Cyber Security Best Practices: What to do?

Howard Kleinberg
kleinbergh@uncw.edu

Bryan Reinicke
reinickeb@uncw.edu

Jeff Cummings
cummingsj@uncw.edu

Information Systems and Operations Management Dept.
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

While cyber security is an increasingly important topic for organizations globally, it is also a confusing one for both researchers and practitioners. A great deal has been written about cyber security, but there is comparatively little written about how to actually implement cyber security – specifically, who should actually do what. There also tends to be an assumption made that cyber security is simply something that the networking group will take care of, and is therefore put out of mind by most users and IT professionals. In this paper, we examine some of the suggested best practices for cyber security and suggest a framework for thinking about these practices. We also examine how cyber security tasks can be broken out by area of responsibility within an organization.

Keywords: security; cyber security; best practices.

1. INTRODUCTION

Information security has been a hot topic in the popular press, with revelations about the NSA's various programs (Gorman, 2008) and data breaches at large retailers in the US (Rawlings, 2013) being covered extensively. There has been an increasing level of interest on the topic, as the general public has realized that their data is, in fact, at risk in these types of incidents.

Information security, however, is a broad term that covers a wide range of topics and areas. One area receiving increased focus has been cyber security. Cyber security is a sub-set of information security that focuses specifically on those computing devices that are connected to the network, and how to secure them. Cyber Security is, without a doubt, one of the most critical aspects of the computer information systems world today. However, questions inevitably arise as to how to go about providing cyber security. For instance, how does one know what to protect? How does one go about determining how to protect one's information and information assets? What kinds of measures, both technological and human, must be taken to safeguard both presence in and access to (and from) the Internet? How does one even know where to begin to do so effectively yet affordably and manageably?

In at least partial response to these "how to" questions, many standards and advisory bodies exist today. These organizations provide full

'bodies of knowledge' that enable organizations of almost any size and type to defend their information and systems, while operating in cyberspace. However, these bodies are all separate organizations, and incorporate entirely separate systems of thought and operation, oftentimes embodied in large volumes of guidelines, standards, and recommendations. In addition, these standards and recommendations are not presented in any type of standard format, leading to confusion for those trying to implement cyber security policies.

The purpose of this paper is to try to bring these various sets of best practice recommendations for cyber security together into a more approachable format for both practitioners and researchers in this field.

2. LITERATURE REVIEW

Information security is a very broad area of research, spanning any number of sub branches. The purpose of this paper is not to review and summarize every possible area of information security. Rather, this paper focuses specifically on aspects of cyber security. This choice was made to narrow the field of study to one that was both manageable and applicable for both researchers and practitioners. Recent reports of cyber-attacks against major retailers in the United States have emphasized the need for work in this area.

Cyber Security

There is surprisingly little academic research in the area of cyber security. This is likely because most of the focus in this area has been on the practical "how to" aspects of the field, rather than any sort of theoretical justification for performing certain tasks. This is an area that needs to be addressed, and we have presented some thoughts in the closing section of the paper on this.

While there is little academic research in the area, there are many practitioner articles and textbooks available (e.g. (Whitman & Mattord, 2010)). The attention to cyber security in industry press is understandable, as it has been called out as critical by heads of the NSA and CIA in the United States (Panchak, 2014). There are also frameworks dedicated to information security broadly, with applications to cyber security that are examined here.

Some of the notable frameworks in this area are the Control Objectives for Information and Related Technology (COBIT), the Information Technology Infrastructure Library (ITIL) and the ISO/IEC 17799 standards for Information Security Management (Saint-Germain, 2005).

COBIT is a framework for managing enterprise IT created and managed by the Information Systems Audit and Control Association (ISACA) and, as such, goes well beyond just information security. COBIT does have specific modules that deal with Information Security, Assurance and Risk (ISACA, 2014), and the framework is used extensively in industry (Turner, Oltsik, & McKnight, 2008).

The ISO/IEC 17799 standards are set by the International Organization for Standardization (ISO), and are the most complete framework available for information security management (Saint-Germain, 2005). The overall goal of the standards is to give companies standards for information security to allow them to comply with various regulations, and to allow them to create security that can be audited.

ITIL was originally developed by the British government to manage the IT resources for that nation. Since then, it has developed into an approach for aligning information systems services with the business processes they support. While it is not focused specifically on information systems security, security of information is one of the components for the framework.

In addition to these formal bodies of knowledge, there are other cyber security guidelines that are issued by companies like Invensys and Symantec's IT Policy Compliance Group. Each of these groups have different suggestions, but they all relate to cyber security. A summary of their recommendations is presented in the table found in Appendix 1.

The table shows a compilation of very specific steps that organizations and individuals can take to implement cyber security measures. This is to be expected as many of these cites are based on practical experience, and an analysis of security breaches in the public domain. As you can see from the citations in the table, many of their recommendations are overlapping, but are unstructured so that they are easily approachable from a research, or practice standpoint.

3. MAKING SENSE OF CYBER SECURITY

The literature review found a large number of cyber security best practices from numerous sources. What it did not find was a way to organize these items into an approachable list of best practices (see Appendix A for list). In this section, we will present two ways of organizing and approaching these best practices.

Area of Threat

While the list of possible actions to take to ensure some level of cyber security is broad, it is possible to organize and examine them in a logical way. For this paper, we have taken the approach of examining the policies, procedures and technology affected by the specific recommendations. After reviewing the best practices, we have broken them down by Hardware (HW), Software (SW), Antivirus (AV), Network (NW) and finally People, Policies and Procedures (P3).

Item	Best Practice	Tech Type
1	Inventory of Authorized and Unauthorized Devices	HW
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
7	Wireless Device Control	HW
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
23	Physical Facilities Security	HW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 2 – Hardware related best practices

We chose this method for several reasons. First, it provides a grouping for the best practices that naturally follows the breakdown of tasks in both industry and education for approaching technology. This, in turn, allows us to focus on how to approach the implementation or teaching of these best practices. This also has allowed us to reduce the best practices list down to manageable pieces. The original list of 30 is more than a little unwieldy – breaking it down by area makes it much more approachable. We have kept the item numbering the same as in Appendix A to make it easier to refer between the tables. There are a number of the best practices that reach across the different distinctions. For example, Information System Security Systems Design and Planning deals with multiple technology types including hardware, software, network, and people, policies and procedures. The best practices for Hardware are shown in table 2.

Many times when the topic of security arises the focus is on the user and what the user interacts with, i.