several popular VPN vendors supply a default configuration that trusts the local network, meaning a machine remains vulnerable to attackers on the same local network. This setup is called 'split tunnel' and nullifies much of the advantage of VPN on public wireless networks, for example. These tools often have a configuration to force all network applications to use the VPN tunnel.

S/MIME

Price: *Free*
Setup: *Easy*
Link: http://en.wikipedia.org/wiki/S/MIME

S/MIME is an extension for general-purpose encryption of email. Most modern email clients have S/MIME built in, and it will usually work seamlessly by requesting a password or key to open an encrypted email. Potentially, S/MIME constitutes a friendly, secure collaboration tool.

There are some limitations to S/MIME. S/MIME can complicate access to webmail, because ideally a secret key would not be transmitted to a webserver. In addition, some organizations do not allow encrypted email because an encrypted attachment is a common technique to bypass malware filters. An email that includes an encrypted file together with the encryption key is illogical and assuredly malware.

Secure Web Shares

Price: *Free (existing corporate site)*
Setup: *Moderate*
Link: N/A

Secure websites have become a viable alternative to direct communication. Businesses can create sites, upload data, and provide access to affiliates. Affiliates can then logon to the website and download the data. As always, passwords should be exchanged by other channels and remote sessions should be tightly constrained. Typically, the best setup is to create a site for a particular affiliate and a particular project. As with any remote collaboration with outside organizations, it is also a good idea to limit the scope of a credential to a particular purpose, so passwords should not be reused from unrelated projects, even if the companies and employees are the same.

One caveat is to ensure website shares enforce the same labeling and role permission requirements as local network folders. It can be an inconvenience, but limiting folder creation to administrators can limit the disorganization and unsecure permissions that arise when employees create their own shares.

Port and Address Blocking

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.FIR.1	Simplified Firewall	Reduces configuration errors and hardens firewall configuration, reduces administration effort; decreases damages from network intrusion	Admin.	High	High	Low	Low	Low
TC.FIR.2	Block IP Access	Restricts command and control to bot controllers, slows expansion of influence; reduces damages from exfiltration after compromise	Admin.	Medium	Medium	Low	Medium	Low

A Firewall is the principal protection for a network. Firewalls come in two flavors. Network firewalls are installed on routers and other network infrastructure and do most of the heavy work of filtering large numbers of packets. Network firewalls can range from built-in versions inside routers to dedicated enterprise firewalls. Host-based firewalls run on a local computer and can benefit from computer-specific policies. A host-based software firewall cannot prevent a large brute-force network attack like denial-of-service.

A firewall works by checking rules until the first match and dropping packets that violate the rules of the firewall. Firewalls today typically distinguish between application-level protocols, rather than simply port numbers. This is important because protocols, like SSH, can be run on any port, and blocking the SSH protocol, instead of the standard SSH port, will disable SSH regardless of port. A typical rule would be to allow web browsing from any machine on the network, or to drop all packets not explicitly allowed.

For larger companies, an experienced administrator will meticulously configure each firewall. A systematically configured network allows every network connection to be labeled with the protocols and ports allowed by the firewall.

Firewalls and other protection devices are frequently attacked. Usually protection devices run minimalistic software installations and are secure. However, like other infrastructure, firewalls are prone to missing patches. Another note about firewalls and protection devices is that they should fail safely. This means that an appliance should reduce function rather than reduce security. For example, a failed firewall should block all traffic, not let all traffic through. Almost all appliances are designed this way.

Firewall Rule Set

Price: *Varies*
Setup: *Moderate*
Link: N/A

We do not recommend specific firewalls here. For small companies, without hosting onsite, the following tips will form the basis of a minimal secure setup for an external gateway firewall (or router at the entrance to the internal network).

- Smaller is better for rule sets. Complex rule sets tend to have more errors.
- The last rule should be the ‘stealth rule’: deny everything not already allowed. Some routers already have ports closed by default.

- Deny by dropping packets. A reply message that a connection has been rejected or that a protocol failure has occurred provides information about the existence of hosts in the network. Replies also make scanning faster because when a packet is dropped the scanner must wait the maximum time between packets until protocol timeout.
- Disable Universal Plug and Play (UPnP). UPnP automatically creates a new firewall rule to allow the setup of a new connection. UPnP is entirely inappropriate in many scenarios and otherwise often poorly implemented and used by malware to bypass a firewall.
- Do not allow all outbound traffic. Infected internal machines can thereby communicate with bot controllers.
- Start with a minimal, restrictive configuration and add a rule if something stops working. A starting set of protocols to allow in an office setting: websites (HTTP, port 80); secure websites (HTTPS, port 443); incoming email (secure SMTP, port 465). To check external email, secure email (secure IMAP, ports 585&993).
- Reject all external access to the firewall and network. Hosting externally viewable webpages, or other services, is outside the scope of this document.

Force DNS lookup

Price: *Free*
Setup: *Moderate*
Link: N/A

Most malware avoids looking up hostnames by Domain Name System (DNS) for two reasons. First, bot networks want to avoid blacklisting, and so try to minimize footprint and overall visibility. Second, malware, and hackers in general, tend to use lower-level interfaces to search and communicate on a network. Typically, IP addresses are used instead of host names. Almost any legitimate outbound traffic uses DNS.

This distinguishing feature of hacking can be targeted by forcing DNS lookup. This can be done by disabling direct access by IP to external networks. To do this, a web proxy is required. This proxy simply refuses requests for IP addresses. Typically, a web proxy and web cache can be installed on the same machine to improve internet performance simultaneously.

Wireless Networks

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.WRL.1	Hardened Wi-Fi	Prevents many known attacks; reduces risk while maintaining Wi-Fi convenience	Admin.	High	High	Low	Low	Low
TC.WRL.2	Manual Wi-Fi Connections	Mitigate vulnerability due to host promiscuity; Reduces damages related to offsite work	All	High	Medium	Medium	Low	Low
TC.WRL.3	Access Point Scanning	Mitigates vulnerability due to wireless breaches and spoofed networks; reduces damages due to attacks on wireless networks	Admin.	High	Medium	Medium	Low	Low

Wireless networks are more vulnerable than wired networks for two reasons. First, the packets on a wireless network can be observed and manipulated without physical access and without violating any physical security controls, so wireless networks have fewer layers of security than wired networks. Because of this, wireless networks usually require authentication and include some form of encryption.

Second, wireless protocols must address limited visibility, interference and disconnection. Wireless network protocols are fundamentally vulnerable to denial of service attacks and other protocol manipulations. Collision avoidance is used, so denial of service is as simple as broadcasting constantly.

Connections can also manipulated to force hosts to disconnect by sending unsolicited protocol messages. This means a wireless host configured to auto-connect can be made to reconnect at will. Once disconnected, wireless clients are vulnerable to access point spoofing and other tricks. Understandably, secure areas often cannot allow wireless networks.

Even when wireless is deemed a prudent business tool, both faulty hardware and misconfigurations needlessly undermine wireless security. Below are some tips to help protect wireless hosts from the vulnerabilities of wireless networks.

Access Point Configuration

Price: *Free*
Setup: *Easy*
Link: N/A

Some things cannot be fixed by prudent configuration. Some inexpensive routers lack features. Other routers include protocol vulnerabilities or use outdated, vulnerable versions of software. However, many wireless networks are insecure due to configuration problems. Here is a list of critical features and setting that should be supported by almost any modern (2006 or newer) wireless router or access point:

- Secure the network with a strong password. Wi-Fi passwords should be stronger than normal passwords because brute force guessing can be used by any person within antenna range to break the password. Hackers use long-range antennas. This password will be cached by each host and will seldom need to be manually entered, so it does not need to be

easily memorized. Typically, a random password of at least twelve characters or phrase of a least six words should be used.

- Always change default passwords. Default passwords for routers are cataloged on the internet for both customer service and hackers. Scanning for default credentials is a simple and common attack coming from the internet.
- Change the SSID of all routers. The SSID is the name of the network that appears when searching for or connecting to a network. Encryption in WPA2 uses the SSID in calculations, so the default SSID should always be changed to something unique to avoid precomputation attacks.
- Wireless configurations are a jumble of acronyms, but all security options but WPA2 should be disabled. To maximize compatibility, most routers have multiple security protocols enabled by default, so this setting must be changed.

  The alternatives are poor. WEP is obsolete and can be broken by brute force in minutes. WPA was an interim solution until WPA2 became commercially available. Even with all optional features disabled, WPA by itself is vulnerable to brute force attacks. WPA can be broken by brute force in hours to days, depending on other settings.

  Almost all routers now support WPA2. If an older router (pre 2006) is in service and does not support WPA2, WPA (hours to days) is preferable to WEP (minutes). Strong consideration should be given to replacing any such device.

Here are some additional features that can be used to make a wireless network more secure.

- Disable wireless protected setup (WPS) on all access points. In isolation, WPA2 is reasonably secure. However, WPS contains protocol flaws that can be used to break WPA or WPA2 security in a matter of hours.
- Disable Quality of Service (QoS). QoS allows additional attacks on WPA-TKIP.
- Use WPA2-AES security. AES is a specific encryption method used within WPA. AES is immune to several attacks on WPA-TKIP, and the number of known attacks on TKIP increases with the combination of TKIP and QoS. AES is also needed to realize IEEE-802.11n high bitrate schemes. As of this writing, WPA2-AES cryptography is secure, but the tips for SSID naming and disabling QoS above should be heeded to avoid attack vectors against other aspects of the protocol.

  Some routers offer WPA2-AES+TKIP. This simply supports either AES or TKIP for backward compatibility with devices that do not support AES. Most operating systems will default to AES if supported, but forcing an obsolete but enabled protocol is a common hacker tactic. Pure AES should be used when possible.

- MAC filtering can be useful for management of enterprise networks. However, MAC filtering does not improve wireless security. This is ‘security by obscurity’ and creates a false sense of security. The MAC address is the link-layer address of a device. MAC addresses of devices on a wireless network are easy to find and clone.
- Do not hide the SSID of a network. Doing so disables advertisement of the network by the base station. This is ‘security by obscurity’ and introduces serious security vulnerabilities.

  First, hidden SSIDs are trivial to discover in minutes by listening for wireless packets. Someone must advertise the existence of a wireless network to make connecting possible.

Hiding the router SSID shifts the burden for advertising from the single base station to multiple low-power mobile hosts. Thus, the identity of the network is divulged as before and network performance is degraded.

In fact, a hidden SSID makes the existence of an access point known beyond the range of the access point. Because wireless clients are forced to query for an access point, mobile hosts will broadcast the SSID of a preferred 'hidden' network whenever they are searching for a base station. By force-disconnecting wireless devices and listening for the re-association broadcast, the identity of a 'hidden' access point that is preferred by a client can be discovered. This creates greater scope for spoofing attacks.

Auto-connect interacts with a hidden SSID and leads to vulnerable hosts. An adversary can listen for requests for hidden networks, and spoof a matching access point. Mobile hosts will happily connect to the hostile network in many cases. Even worse, after momentary disconnection from a 'hidden' network, some older laptop and mobile operating systems will preferentially connect to *any* Wi-Fi network that is advertising rather than a hidden network. Because wireless clients can be force-disconnected by an adversary at any time, employees can be left unknowingly connected to untrusted networks.

- Decreasing signal strength to obscure a wireless network is silly advice one can find on the internet. Wi-Fi hackers use powerful antennas that can interact with a network at far greater distance than can a standard built-in antenna.

Host Configuration

Price: *Free*
Setup: *Easy*
Link: N/A

From the discussion above, it is apparent that several host configurations are unsecure. These are summarized below.

- Auto-connect will frequently leave hosts connected to untrusted networks. This applies even in a trusted location because hosts can always be force-disconnected. Therefore, any computer connected to a wireless network can be forced to reconnect, possibly to a spoofed access point.

Access Point Scanning

Price: *Varies*
Setup: *Moderate*
Link: N/A

Unapproved wireless networks can be a more important vulnerability than slight configuration errors on known access points. There are two primary types of unapproved Wi-Fi network. Rogue Access Points (AP) are usually setup by well-meaning employees or even IT as a convenience when connecting to the internal network. These can be located in individual offices, conference rooms, or corners of a facility—often where there is not an Ethernet jack or where the official Wi-Fi signal is weak. Rogue APs are often not configured securely. Occasionally rogue Wi-Fi is used to breach a wired network, especially an air-gapped network.

The second common type is spoofed or adversary-controlled APs. These often spoof the SSID of a legitimate AP but require no authentication and connect to an external network. Spoofed networks are usually setup by third parties to attack an organization by capturing website credentials, stealing information or infecting hosts that connect.

APs can be identified by doing a Wi-Fi scan around a facility. This can be done by configuring existing APs to report other APs to a central location (they already listen for other APs) or by setting up dedicated sensors (e.g. Kismet drones). Enterprise APs will already have a method to report to a central controller. Laptops and other Wi-Fi devices can be configured to do the same thing. A single sensor can be walked around a facility to catch always-on networks, but breach networks are often turned on for a short interval.

For detection specifically of rogue networks, network scans (NMap) can identify common network infrastructure by looking for router login webpages on ports 80 or 443. A MAC address from a wired network appearing on Wi-Fi also indicates that the internal network has been exposed by an AP. Another method is to check wired infrastructure for bridge forwarding tables that contain MAC addresses that match any Organizationally Unique Identifier (OUI) of a manufacturer of wireless equipment. This latter method proves difficult in practice and does not work across internal routers because a router only forwards network-layer traffic.

An unapproved AP can be blocked in a number of ways. The most direct way to take advantage of the inherent weakness of Wi-Fi is to force dissociate every host from an AP by forging IEEE 802.11 protocol packets. Otherwise, the AP can be physically disabled after using network mapping software to triangulate the location of the AP. Rogue AP are easily disconnected at an upstream switch. Installing software to force hosts to connect only to approved APs can help, but has a high cost-benefit ratio if devices are used to travel or work remotely.

Disreputable Software

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.SFT.1	Free Apps	Eliminates a common vector for Trojan horses; reduces damages from compromised machines	Admin.	High	Medium	Medium	Medium	Low
TC.SFT.2	Pirated Content	Mitigates threats from malicious websites; reduces damages from host compromise	Admin.	High	Medium	Low	Low	Low

This section offers warnings about products, rather than recommendations. Many free applications are available; this document almost exclusively recommends free software. However, there is a sharp distinction between reputable open-source software and dubious offerings. Reputable free software is typically written and distributed by one of several identifiable groups: commercial contributors that benefit from amortizing effort to create open source software infrastructure, open source advocates, or hacker hobbyists. Disreputable software is usually distributed by groups that do minor modifications to existing software.

Many attack vectors on organizations and private individuals take advantage of mischievous behavior on the part of the victim. Typical behaviors are trying to illegally obtain software, or bypass content restrictions. The providers of software that aid in breaking the law should always be suspect. The basic principle of economics states that people respond to incentives. Turned around, this means no organization would incur the risk inherent in breaking the law without some gain. A warning signal should be triggered anytime a piece of software or media content is being distributed by a group that does not own the rights to that content.

Free Apps

Price: *Free*
Setup: *Easy*
Link: N/A

Distributors of unlocked, broken or otherwise pirated software usually incur the risk of doing so to reap the rewards of infecting their 'customers' with malware. The free programs that are distributed usually have added code that infects any computer on which the software runs. An otherwise desirable program that contains malware is called a Trojan horse. The most common sources of Trojan horses are unlocked or free versions of proprietary software. Common cases are operating systems, games and office software. Some sites simply post modified versions of free software to catch unwary users.

An infected computer is called a bot. Tens of thousands of bots can form a botnet. Botnets can make money for their controllers by sending spam email or by exfiltration of financial information, among other things.

The effects of software piracy on rates of malware infection are stark. In North America, where piracy is relatively uncommon, infection rates for computers are often estimated at 10-20%. In Eastern Europe and parts of Asia, where piracy is rampant, the infection rate sometimes exceeds 90%.

Free Content

Price: *Free*
Setup: *Easy*
Link: N/A

Often television and other content can be accessed on sites not affiliated with the owner of the broadcast. This is commonly done to bypass geographical restrictions. As with free apps, a warning should be signaled anytime an unaffiliated website is hosting restricted content.

These sites make use of malicious links, active controls, scripting and other techniques to infect computers that access those sites, see the 'Phishing Websites' section on page 59. A common tactic is to require download of a media player or plugin that is a Trojan horse.

Mid-Tier Security Tips

Mid-Tier tips are typically targeted for IT professionals. Most deal with IT functions that are not directly visible to users. Often the use of these tools requires expertise not possessed by all employees. Setup can also be extensive, sometimes requiring multiple machines or virtual machines to be deployed. These tools are also irrelevant if Small-Tier tips are not implemented; intrusion detection is pointless if employees are sending sensitive information through email.

However, without deployment of these or similar security tools, it is difficult to attain a high level of security, or to be able to pass a security audit. Most of the tools here are specialized, targeting a specific security task. For those unfamiliar with computer security, the ordering of tools here indirectly provides an outline of a procedure for penetration testing and system hardening.

Network Inventory

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.INV.1	Network Scanning	Reduces number of undocumented hosts and processes, prerequisite to other scanning; provides reportable security state	Admin.	Medium	Medium	Low	Low	Low
TC.INV.2	Automated Inventory	Aids enforcement of versioning and patching policies; reduces costs of domain administration	Admin.	Medium	Medium	Low	Low	Medium
TC.INV.3	Documented Networks	Reduces instances of unnecessary network exposure; reduces long term costs of administration	Admin.	Medium	Medium	Medium	Medium	Low

By default, networks become cluttered as things are added and removed. Keeping inventory is strained by several employees installing devices, and especially development or maintenance activities that reconfigure hosts rapidly and create “temporary” setups. Eventually, no one person can vouch for everything on the network. It is impossible to monitor a network effectively when it is impossible to say if a service or even a machine should be present.

All systems should be formally added into inventory before being placed on a production network. Inventory includes the host name, its address on the network, the ports on which it has services running and the machines and services it is permitted to access. Access can be specified by block or class of machine (e.g. accounting workstations).

This is especially critical in two cases. Development systems, like proprietary applications and new servers, should go through a formal release procedure before being placed on a production network. This is analogous to the commissioning control for new infrastructure and should include the same checks (weak passwords, unneeded services, etc.), but tends to be neglected more frequently because internal development is viewed as incremental compared to procurement.

A worse problem of 'incremental creep' applies to VM instances. Cloud instances and virtual machines in general tend to have significantly more vulnerabilities than traditional servers do because they bypass purchasing, inspection and other controls. Fewer layers of controls fosters the perception of new VMs as minor changes to the network when they are the equivalent of new infrastructure with regard to security.

To prevent network inventory from falling behind, an external 'audit' is useful as a check that device and feature creep do not set in. Together with a formal inventory, scanning and automated inventory provide a two-level defense against rogue machines and unmanaged attack vectors.

Nmap

Price: *Free (Commercial version available)*
Setup: *Easy*
Link: http://nmap.org/

Nmap is based on the simple idea to attempt to connect to every port at every address within a range and report all ports that are open. The feature set is richer than this—services, versions and even vulnerabilities can be reported—but the simple concept of script to inventory all open ports on a network is the foundation of network visibility. Some inventory tools integrate Nmap into consoles or web interfaces. However, Nmap is the de facto standard exchange format for network scans and many security assessment services will ask for a comprehensive Nmap scan or generate one themselves on the first day.

OCS Inventory NG

Price: *Free*
Setup: *Moderate*
Link: http://www.ocsinventory-ng.org/en/

One of the first and most critical steps to securing an organization's information is to inventory what actually needs to be protected and monitored. There is little substitute for manual inventory of intellectual property and other sensitive data, but products do exist to automate the inventory of computer assets. The core function of an IT asset manager is to scan hosts on the network and report inventories of all installed software. Such products typically involve two components, a central server to collect and manage client data, and client agents to scan local hosts.

A network inventory monitor or IT asset management system can inventory not just machines attached to the domain, but also search for rogue machines. Among several popular options, OCS NG is a free and open source choice. Commercial products also offer conformity monitoring, to push software installs and updates around a network.

One obstacle when maintaining inventory is to avoid redundancy and complexity. If inventory is distributed across multiple documents or programs, assets records will tend to become redundant or missing. If the procedures for updating inventory become byzantine or time consuming, current administrators will tend to fall behind and new administrators will make mistakes or neglect the system.

Network Map

Price: *Free*
Setup: *Moderate*
Link: N/A

Inventory is the first step in minimizing the vulnerability surface of a network by allowing a port to remain open only if there is documented need. Once inventory is known, this information should be summarized to both document the inventory, make it more understandable and represent it in a manner that allows analysis. Documenting the architecture of a network is critical to allowing formal review and preventing feature creep. Over time, more holes tend to be poked in the firewalls, and unsecure machines connected to the network.

A network map is a diagram showing every open port on every machine, and the ports open on firewalls between each group of machines. A regular inventory or map of network ports should be incorporated into a security control. A port connection diagram is shown in the context of secure network architecture in the 'Secure Networks' section below.

Secure Networks

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.INV.4	Secure Networks	Hardens an entire network, protects the most sensitive systems; Reduces damages from exfiltration of sensitive information, reduces of costs of domain administration	Admin.	Medium	High	Medium	Medium	Low

Proper network architecture is the foundation of a secure network. To minimize vulnerability surface, when malicious actors scan the internet, they should see only what must be visible. The same is true of any machine internal to the network, and as a general security practice, minimizing visibility slows information gathering by a compromised machine and forces wider scans that can be detected more easily.

When partitioning machines into segments, dissimilar vulnerabilities should be isolated to reduce attack vectors.

- Office machines suffer promiscuous behavior (email and internet) due to naïve or mischievous employees. The result is a high infection rate by malware and frequent data spillage.
- Production servers are usually the most secure machines, because they have less software installed, serve a dedicated function, and are the most closely inventoried and managed hosts on a network. However, servers are also the most exposed to attack because they must be visible to other segments, sometimes the public internet.
- Many security controls are heavyweight when development configurations change rapidly, so development machines predictably violate security controls. This leaves development machines with unsecure configurations and undocumented inventory. This creates vulnerability to simple attacks.
- Industrial controls are similar to development machines in that they contain many vulnerabilities. Few industrial systems are patched. Many control devices and control networks are not designed to interoperate with office traffic.

Much of secure network architecture aims at isolating these four types of machine into dedicated segments to protect each from the weaknesses of the others. Access to every subnet is enforced using firewalls. Ideally, the network map will be minimized, so that only specific machines in each segment access specific machines and ports in other segments. For example, rarely do many machines have need to connect to and configure external servers. Any development segments, defined as rapidly changing and not inventoried, should always be isolated and visible from a minimal number of developer machines. For optimal security, logical network segments should also be on different subnets. Isolation can be as simple as creating a separate Virtual Local Access Networks (VLANs) using a single managed switch. It is more secure to have two firewalls and a demilitarized zone (DMZ) between segments.

A securely designed network will allow administrators to understand traffic patterns quickly. When an event is detected, sparsely connected networks also facilitate disconnection of subnets for maintenance or protection while minimally disrupting other network segments.

Some basic architectural patterns for dividing networks are presented below. These templates tend to be repeated as the building blocks of a larger network. The workflow for tracking and documenting open ports is also shown.

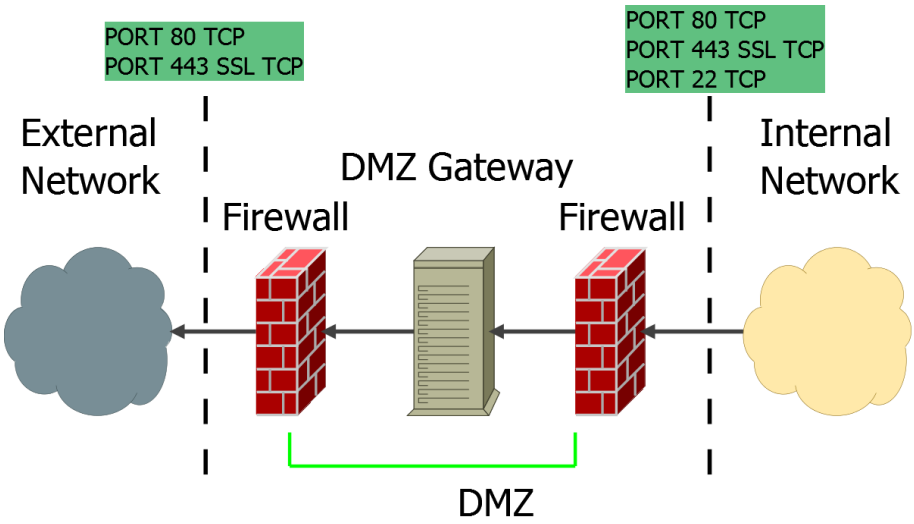
DMZ

Price: Less than $2000 (gateway and consumer firewalls)
Setup: *Moderate*
Link: N/A

The basic building block of a secure network is a demilitarized zone (DMZ). A basic DMZ is shown below. Enterprise firewalls can increase hardware cost substantially.

The idea of a DMZ is to have an isolated computer that mediates all external access. This mediation is enforced by restricting all connections across the DMZ. All inbound connections from the external network must go to the DMZ gateway. All outbound connections from the internal network must also go to the DMZ gateway. Connections are restricted by adding firewalls to both sides of the DMZ gateway.

Security is enhanced because both the view on the internal network is severely restricted and because the DMZ gateway is a secure machine. Because all external connections are to the gateway, it is much more difficult to determine the machines or network architecture on the internal network. The gateway must be compromised to gain unauthorized access to the internal network, even to perform basic scanning and enumeration of machines.



Some points about the DMZ gateway are critical.

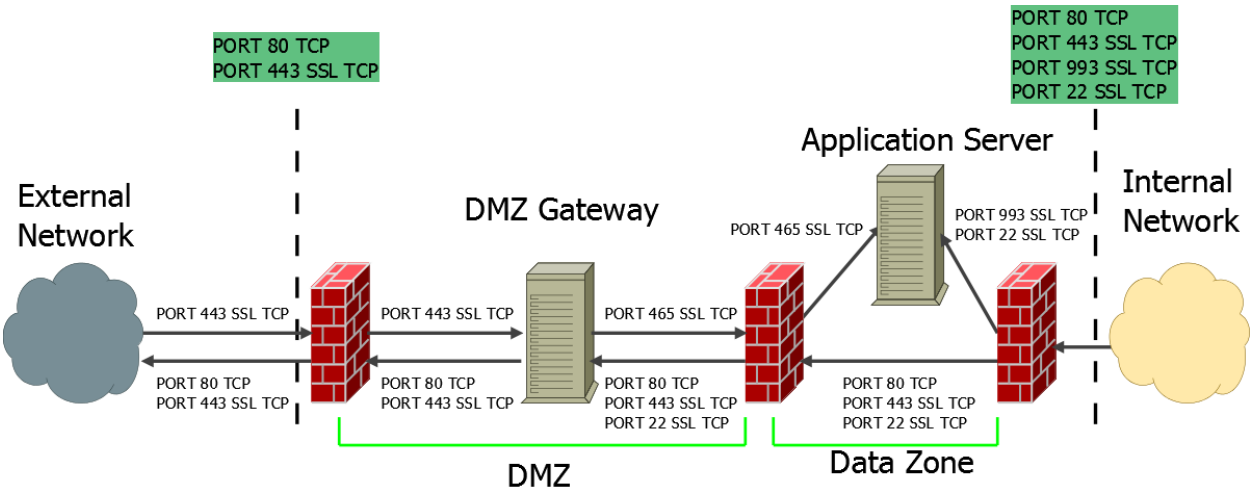
- The DMZ is on an isolated network. This means that IP addresses in the DMZ are on a different subnet than the internal network. The internal firewall must know how to reach the DMZ and network address translation (NAT) is needed to access the DMZ.
- The DMZ gateway has the bare minimum of services running. This is a general rule for secure systems because every service is another vector for attack. Services should also run at the lowest possible privilege. In addition to the firewalls, the gateway should have all ports blocked except those required to be open.

- No data are stored on the gateway. This way, if compromised, an adversary can plunder very little that is helpful for pivoting and expanding influence on the internal network.
- If authentication must be performed in the DMZ, strong passwords should be used so that even if a password hash is plundered it is impossible to crack.
- Encrypted packets pass through the gateway.
- Small, highly secure networks usually allow only outbound connections.

For larger networks, the DMZ might comprise several servers and allow inbound connections. A secure hosting architecture is shown below. Here, an externally visible server is hosting webmail. In this example, the external network can access secure webmail over HTTPS on port 443. The internal network can access external webpages on ports 80 and 443. The internal network can also SSH into both servers on port 22 and access IMAP email on port 993.

As shown here, the DMZ gateway is often an HTTP or HTTPS server. A single server should not host both HTTP and HTTPS. A second protection zone is demarcated to host the web application. This arrangement of separating webhosting from databases or web applications is standard for secure hosting.

Also notable is that encrypted connections are used between servers. Encryption should be used between email servers, database servers, and for any connections that transmit sensitive data. When in doubt, all connections should be encrypted.



The hosting architecture above shows a full port connection diagram. Every open port is shown on every connection. Connections are also directional. This way, exactly the needed ports from each source to each destination can be opened, and everything else blocked. Green boxes are included to emphasize the ports that are open at critical firewall interfaces.

Industrial systems especially are unfit for integration into the enterprise network, so should never be directly visible from outside their dedicated segment. Bursty office traffic can interfere with the reliable schedule of industrial networks, and simple port scanning can crash older industrial controllers. Unfortunately, the drive for increased process visibility sometimes leads industrial systems to be plugged into an enterprise network without proper isolation. A local

machine in a SCADA room can act as a DMZ gateway, and real-time data can be relayed through it.

The most difficult isolation to implement is for development segments. Developers and administrators must login to machines frequently, and the addresses of machines change frequently. Logging in to a DMZ to relay to a development machines introduces a 'remote session within a remote session' into the workflow for accessing development machines and inherently disrupts developer workflow. If employee resistance is too great, it is better to loosen the rules than to abandon isolation. Rather than specific ports and addresses, liberal firewall rules can allow specific addresses in an office segment to create remote sessions on a small block of addresses in a development segment, but then departments engaged in development should be on dedicated segments themselves.

Hard Drive Destruction

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.HDD.1	Drive Destruction	Mitigates loss vectors through used electronics; increases residual value of electronics without increased risk	Admin.	Medium	High	Low	Medium	Low
TC.HDD.2	Drive Degaussing	Required destruction method for defense contractors	Admin.	Medium-High	High	Low	Medium	Low

Many devices are available for on-site destruction of hard disks. HDD destruction services are also available, although a vendor for this sensitive operation should be subject to an extensive vetting process.

The National Security Agency (NSA) standard for hard disk destruction will satisfy all US Department of Defense regulations for destruction of classified material. It should be noted that the NSA standard is limited to degaussing of magnetic media to remove information therein. An NSA-approved degausser can be several times as expensive as a commercial model, so both are included below for reference.

Physical destruction of a hard drive is a NSA-recommended security control that aids in physically distinguishing a decommissioned hard drive. A center punch, bend, crush or other obvious, disabling damage is sufficient for this purpose. It should be noted that a degaussed hard drive is inoperable to begin, so destruction adds only a visual indicator. General-purpose machine tools can be used for this, but a dedicated hard disk destroyer is included below.

In some non-classified applications, extensive physical destruction is substituted for degaussing. A hard disk shredder is often less expensive than an NSA-approved degausser, but does not satisfy the NSA standard. Hard drive shredders are distinguished primarily by the grain size of the remnants after a hard drive is shredded.

Garner HD-2

Price: *$4000*
Setup: *Easy*
Link: http://www.garnerproducts.com/HD-2.htm

Like other commercial degaussers, the entry-level product from Garner offers a high level of security from forensic analysis of a hard drive, but does not satisfy NSA or DoD requirements.

Garner TS-1

Price: *$16,000*
Setup: *Easy*
Link: http://www.garner-products.com/TS-1.htm

An NSA-approved degausser like this one is required for destruction of classified hard drives.

SEM 0100

Price: *$1,000*
Setup: *Easy*
Link: http://www.semshred.com/manual_hard_drive_crushers

Because physical destruction acts only as a security control procedure, a simple manually operated press or crusher like this one is sufficient for small-quantities of hard drives.

Garner PD-4

Price: *$4,000*
Setup: *Easy*
Link: http://www.garner-products.com/PD-4.htm

An automatic crusher can destroy hard drives somewhat faster than a manual press and allows a single employee to destroy more hard drives in one session. Hard drive destroyers range from this entry-level, hand-loaded Garner model to high-volume models with conveyor feed and downstream bagging stations.

Security Information and Event Management (SIEM)

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.SIM.1	SEIM Deployment	Security Information and Event Management provides visibility of network security; reduces costs of security administration	Admin.	High	Medium	Low	Medium	Low
TC.SIM.3	Centralized Configuration Policies	Enforces security policies across a network, reduces nonconforming configurations; reduces costs of security administration	Admin.	High	Medium	Medium	Medium	Low

These tools are useful for integrating and monitoring an overall computer security portfolio. The common theme is centralization. Conformance and visibility necessitate some form of centralized policy server for installed software, patch versions, passwords, timeout, account lockout, etc. Network intrusion detection also requires centralized log monitoring and correlating events at different machines.

OSSIM

Price: *Free (Commercial version available for $36,000/site)*
Setup: *Extensive*
Link: http://communities.alienvault.com/

OSSIM (Open Source Security Information Management) is an extensive front end for integrating and monitoring security tools. By default, an OSSIM virtual machine comes packaged with many individual tools listed elsewhere in this document. Aside from a graphical interface with powerful monitoring and summarizing widgets, OSSIM includes configurable sensors and agents.

OSSIM integrates and groups logs from diverse tools and allows correlating and setting incident thresholds to aid in filtering log data and generating alerts. This centralized log monitoring is perhaps the core feature of a SIEM product. OSSIM also scales to enterprise-level features like automated ticket generation—all included in the free version.

Two important applications of SEIM are auditing and forensics. To aid in recording events an SEIM appliance will maintain a database of past events, in addition to synthesized alerts and reports. Raw logs can be important for building cases or identifying root cause after a breech is detected. Data are also available for deeper inspection in real time if suspicious activity is suspected but making a conclusion requires further analysis. One nuance of logging is that ordering events can be contentious after the fact. Any SEIM appliance should have access to a timeserver so that clocks for the monitoring and production systems remain synchronized. For optimal resilience to network takeover, this time server should be geographically remote, as with a public time server.

One of the most difficult things to do is identify multistep attacks. Vulnerabilities have complex dependencies between them. This can be very important for the progress of hackers. Rarely is there a single vulnerability that when exploited provides control over an entire network. Instead, hackers gain influence incrementally, first scanning to find what can be seen and

attacked, then using new access to scan and attack new assets. In many cases, some function or privilege becomes a vulnerable only after a different vulnerability is exploited.

Unfortunately, finding all of the paths between vulnerabilities and understanding what new vulnerabilities are activated if others are exploited is difficult and has not been automated. This is one area of network monitoring where experience is invaluable. For small businesses, it is important to understand that individual events are not isolated. If one machine is infected or vulnerability, it is important to spend some time to catalog what could have been stolen from that machine, what secrets (passwords, keys) could have been exposed, and what other assets could have been attacked by someone who controlled that machine, given the new secrets an adversary would then possess.

Consistency can be important, as differences in settings can affect how administrators interpret alerts. Most SEIM solutions provide a distributed architecture for multiple sensors and filters but still provide centralized configurations and policies. At the minimum, it should be possible to export and import a standard configuration. Malware detection and packet filtering settings also benefit from centralized settings. If possible, SEIM databases for malware and other definitions should be updated automatically.

SEIM Attacks

Malicious actors also understand the importance of logs for investigation, so SEIM appliances and audit tools are prime candidates for attack. Luckily, the makers of auditing software are security-oriented so these instances tend to be reasonably secure, including few vulnerable services or versions, minimal software running, and encrypted images.

Nonetheless, access to monitoring and audit tools should be minimized. Very few machines need to initiate connections to monitoring machines; typically, the monitors will be making connections to other machines. Firewall rules can therefore tightly restrict incoming connections to security software.

All of the principles of passwords and two-factor authentication are heightened for auditing software. Few administrators need to manage SEIM appliances, so the principle of least privilege dictates that few accounts be created on security appliances. Such accounts are highly sensitive, so password complexity and expiration should be more stringent for SEIM accounts than for general administrator accounts. Two-factor authentication can be used here even if not for general administrator accounts. Relevant discussions can be found in the ‘Secure Passwords’ section on page 37 and the ‘Two Factor Authentication’ section on page 45.

Logs and audits should be backed up to offline copies on a schedule; for maximum security, backups can be made to write-once media, e.g. optical discs. Like all backups, encryption is important for audit logs.

Active Directory

Price: *Free (Windows only)*
Setup: *Moderate*
Link: http://www.microsoft.com/en-us/server-cloud/windows-server/identity-access.aspx

Active directory is the default Windows authentication and security server. A machine running Windows Server (a domain controller) is the default tool for centralized authentication and password rules. A domain controller also can be configured to push updates to all hosts and enforce other administrator policies in a Windows network.

Penetration Testing

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
---	Network Scanning	Discussed under Network Inventory on page 145						
TC.PEN.1	Vulnerability Scanning	Identifies commonly exploited vulnerabilities; reduces damages from compromised hosts	Admin.	High	Medium	Low	Low	Low
TC.PEN.2	Penetration Testing	Identifies configuration- and operations-specific vulnerabilities; reduces damages from compromise of business dataflow	Admin.	Medium	Medium	Low	Low	Medium

Penetration testing (pen testing) involves attacking an organization's own computer system to identify vulnerabilities. The discovered vulnerabilities can provide a roadmap for hardening a computer system. Pen testing can be done to harden a system before that system is put online or to evaluate an operational system.

Penetration testing involves multiple steps. The first step is to discover what is connected to the network; this was discussed in the 'Network Inventory' section on page 145. Inventory should be done in conjunction with setting the rules of engagement. Often at small businesses infrastructure is operated by third parties like hosting companies or IT providers. Every device on a network should have a known owner and should appear on either a blacklist of devices that that cannot be attacked or a whitelist of devices that must be tested. Initial inventory scans should flag any unknown device that is detected for inspection and inventory. Second, any network assets must be tested for vulnerabilities. Third, intrusive testing can be done to determine what is actually exposed by the vulnerabilities. Finally, all vulnerabilities that are discovered should be gathered in a list and reviewed for priority and mitigation plan. The most numerous vulnerabilities are easy to fix by applying patches or changing configurations, but a few will require planning and possibly budgeting.

Also important is to identify what information could have been exposed by discovered vulnerabilities. Vulnerabilities are dependent on each other, such that the existence of one vulnerability can create a vulnerability in an operation that is otherwise safe. For example, the Heartbleed vulnerability can expose encryption keys, rendering subsequent encrypted connections vulnerable. After identifying that encryption keys could have been exposed, a mitigation plan should include generating new certificates. With the knowledge that a specific vulnerability was present, logs from SEIM monitors can sometimes be reviewed to ascertain if the vulnerability was exploited.

Each tool below is useful in one of these stages.

Nmap

Price: *Free (Commercial version available)*
Setup: *Easy*
Link: http://nmap.org/

Nmap is the venerable tool for network reconnaissance (and inventory), and is included here to make clear the procedure for pen testing. Several higher-level scanning tools integrate Nmap, so possibly there is no need to use Nmap by itself. Nmap handles the initial low-level task of

scanning network addresses and detecting each unique host connected to a network. The result is an inventory of assets to exploit. Other network scanners include Nessus (http://www.tenable.com/products/nessus).

OpenVAS

Price: *Free (Commercial version available)*
Setup: *Moderate*
Link: http://www.openvas.org/

Vulnerability scanners are needed because keeping informed of vulnerabilities and ensuring network-wide coverage is impossible to do manually. For example, the mere presence of naïve applications like Telnet and RSH is a vulnerability, legacy protocols like LANMAN password hashes or older versions of authentication routines undermine the security of an entire network. The sheer number of software vulnerabilities patched every month makes keeping informed a full-time endeavor. Leveraging the accumulated knowledge in vulnerability scanners is the only viable option for small businesses.

Several scanners offer the option to report vulnerable service versions and unpatched software. OpenVAS is a dedicated vulnerability scanner, along with Nessus (http://www.tenable.com/products/nessus) and Nexpose (http://www.rapid7.com/products/nexpose/). Other vulnerability scanners include the NMAP scripting engine (http://nmap.org/book/nse.html). It is advisable to use multiple scanners after reconfiguration or during in-depth testing, as different scanners tend to detect somewhat different vulnerabilities. It is also necessary to update the vulnerability database before scanning, as patch notes disclose new vulnerabilities weekly.

Vulnerability scanners automate much of the task of penetration testing, and accordingly most security assessment services run a vulnerability scanner early on the first day before doing in-depth testing. The tradeoff for scanning compared to manual penetration testing is that scanners can attempt a larger number of exploits with less effort, but lack the 'white box' intuition of manual testing and so miss more system-specific vulnerabilities and sometimes obscure the need to evaluate what really needs protection. There is a commensurate tradeoff in labor: automatic scanning has lower cost but provides little training. A common strategy for continuous mitigation is to run a vulnerability scanner when online and do manual penetration testing during upgrades and maintenance.

Scanning is the first step in a network assessment; many organizations treat vulnerability scanning as an easy way to 'check off' security auditing requirements. Mitigating all 'high' risk vulnerabilities that are flagged by a scanner does not constitute securing a system. Firstly, even 'low' risk vulnerabilities can be used to gain access by a determined adversary. The actual risk from any vulnerability is a function of the use of a specific machine and the information contained therein. Secondly, scanning cannot identify data at rest that should be encrypted, communication that is unsecure, or any of the other gaps in process that often leave sensitive information exposed. Therefore, hardening an information security system always requires organizational review.

In short, nanny grade security requires nannies, and scanner results must be reviewed down to the 'low' risk vulnerabilities. This should be scheduled and resources allocated. Full time

security departments review alerts in real time (text message, etc.) For small companies alerts are ideally reviewed weekly to prevent complete network takeover, but possibly monthly to detect that it has happened.

Metasploit

Price: *Free (Commercial version available)*
Setup: *Extensive*
Link: http://www.metasploit.com/

Once network assets are inventoried, the next step is to breach each asset. Metasploit is a 'hackers toolkit' built around a large collection of vulnerabilities and exploits. While an IT background and extensive training are required to do manual penetration testing, the return on investment can be huge. First, penetration testing is probably the best training to start IT professionals thinking about the 'nuts and bolts' of security. Second, penetration testing can provide an eye-opening demonstration for management who are hesitant to allocate budget space to implementing security: with a few hours and a laptop, a penetration tester can provide visible evidence of breaking in and compromising sensitive but unsecure company data.

Web Application Testing

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.WAP.1	Server Scanning	Identifies most common server vulnerabilities; reduces costs of security staff remaining current on vulnerabilities	Admin.	High	Medium	Low	Low	Low
TC.WAP.2	Web App Testing	Identifies common vulnerabilities easily, facilitates in-depth testing for malicious inputs; lowest-cost measure to ensure minimum application security	Admin.	High	Medium	Low	Low	Medium

Not only are websites a large facet of the external surface of organizations, but web applications are also increasingly used for internal administration and collaboration. Unfortunately, two factors make web applications more vulnerable than native programs. First, web applications have not gone through nearly as many years of penetrate and patch cycles that have found most of the obvious bugs. Second, web applications make use of a high proportion of in-house code that is subjected to very limited testing.

Best practices and knowledge of common exploits against websites have been compiled into several applications. The tools below provide automatic scanning or attack features that will test websites against common exploits.

Nikto

Price: *Free*
Setup: *Easy*
Link: http://www.cirt.net/nikto2

Nikto can be used to scan webservers for vulnerabilities. The concept is very similar to other vulnerability scanners, except Nikto will scan for vulnerabilities that are exclusive to webservers: configuration errors, dangerous files, server versions with known exploits, etc. Nikto can also check for Cross-Site Scripting (XSS) vulnerabilities in common programs that are run on servers. Nikto does not test custom web applications.

ZAP

Price: *Free*
Setup: *Easy*
Link: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

ZAP (Zed Attack Proxy) includes an automatic attack mode that will scan a website and attempt common exploits against it.

For more in-depth testing, ZAP includes extensive capabilities for manipulating the packets sent between clients. An exchange can be paused and malicious messages inserted to test for how a web application will handle these. ZAP also acts as a proxy, and this facilitates performance of more complex attacks, such as Cross-Site Request Forgery (XSRF).

To test for SQL injection, format string exploits, buffer overflows, name resolution attacks and other malicious packets, Zap provides extensive fuzzer capabilities. Any text within a packet can

be highlighted and marked for fuzzing. This packet will be resent many times with the highlighted text replaced by a different malicious payload.

Intrusion Detection

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.IDS.1	Log Monitoring	One of the primary methods for intrusion detection, better for detection of compromised hosts; Reduces damages from resident adversaries	Admin.	High	Medium	Medium	Low	Medium
TC.IDS.2	Port Obscurity	Slows initial reconnaissance, reduces the noise that needs to be filtered from logs; reduces costs for network monitoring	Admin.	Medium	Medium	Low	Low	Low
TC.IDS.3	Packet Monitoring	Improves detection of initial infiltration activities and detection of compromised machines, limits exfiltration to external machines; Reduces damages following a breach	Admin.	High	Medium	Low	Low	Low

Intrusion detection complements penetration testing by finding malicious behavior within a live system. This problem is more involved than, for example, configuring a firewall because intrusion detection often requires keeping track of behavior over time or correlating events happening at different places in a network.

Because of the complexity of defining an intrusion event, one of the primary challenges in intrusion detection is balancing false alarms and missed detection. Finding an acceptable balance will require iterative configuration as an intrusion detection system is deployed. Intrusion detection also depends on detecting changes from 'normal' behavior and so will need to be retooled when a system is reconfigured.

OSSIM

Because intrusion detection requires a high-level view of a computer system, some of the best tools for intrusion detection overlap with SIEM. See the 'Security Information and Event Management (SIEM)' section on page 145 for more on OSSIM.

The individual components of a network—firewalls, servers, etc.—track local events and generate large amounts of log data. These data are too numerous and low-level to digest manually in real time. However, collectively these logs constitute enough data to develop a high-level, statistical view of a network.

By filtering and correlating events across a network, OSSIM becomes a primary tool for intrusion detection. OSSIM integrates sensors on each node that monitor individual tools and parse local logs. Network events are defined by configuring combinations of log events. Thresholds on severity or number of events can be set to balance timely alerts and a tolerable number of alerts.

Snort

Price: *Free*
Setup: *Moderate*
Link: http://www.snort.org/

Snort monitors network traffic and can detect intrusions using common recognition methods. Sort understands the protocols for network interactions and can evaluate violations, like asking for data before authenticating. More advanced methods include looking for signatures of known attacks and learning 'normal' behavior for a network and detecting anomalies in this behavior. Some behaviors apply to individual packets or sequences of packets, other behaviors apply to bulk traffic, such as volume or source and destination pairs.

Another, more specialized, protocol analyzer is Wireshark (http://www.wireshark.org/). Kismet (http://www.kismetwireless.net/) is a protocol analyzer for wireless networks. Suricata (http://suricata-ids.org/) specializes in deep analysis of web (HTTP) traffic. Protocol analysis facilitates defending against many flood attacks and malicious communications.

Packet inspection is often performed at network boundaries to enforce policy and prevent attack. Scanning incoming connections for malware is one common use. This is helpful because malware can be blocked regardless of what application-layer program is waiting to receive it. Like host-based malware scanners, network filters should be updated frequently.

Exfiltration can be detected by looking at payloads for data with sensitive labels. Support for content blocking is an in-depth undertaking and can require disassembling payloads at hosts into units that can be inspected by filters. Typically, such measures are employed only in classified or high security environments.

Any packets that are blocked should trigger alerts for administrators. Packet analysis can generate masses of events and alerts, so it can be difficult to find a good operating point between excessive false positives and false negatives. Malware detection events should have high priority for generating alerts.

The impact of false positives and filtering settings should be examined. In many cases, small businesses tune alert filters to reduce noisy alerts and detection ability sufferers. This is a defendable tradeoff given scares resources, but the impact of this on traffic detection ability should be acknowledged so that absent or ineffective packet inspection is not relied on for more security than it provides.

Testing of intrusion detection is crucial to determining if no news really is an indicator that nothing is wrong. Benign malware samples can be sent between machines to test malware detection capability. Routine IT tasks also provide natural tests. If an Nmap scan of a subnet at default aggressiveness does not generate a traffic or intrusion alert, then detection is not going to detect a hacker scanning with impunity.

Keep Logs Clean

Price: *Free*
Setup: *Moderate*
Link: N/A

One of the most difficult aspects of administering security for a network is filtering nuisance alerts. For example, a frequent event is an attempted login on SSH on port 22. One of the best methods for securing a network is simply to minimize the number of services running and the number of open ports and block everything else at the firewall. Certainly SSH should be running only if remote login to that machine is desired.

However, for those few services that must be available, events can remain a nuisance. The number of logged events can be reduced by changing default ports. This works because many opportunistic attackers, worms and scanning scripts try only well-known ports. This behavior is driven by the logistics of scanning all 65,536 ports on every machine, with each unused port taking at least one second to wait for a reply. For this reason also, a firewall should always drop packets, not reject. On average, a rejection will return much faster than the wait time after a dropped packet. If these ports are instead blocked by a firewall, then no attempted logins or other intrusions will make it through.

This configuration does not provide real hardened security and has other drawbacks. Changing ports can make penetration testing harder because full port scans are time consuming relative to the length of a test. To ensure the returns from testing are not diminished, if obscure ports are used testers should be given a list of open ports. Conversely, a persistent threat will be undeterred by changing ports, because full port scans are easily afforded during a protracted attack. Non-standard ports will also break default settings, so all applications will have to be configured. To make this method practical, unusual ports should be standardized within an organization.

Security Training

Code	Technique	Security Value; Business Value	End User	Overall Priority	Efficacy	Employee Resistance	Upfront Cost	Ongoing Cost
TC.STR.1	Security Training	Keeps security staff up to date, ensures competency in core areas; reduces preventable damages from mismanaged systems	Admin.	High	Medium	Low	Medium	Medium

MITRE

Price: *Free*
Setup: *Easy*
Link: http://www.mitre.org/work/cybersecurity/training.html

MITRE provides many free e-courses, documents, and some online interactive activities to help train IT professionals in security threat awareness and practical testing techniques.

SANS Institute

Price: *$2000-$6000*
Setup: *Easy*
Link: http://www.mitre.org/work/cybersecurity/training.html

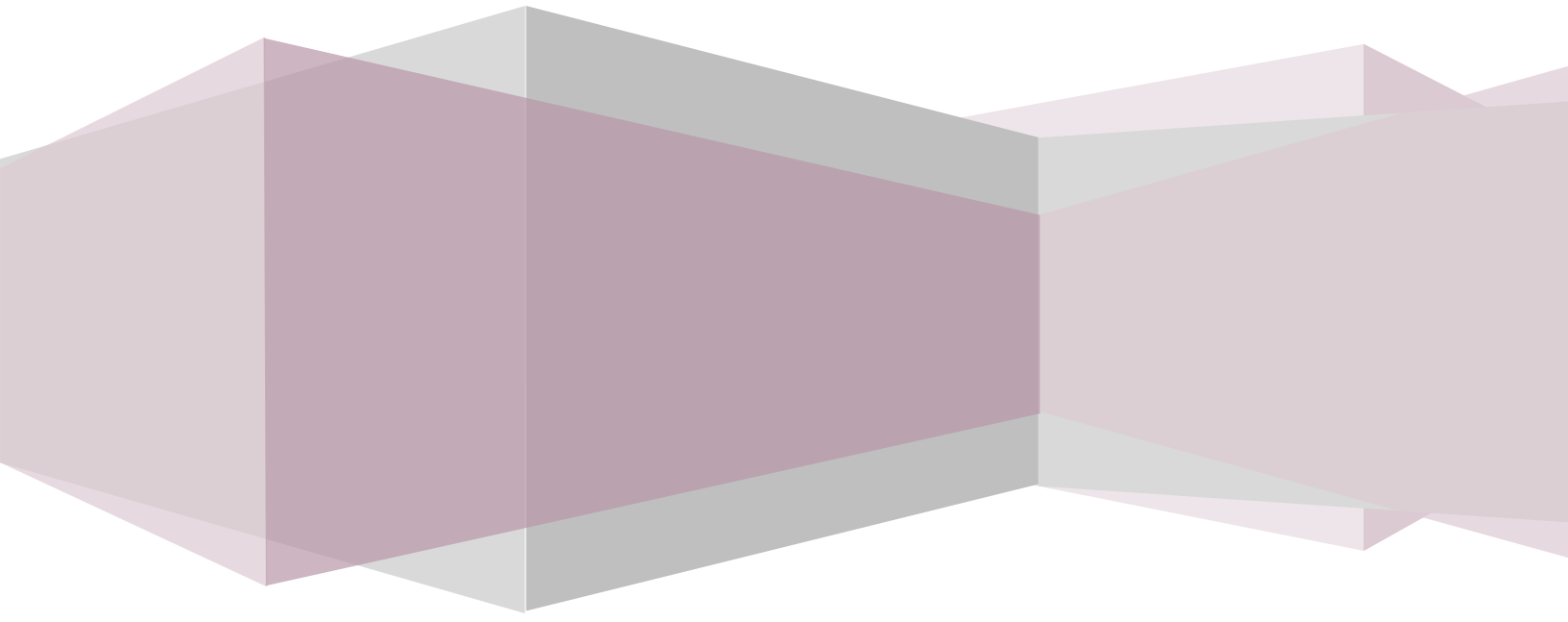
The SANS institute offers many courses for training and certification at sites around the United States. Classes typically follow the weeklong boot camp format.

Applied Research Laboratory
The Pennsylvania State University

Understanding Security

APPENDICES

Brice A. Toth
Caleb J. Severn
Jonathan Hoerr



Mapping to NIST 800-53 and DFARS

Defense contractors are subject to the requirements in Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 204.7303—Safeguarding Unclassified Controlled Technical Information—and DFARS 252.204-7012 as a clause in contracts. The DFARS clause is transitive to subcontractors, so a large number of smaller companies that operate several tiers below direct military suppliers are subject to DFARS although they have not directly contracted with government or defense suppliers.

DFARS Subpart 204.7303 requires a subset of the controls in NIST 800-53 to be implemented. For the aid of SMBs that must implement DFARS but benefit from the more detailed guidance of *Understanding Security*, below is a mapping of the DFARS subset of NIST 800-53 security controls to the techniques in *Understanding Security*. For each NIST 800-53 control, the codes for all relevant techniques are listed. A description for each code can be found in the corresponding section or in the summary of techniques given in the introduction to this book. Due to overlap with multiple NIST 800-53 controls, many techniques appear more than once.

The final column of the table indicates level of coverage: full, partial, none, or N/A. The concept of coverage here bears some explanation. NIST 800-53 provides a general framework for security controls that govern information systems. Similar to other general frameworks (e.g. the ISO series), NIST 800-53 provides an ontology of the subject, here information security, and populates a taxonomy with templates for controls. NIST 800-53 does not stipulate a set of concrete security controls, as doing so would sacrifice the generality of the framework.

In contrast, *Understanding Security* is not a general framework but a guidebook for the subset of businesses that fall within the Small- and Medium-Tiers. Most of the text in *Understanding Security* is dedicated to explaining many of the concepts that are enumerated in NIST 800-53, providing motivation for choosing one approach over another, as well as directly advising concrete controls. NIST 800-53 does not specify what assignments to make when instantiating a control template. A control template can be instantiated with a null assignment if not applicable. This is a design intent of a general control framework.

We avoid a trivial answer to the question of coverage by appealing to the supplemental guidance provided with most 800-53 controls. We define full coverage of a control, in reference to the supplemental guidance, as the existence of text in *Understanding Security* that 1) declares every example assignment that is mentioned in the supplemental guidance, and 2) discusses at any length every protection concept that is emphasized in the supplemental guidance (implications are typically covered but not guaranteed, definitions of prerequisite concepts are not guaranteed). The caveat is that *Understanding Security* does not address Large Tier businesses and so any assignment or concept that only applies to Large Tier businesses is excluded. In the case all assignments and concepts under a control apply only to Large-Tier organizations, the coverage is designated as not applicable. *Understanding Security* does not provide guidance for handling of classified information, so coverage level of all controls for classified information is not applicable.

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
AC-2	Account Management	---	---
AC-2a.		PT.ROL.3	Full
AC-2b.		PT.ROL.3	Full
AC-2c.		PT.ROL.3, PT.ROL.6	Full
AC-2d.		PT.ROL.3	Full
AC-2e.		PT.ROL.3, PT.ROL.6	Full
AC-2f.		PT.ROL.5	Full
AC-2g.		PT.ROL.7, PT.ROL.8	Full
AC-2h.		PT.ROL.6, PT.ROL.7, PT.ROL.8	Full
AC-2i.		PT.ROL.3	Full
AC-2j.		PT.ROL.7	Full
AC-2k.		PT.ROL.6	Full
AC-2 (1)	Automated System Account Management	PT.ROL.6	Full
AC-2 (2)	Removal Of Temporary / Emergency Accounts	PT.ROL.3, PT.ROL.4, PT.ROL.6	Full
AC-2 (3)	Disable Inactive Accounts	PT.ROL.6	Full
AC-2 (4)	Automated Audit Actions	PT.ROL.6	Full
AC-2 (5)	Inactivity Logout	PT.ACC.3, PT.ACC.4	Full
AC-2 (6)	Dynamic Privilege Management	PT.ROL.3, PT.ROL.6	Full
AC-2 (7)	Role-Based Schemes	---	---
AC-2 (7)(a)		PT.ROL.2, PT.ROL.3	Full
AC-2 (7)(b)		PT.ROL.6	Full
AC-2 (7)(c)		PT.ROL.6	Full
AC-2 (8)	Dynamic Account Creation	---	None
AC-2 (9)	Restrictions On Use Of Shared / Group Accounts	PT.ROL.2	Full
AC-2 (10)	Shared / Group Account Credential Termination	PT.ROL.6, PT.ROL.8	Full
AC-2 (11)	Usage Conditions	PT.ROL.4	Full
AC-2 (12)	Account Monitoring / Atypical Usage	PT.ROL.4	Full
AC-2 (13)	Disable Accounts For High-Risk Individuals	PT.ROL.6	Full
AC-3 (4)	Discretionary Access Control	---	---
AC-3 (4)(a)		PT.ROL.3	Full
AC-3 (4)(b)		PT.ROL.3	Full
AC-3 (4)(c)		PT.ROL.3	Full
AC-3 (4)(d)		PT.ROL.3, PT.ROL.6	Full
AC-3 (4)(e)		PT.ROL.6	Full
AC-4	Information Flow Enforcement	PT.DCT.1, PT.DCT.2, PT.CAC.2, PT.REM.1, PT.REM.2, PT.CLO.2., PT.DEV.2	Full
AC-4 (1)	Object Security Attributes	PT.DCT.1, PT.DCT.2	Partial
AC-4 (2)	Processing Domains	PT.DCT.1, PT.DCT.2, PT.ROL.3	Partial
AC-4 (3)	Dynamic Information Flow Control	PT.DCT.2, PT.ROL.4, PT.ROL.6	Full
AC-4 (4)	Content Check Encrypted Information		None
AC-4 (5)	Embedded Data Types	TC.HST.3	Partial
AC-4 (6)	Metadata		None

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
AC-4 (7)	One-Way Flow Mechanisms		None
AC-4 (8)	Security Policy Filters	PT.ROL.2, PT.ROL.3, PT.ROL.6	Full
AC-4 (9)	Human Reviews		None
AC-4 (10)	Enable / Disable Security Policy Filters	PT.ROL.6	Full
AC-4 (11)	Configuration Of Security Policy Filters	PT.ROL.4, PT.ROL.6	Full
AC-4 (12)	Data Type Identifiers	PT.ROL.2, PT.ROL.3, PT.ROL.6	Full
AC-4 (13)	Decomposition Into Policy-Relevant Subcomponents		None
AC-4 (14)	Security Policy Filter Constraints	TC.HST.3	Partial
AC-4 (15)	Detection Of Unsanctioned Information	TC.HST.3	Partial
AC-4 (16)	Information Transfers On Interconnected Systems [Withdrawn]		---
AC-4 (17)	Domain Authentication		None
AC-4 (18)	Security Attribute Binding		None
AC-4 (19)	Validation Of Metadata		None
AC-4 (20)	Approved Solutions		None
AC-4 (21)	Physical / Logical Separation Of Information Flows		None
AC-4 (22)	Access Only	PT.ROL.3, PT.ROL.6	Full
AC-6	Least Privilege	PT.ROL.2, PT.ROL.3, PT.ROL.4	Full
AC-6 (1)	Authorize Access To Security Functions	PT.ROL.3, PT.ROL.4, PT.ROL.7,	Full
AC-6 (2)	Non-Privileged Access For Nonsecurity Functions	PT.ROL.3	Full
AC-6 (3)	Network Access To Privileged Commands	PT.REM.3, PT.ROL.4	Full
AC-6 (4)	Separate Processing Domains	PT.ROL.3, TC.INV.4	Partial
AC-6 (5)	Privileged Accounts	PT.ROL.3	Full
AC-6 (6)	Privileged Access By Non-Organizational Users	PT.REM.2, PT.REM.3	Full
AC-6 (7)	Review Of User Privileges	---	---
AC-6 (7)(a)		PT.ROL.7	Full
AC-6 (7)(b)		PT.ROL.7	Full
AC-6 (8)	Privilege Levels For Code Execution		None
AC-6 (9)	Auditing Use Of Privileged Functions	TC.SIM.1, TC.IDS.1, TC.IDS.3	Full
AC-6 (10)	Prohibit Non-Privileged Users From Executing Privileged Functions	PT.ROL.6, TC.IDS.1, PT.DCT.4	Full
AC-7	Unsuccessful Logon Attempts	---	---
AC-7a.		PT.PAS.4	Full
AC-7b.		PT.PAS.4	Full
AC-7 (1)	Automatic Account Lock [Withdrawn]		---
AC-7 (2)	Purge / Wipe Mobile Device		None
AC-11 (1)	Pattern-Hiding Displays	PT.ACC.4	Full
AC-17 (2)	Protection Of Confidentiality / Integrity Using Encryption	PT.CAC.2. PT.REM.1	Full
AC-18 (1)	Authentication And Encryption	TC.WRL.1	Full
AC-19	Access Control For Mobile Devices	---	---
AC-19a.		PT.DEV.3	Full
AC-19b.		PT.DEV.3	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
AC-19 (1)	Use Of Writable / Portable Storage Devices [Withdrawn]		---
AC-19 (2)	Use Of Personally Owned Portable Storage Devices [Withdrawn]		---
AC-19 (3)	Use Of Portable Storage Devices With No Identifiable Owner [Withdrawn]		---
AC-19 (4)	Restrictions For Classified Information	---	---
AC-19 (4)(a)			N/A
AC-19 (4)(b)			N/A
AC-19 (4)(c)			N/A
AC-19 (5)	Full Device / Container-Based Encryption	PT.DEV.4, TC.CAC.2	Full
AC-20 (1)	Limits On Authorized Use	---	---
AC-20 (1)(a)		PT.DEV.6	Full
AC-20 (1)(b)		PT.CLO.1, PT.CLO.2	Full
AC-20 (2)	Portable Storage Devices	PT.DCT.1, PT.DEV.2	Full
AC-22	Publicly Accessible Content	---	---
AC-22a.		PT.SME.2, PT.SME.3	Partial
AC-22b.		PT.SME.2	Partial
AC-22c.		PT.SME.2	Partial
AC-22d.		PT.SME.2	Partial
AT-2	Security Awareness Training	---	---
AT-2a.		PT.ROL.9	Full
AT-2b.		PT.ROL.9	Full
AT-2c.		PT.ROL.9	Full
AT-2 (1)	Practical Exercises	PT.RAC.1, PT.RAC.2	Partial
AT-2 (2)	Insider Threat	PT.BUY.1, PT.SEN.1	Partial
AU-2	Audit Events	---	---
AU-2a.		PT.AFF.2	Full
AU-2b.		PT.AFF.2	Full
AU-2c.		PT.CRT.3	Partial
AU-2d.		PT.AFF.2	Full
AU-2 (1)	Compilation Of Audit Records From Multiple Sources [Withdrawn]		---
AU-2 (2)	Selection Of Audit Events By Component [Withdrawn]		---
AU-2 (3)	Reviews And Updates	PT.AFF.2	Full
AU-2 (4)	Privileged Functions [Withdrawn]		---
AU-3	Content Of Audit Records	PT.CRT.3	Full
AU-3 (1)	Additional Audit Information	PT.CRT.3	Full
AU-3 (2)	Centralized Management Of Planned Audit Record Content		None
AU-6 (1)	Process Integration		None
AU-7	Audit Reduction And Report Generation	---	---
AU-7a.		PT.CRT.3, TC.SIM.1	Full
AU-7b.		TC.SIM.1	Full
AU-7 (1)	Automatic Processing	TC.SIM.1	Full
AU-7 (2)	Automatic Sort And Search	TC.SIM.1	Full
AU-8	Time Stamps	---	---

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
AU-8a.		TC.SIM.1	Full
AU-8b.		TC.SIM.1	Full
AU-8 (1)	Synchronization With Authoritative Time Source	---	---
AU-8 (1)(a)		TC.SIM.1	Full
AU-8 (1)(b)		TC.SIM.1	Full
AU-8 (2)	Secondary Authoritative Time Source	TC.SIM.1	Full
AU-9	Protection Of Audit Information	TC.SIM.1	Full
AU-9 (1)	Hardware Write-Once Media	TC.SIM.1	Full
AU-9 (2)	Audit Backup On Separate Physical Systems / Components	TC.SIM.1	Full
AU-9 (3)	Cryptographic Protection	TC.SIM.1	Full
AU-9 (4)	Access By Subset Of Privileged Users	TC.SIM.1	Full
AU-9 (5)	Dual Authorization	TC.SIM.1	Full
AU-9 (6)	Read Only Access	TC.SIM.1	Full
CM-2	Baseline Configuration	PT.SWI.3, TC.CSH.4, TC.INV.3	Full
CM-2 (1)	Reviews And Updates	---	---
CM-2 (1)(a)		PT.SWI.3	Full
CM-2 (1)(b)		PT.SWI.3	Full
CM-2 (1)(c)		PT.SWI.3	Full
CM-2 (2)	Automation Support For Accuracy / Currency		None
CM-2 (3)	Retention Of Previous Configurations	PT.SWI.3	Full
CM-2 (4)	Unauthorized Software [Withdrawn]		---
CM-2 (5)	Authorized Software [Withdrawn]		---
CM-2 (6)	Development And Test Environments	TC.INV.4	Partial
CM-2 (7)	Configure Systems, Components, Or Devices For High-Risk Areas	---	---
CM-2 (7)(a)		PT.DEV.8, PT.DEV.9	Full
CM-2 (7)(b)		PT.DEV.10	Full
CM-6	Configuration Settings	TC.CSH.1, TC.CSH.2, TC.CSH.3, TC.CSH.4, TC.CSH.5	Full
CM-6 (1)	Automated Central Management / Application / Verification	TC.SIM.2	Full
CM-6 (2)	Respond To Unauthorized Changes	TC.SIM.2	Full
CM-6 (3)	Unauthorized Change Detection [Withdrawn]		---
CM-6 (4)	Conformance Demonstration [Withdrawn]		---
CM-7	Least Functionality	---	---
CM-7a.		TC.CSH.3, TC.CSH.4	Full
CM-7b.		TC.CSH.2, TC.TCH.5	Full
CM-7 (1)	Periodic Review	---	---
CM-7 (1)(a)		TC.CSH.4, TC.INV.2, TC.INV.3	Full
CM-7 (1)(b)		TC.CSH.4, TC.INV.2, TC.INV.3	Full
CM-7 (2)	Prevent Program Execution	TC.HST.1, TC.INV.2	Full
CM-7 (3)	Registration Compliance	TC.CSH.4, TC.CSH.5, TC.INV.1	Full
CM-7 (4)	Unauthorized Software / Blacklisting	PT.NET.1, TC.HST.4	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
CM-7 (5)	Authorized Software / Whitelisting	PT.NET.1, TC.HST.4	Full
CM-8	Information System Component Inventory	---	---
CM-8a.		TC.INV.1, TC.INV.2	Full
CM-8b.		TC.INV.1, TC.INV.2	Full
CM-8 (1)	Updates During Installations / Removals	TC.CSH.4	Full
CM-8 (2)	Automated Maintenance	TC.INV.2	Full
CM-8 (3)	Automated Unauthorized Component Detection	---	---
CM-8 (3)(a)		TC.INV.1, TC.INV.2	Full
CM-8 (3)(b)		PT.RAC.1, TC.SIM.2	Full
CM-8 (4)	Accountability Information	PT.SRD.1	Full
CM-8 (5)	No Duplicate Accounting Of Components	TC.INV.2	Full
CM-8 (6)	Assessed Configurations / Approved Deviations	TC.CSH.4, TC.WLK.5	Full
CM-8 (7)	Centralized Repository	PT.DEV.2. TC.INV.2	Full
CM-8 (8)	Automated Location Tracking	PT.DEV.2. TC.INV.2	Full
CM-8 (9)	Assignment Of Components To Systems	---	---
CM-8 (9)(a)		TC.INV.1, TC.INV.2	Full
CM-8 (9)(b)			None
CP-9	Information System Backup	---	---
CP-9a.		PT.DIN.1, PT.DIN.3	Full
CP-9b.		PT.DIN.1, PT.DIN.3	Partial
CP-9c.		PT.DIN.1, PT.DIN.4, TC.SIM.1	Full
CP-9d.		PT.DIN.2, PT.DIN.4, PT.DIN.5	Full
CP-9 (1)	Testing For Reliability / Integrity	PT.DIN.4	Full
CP-9 (2)	Test Restoration Using Sampling	PT.RAC.4	Full
CP-9 (3)	Separate Storage For Critical Information	PT.DIN.2	Full
CP-9 (4)	Protection From Unauthorized Modification [Withdrawn]		---
CP-9 (5)	Transfer To Alternate Storage Site	PT.DIN.2	Full
CP-9 (6)	Redundant Secondary System	PT.DIN.2, PT.RAC.4	Full
CP-9 (7)	Dual Authorization	PT.SRD.3	Full
IA-2	Identification And Authentication (Organizational Users)	PT.ROL.3	Full
IA-2 (1)	Network Access To Privileged Accounts	PT.AUT.2	Full
IA-2 (2)	Network Access To Non-Privileged Accounts	PT.AUT.2	Full
IA-2 (3)	Local Access To Privileged Accounts	PT.AUT.1, PT.AUT.2	Full
IA-2 (4)	Local Access To Non-Privileged Accounts	PT.AUT.1, PT.AUT.2	Full
IA-2 (5)	Group Authentication	PT.ROL.3	Full
IA-2 (6)	Network Access To Privileged Accounts - Separate Device	PT.AUT.2	Full
IA-2 (7)	Network Access To Non-Privileged Accounts - Separate Device	PT.AUT.2	Full
IA-2 (8)	Network Access To Privileged Accounts - Replay Resistant	PT.AUT.2	Full
IA-2 (9)	Network Access To Non-Privileged Accounts - Replay Resistant	PT.AUT.2	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
IA-2 (10)	Single Sign-On		None
IA-2 (11)	Remote Access - Separate Device	PT.AUT.2	Full
IA-2 (12)	Acceptance Of PIV Credentials		None
IA-2 (13)	Out-Of-Band Authentication	PT.AUT.2	Full
IA-4	Identifier Management	---	---
IA-4a.		PT.ROL.6	Full
IA-4b.		PT.ROL.3	Full
IA-4c.		PT.ROL.3	Full
IA-4d.		PT.ROL.3, PT.REM.2	Full
IA-4e.		PT.ACC.4	Full
IA-4 (1)	Prohibit Account Identifiers As Public Identifiers		None
IA-4 (2)	Supervisor Authorization	PT.ROL.6, PT.ROL.7	Full
IA-4 (3)	Multiple Forms Of Certification	PT.SEN.5	Full
IA-4 (4)	Identify User Status	PT.ROL.7	Full
IA-4 (5)	Dynamic Management		None
IA-4 (6)	Cross-Organization Management	PT.SEN.3	Full
IA-4 (7)	In-Person Registration	PT.SEN.5	Partial
IA-5 (1)	Password-Based Authentication	---	---
IA-5 (1)(a)		PT.PAS.2	Full
IA-5 (1)(b)		PT.PAS.2	Full
IA-5 (1)(c)		PT.PAS.2, TC.CSH.5	Full
IA-5 (1)(d)		PT.PAS.3	Full
IA-5 (1)(e)		PT.PAS.2	Full
IA-5 (1)(f)		PT.PAS.4	Full
IR-2	Incident Response Training	---	---
IR-2a.		PT.ROL.7, PT.SRD.1, PT.SRD.2	Full
IR-2b.		PT.SRD.2	Full
IR-2c.		PT.SRD.2	Full
IR-2 (1)	Simulated Events	PT.RAC.4	Full
IR-2 (2)	Automated Training Environments		None
IR-4	Incident Handling	---	---
IR-4a.		PT.CRT.2, PT.CRT.3	Full
IR-4b.		PT.RAC.2, PT.RAC.4	Full
IR-4c.		PT.CRT.3	Full
IR-4 (1)	Automated Incident Handling Processes		None
IR-4 (2)	Dynamic Reconfiguration		None
IR-4 (3)	Continuity Of Operations	PT.RAC.2	Full
IR-4 (4)	Information Correlation	PT.CRT.3	Full
IR-4 (5)	Automatic Disabling Of Information System	PT.RAC.2	Partial
IR-4 (6)	Insider Threats - Specific Capabilities	PT.SEN.1, PT.CRT.1	Partial
IR-4 (7)	Insider Threats - Intra-Organization Coordination		None
IR-4 (8)	Correlation With External Organizations	PT.PSH.9, PT.CRT.3	Full
IR-4 (9)	Dynamic Response Capability	PT.RAC.2	Full
IR-4 (10)	Supply Chain Coordination	PT.RAC.2	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
IR-5	Incident Monitoring	PT.CRT.3	Full
IR-5 (1)	Automated Tracking / Data Collection / Analysis	TC.SIM.1	Full
IR-6	Incident Reporting	---	---
IR-6a.		PT.CRT.1	Full
IR-6b.		PT.CRT.3	Full
IR-6 (1)	Automated Reporting		None
IR-6 (2)	Vulnerabilities Related To Incidents	PT.CRT.3, TC.SIM.1	Full
IR-6 (3)	Coordination With Supply Chain	PT.RAC.2	Full
MA-4 (6)	Cryptographic Protection	PT.REM.1, TC.WLK.2	Full
MA-5	Maintenance Personnel	---	---
MA-5a.		PT.SEN.3	Full
MA-5b.		PT.ACC.2, PT.ACC.6	Full
MA-5c.		PT.SEN.3, PT.ACC.6	Full
MA-5 (1)	Individuals Without Appropriate Access	---	---
MA-5 (1)(a)			N/A
MA-5 (1)(b)			None
MA-5 (2)	Security Clearances For Classified Systems		N/A
MA-5 (3)	Citizenship Requirements For Classified Systems		N/A
MA-5 (4)	Foreign Nationals	---	---
MA-5 (4)(a)			N/A
MA-5 (4)(b)			N/A
MA-5 (5)	Nonsystem-Related Maintenance	PT.ACC.1, PT.ACC.6	Full
MA-6	Timely Maintenance	PT.RAC.2	Full
MA-6 (1)	Preventive Maintenance	PT.RAC.2	Full
MA-6 (2)	Predictive Maintenance	PT.RAC.2	Full
MA-6 (3)	Automated Support For Predictive Maintenance	PT.RAC.2, PT.RAC.3	Full
MP-4	Media Storage	---	---
MP-4a.		PT.ACC.1	Full
MP-4b.		PT.DCT.5, TC.HDD.1, TC.HDD.2	Full
MP-4 (1)	Cryptographic Protection		
MP-4 (2)	Automated Restricted Access	PT.ACC.1, PT.ACC.10	Partial
MP-6	Media Sanitization	---	---
MP-6a.		PT.DCT.5, TC.CAC.1	Full
MP-6b.		TC.HDD.1, TC.HDD.2	Full
MP-6 (1)	Review / Approve / Track / Document / Verify	PT.DCT.1, PT.DCT.5	Full
MP-6 (2)	Equipment Testing	PT.DCT.5	Full
MP-6 (3)	Nondestructive Techniques	PT.DEV.1	Full
MP-6 (4)	Controlled Unclassified Information [Withdrawn]		---
MP-6 (5)	Classified Information [Withdrawn]		---
MP-6 (6)	Media Destruction [Withdrawn]		---
MP-6 (7)	Dual Authorization	PT.SRD.3	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
MP-6 (8)	Remote Purging / Wiping Of Information	PT.DEV.5	Full
PE-2	Physical Access Authorizations	---	---
PE-2a.		PT.ACC.2	Full
PE-2b.		PT.ACC.2	Full
PE-2c.		PT.ACC.2, PT.ACC.10	Full
PE-2d.		PT.ACC.1, PT.ACC.2	Full
PE-3	Physical Access Control	---	---
PE-3a.		PT.ACC.1, PT.ACC.2	Full
PE-3b.		PT.ACC.2	Full
PE-3c.		PT.ACC.1	Full
PE-3d.		PT.ACC.5, PT.ACC.6, PT.ACC.7	Full
PE-3e.		PT.ACC.1, PT.AUT.1	Full
PE-3f.		PT.ACC.10	Full
PE-3g.		PT.ACC.10	Full
PE-3 (1)	Information System Access	PT.ACC.1	Full
PE-3 (2)	Facility / Information System Boundaries	PT.ACC.10	Full
PE-3 (3)	Continuous Guards / Alarms / Monitoring	PT.PHY.2, PT.PHY.4	Full
PE-3 (4)	Lockable Casings	PT.ACC.1	Full
PE-3 (5)	Tamper Protection	PT.PHY.4	Full
PE-3 (6)	Facility Penetration Testing	PT.PHY.5	Full
PE-5	Access Control For Output Devices	PT.ACC.1	Full
PE-5 (1)	Access To Output By Authorized Individuals	PT.ACC.1	Full
PE-5 (2)	Access To Output By Individual Identity	PT.ACC.1	Full
PE-5 (3)	Marking Output Devices	PT.ROL.2	Full
PM-10	Security Authorization Process	---	---
PM-10a.		PT.ROL.3	Full
PM-10b.		PT.ROL.3	Full
PM-10c.		PT.ROL.2	Full
RA-5	Vulnerability Scanning	---	---
RA-5a.		TC.PEN.1	Full
RA-5b.		---	---
RA-5b.1.		TC.PEN.1	Full
RA-5b.2.		TC.SIM.1	Full
RA-5b.3.		TC.PEN.1	Full
RA-5c.		TC.SIM.1, TC.PEN.2	Full
RA-5d.		TC.PEN.1	Full
RA-5e.		PT.SRD.1	Full
RA-5 (1)	Update Tool Capability	TC.PEN.1	Full
RA-5 (2)	Update By Frequency / Prior To New Scan / When Identified	TC.PEN.1	Full
RA-5 (3)	Breadth / Depth Of Coverage	TC.PEN.1	Full
RA-5 (4)	Discoverable Information	TC.PEN.1	Full
RA-5 (5)	Privileged Access	TC.SIM.1	Full
RA-5 (6)	Automated Trend Analyses	TC.SIM.1	Full
RA-5 (7)	Automated Detection And Notification Of Unauthorized Components [Withdrawn]		---

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
RA-5 (8)	Review Historic Audit Logs	TC.SIM.1, TC.PEN.1	Full
RA-5 (9)	Penetration Testing And Analyses [Withdrawn]		---
RA-5 (10)	Correlate Scanning Information	TC.SIM.1, TC.IDS.1	Full
SC-2	Application Partitioning	TC.INV.4	Full
SC-2 (1)	Interfaces For Non-Privileged Users	PT.ROL.3, PT.ROL.6	Full
SC-4	Information In Shared Resources	PT.ROL.1, PT.ROL.2	Full
SC-4 (1)	Security Levels [Withdrawn]		---
SC-4 (2)	Periods Processing	PT.ROL.3, PT.ROL.6	Full
SC-7	Boundary Protection	---	---
SC-7a.		TC.INV.4, TC.SIM.1, TC.IDS.1	Full
SC-7b.		TC.INV.4	Full
SC-7c.		TC.INV.4	Full
SC-7 (1)	Physically Separated Subnetworks [Withdrawn]		---
SC-7 (2)	Public Access [Withdrawn]		---
SC-7 (3)	Access Points	TC.INV.4	Full
SC-7 (4)	External Telecommunications Services	PT.CAC.1, PT.REM.1	Partial
SC-7 (5)	Deny By Default / Allow By Exception	TC.FIR.1	Full
SC-7 (6)	Response To Recognized Failures [Withdrawn]		---
SC-7 (7)	Prevent Split Tunneling For Remote Devices	TC.CAC.4	Full
SC-7 (8)	Route Traffic To Authenticated Proxy Servers	TC.INV.4	Full
SC-7 (9)	Restrict Threatening Outgoing Communications Traffic		None
SC-7 (10)	Prevent Unauthorized Exfiltration	TC.HST.2, TC.IDS.1	Partial
SC-7 (11)	Restrict Incoming Communications Traffic	TC.INV.4	Full
SC-7 (12)	Host-Based Protection	TC.HST.1	Full
SC-7 (13)	Isolation Of Security Tools / Mechanisms / Support Components	TC.INV.4, TC.SIM.1	Full
SC-7 (14)	Protects Against Unauthorized Physical Connections	PT.ACC.1	Full
SC-7 (15)	Route Privileged Network Accesses		None
SC-7 (16)	Prevent Discovery Of Components / Devices	TC.INV.4	Full
SC-7 (17)	Automated Enforcement Of Protocol Formats	TC.IDS.3	Full
SC-7 (18)	Fail Secure	TC.FIR.1	Full
SC-7 (19)	Blocks Communication From Non-Organizationally Configured Hosts	PT.DEV.3	Full
SC-7 (20)	Dynamic Isolation / Segregation	TC.INV.4	Full
SC-7 (21)	Isolation Of Information System Components	TC.INV.4	Full
SC-7 (22)	Separate Subnets For Connecting To Different Security Domains	TC.INV.4	Full
SC-7 (23)	Disable Sender Feedback On Protocol Validation Failure	TC.FIR.1	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
SC-8 (1)	Cryptographic Or Alternate Physical Protection	PT.CAC.2, PT.REM.1, TC.CAC.4	Full
SC-13	Cryptographic Protection	PT.DCT.3, PT.DEV.2, TC.CAC.2	Full
SC-13 (1)	Fips-Validated Cryptography [Withdrawn]		---
SC-13 (2)	Nsa-Approved Cryptography [Withdrawn]		---
SC-13 (3)	Individuals Without Formal Access Approvals [Withdrawn]		---
SC-13 (4)	Digital Signatures [Withdrawn]		---
SC-15	Collaborative Computing Devices		None
SC-15 (1)	Physical Disconnect		None
SC-15 (2)	Blocking Inbound / Outbound Communications Traffic [Withdrawn]		---
SC-15 (3)	Disabling / Removal In Secure Work Areas		None
SC-15 (4)	Explicitly Indicate Current Participants		None
SC-28	Protection Of Information At Rest	PT.DIN.1, PT.DIN.2, PT.DIN.3, PT.DIN.5, PT.DCT.3, TC.CAC.2	Full
SC-28 (1)	Cryptographic Protection	PT.DIN.1, PT.DIN.2, PT.DIN.3, PT.DIN.4, PT.DIN.5, PT.DCT.3, TC.CAC.2	Full
SC-28 (2)	Off-Line Storage	PT.DIN.2	Full
SI-2	Flaw Remediation	---	---
SI-2a.		TC.INV.2, TC.SIM.1, TC.PEN.1	Full
SI-2b.			None
SI-2c.		PT.SUP.1, PT.SUP.3, PT.SUP.4, TC.INV.2	Full
SI-2d.		PT.SUP.3, PT.SUP.4, TC.INV.2	Full
SI-2 (1)	Central Management	PT.SUP.3, PT.SUP.4	Full
SI-2 (2)	Automated Flaw Remediation Status	PT.SUP.3, TC.INV.2,	Full
SI-2 (3)	Time To Remediate Flaws / Benchmarks For Corrective Actions	---	---
SI-2 (3)(a)		PT.SUP.4	Full
SI-2 (3)(b)		PT.SUP.4	Full
SI-2 (4)	Automated Patch Management Tools [Withdrawn]		---
SI-2 (5)	Automatic Software / Firmware Updates	PT.SUP.2, PT.SUP.3	Full
SI-2 (6)	Removal Of Previous Versions Of Software / Firmware	PT.SUP.1	Full
SI-3	Malicious Code Protection	---	---
SI-3a.		TC.HST.1, TC.IDS.3	Full
SI-3b.		TC.HST.1, TC.IDS.3	Full
SI-3c.		TC.HST.1, TC.IDS.3	Full
SI-3c.1.		TC.HST.1, TC.IDS.3	Full
SI-3c.2.		TC.IDS.3	Full
SI-3d.		TC.IDS.3	Full
SI-3 (1)	Central Management	TC.SIM.1	Full
SI-3 (2)	Automatic Updates	TC.SIM.1	Full
SI-3 (3)	Non-Privileged Users [Withdrawn]		---

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
SI-3 (4)	Updates Only By Privileged Users	TC.SIM.1	Full
SI-3 (5)	Portable Storage Devices [Withdrawn]		---
SI-3 (6)	Testing / Verification		None
SI-3 (7)	Nonsignature-Based Detection	TC.HST.1	Full
SI-3 (8)	Detect Unauthorized Commands	TC.HST.1	Full
SI-3 (9)	Authenticate Remote Commands	PT.REM.2	Full
SI-3 (10)	Malicious Code Analysis	---	---
SI-3 (10)(a)		TC.HST.1, TC.IDS.3	Full
SI-3 (10)(b)		PT.CRT.1, TC.SIM.1, TC.IDS.3	Full
SI-4	Information System Monitoring	---	---
SI-4a.		---	---
SI-4a.1.		PT.SIM.1, TC.IDS.3	Full
SI-4a.2.		PT.HST.1, TC.IDS.3	Full
SI-4b.		PT.DIN.4, TC.HST.2, TC.SIM.1, TC.IDS.1	Full
SI-4c.		TC.SIM.1, TC.IDS.3	Full
SI-4d.		PT.SRD.3, TC.SIM.1	Full
SI-4e.		PT.CRT.2, TC.SIM.1	
SI-4f.		TC.PEN.2	Partial
SI-4g.		PT.CRT.3	Full
SI-4 (1)	System-Wide Intrusion Detection System	TC.SIM.1, TC.IDS.3	Full
SI-4 (2)	Automated Tools For Real-Time Analysis	TC.SIM.1, TC.IDS.1, TC.IDS.3	Full
SI-4 (3)	Automated Tool Integration	TC.INV.1, TC.SIM.1	Full
SI-4 (4)	Inbound And Outbound Communications Traffic	PT.NET.1, TC.HST.2, TC.INV.4, TC.IDS.3	Full
SI-4 (5)	System-Generated Alerts	TC.SIM.1	Full
SI-4 (6)	Restrict Non-Privileged Users [Withdrawn]		
SI-4 (7)	Automated Response To Suspicious Events	TC.SIM.1	Full
SI-4 (8)	Protection Of Monitoring Information [Withdrawn]		
SI-4 (9)	Testing Of Monitoring Tools	TC.IDS.3	Full
SI-4 (10)	Visibility Of Encrypted Communications		None
SI-4 (11)	Analyze Communications Traffic Anomalies	TC.IDS.3	Full
SI-4 (12)	Automated Alerts	TC.SIM.1	Full
SI-4 (13)	Analyze Traffic / Event Patterns	---	---
SI-4 (13)(a)		TC.IDS.3	Full
SI-4 (13)(b)		TC.IDS.3	Full
SI-4 (13)(c)		TC.SIM.1	Full
SI-4 (14)	Wireless Intrusion Detection	TC.IDS.3	Full
SI-4 (15)	Wireless To Wireline Communications	TC.IDS.3	Full
SI-4 (16)	Correlate Monitoring Information	TC.SIM.1	Full
SI-4 (17)	Integrated Situational Awareness	PT.CRT.3, PT.SRD.1, PT.SRD.3, TC.SIM.1	Full
SI-4 (18)	Analyze Traffic / Covert Exfiltration	PT.ROL.3, TC.HST.2, TC.IDS.3	Full
SI-4 (19)	Individuals Posing Greater Risk	PT.SEN.3	Full

NIST 800-53 rev. 4	Title	Understanding Security	Coverage
SI-4 (20)	Privileged Users	PT.SEN.3	Full
SI-4 (21)	Probationary Periods	PT.SEN.3	Full
SI-4 (22)	Unauthorized Network Services	TC.INV.1, TC.INV.2, TC.INV.4	Full
SI-4 (23)	Host-Based Devices	TC.HST.2	Full
SI-4 (24)	Indicators Of Compromise	PT.SUP.2, TC.HST.2, TC.SIM.1	Full

References

[1] Cyber Security Operations Centre, Intelligence and Security, Department of Defense, Australian Government, "Strategies to Mitigate Targeted Cyber Intrusions," Department of Defense, Australian Government, 2013.

[2] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, "Preliminary Cybersecurity Framework," NIST, 2013.

[3] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, "SP-800," NIST.

[4] Electronic Enterprise Integration Committee, Aerospace Industries of America, "National Aerospace Standard: Cyber Security Baseline (NAS9924)," Aerospace Industries of America, 2013.

[5] International Organization for Standardization / International Electrotechnical Commission, "ISO/IEC 27001:2005," ISO/IEC, 2005.

[6] SANS Institute, "Critical Security Controls - Vesion 5," August 2014. [Online]. Available: http://www.sans.org/critical-security-controls.

[7] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology, Gaithersburg, Maryland, 2003.

[8] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor and J. Lopez, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, Oakland, 2012.

[9] "xkcd.com," [Online]. Available: http://xkcd.com/936/. [Accessed 13 March 2013].

[10] J. Heiser and A. Bona, "Cloud Contracts Need Security Service Levels to Better Manage Risk," Gartner, 2013.

[11] W. S. Mossberg, "Google Redefines Web Browser," Wall Street Journal, 2008.

[12] United States Computer Emergency Readiness Team (US-CERT), "Introduction to Information Security," 2012.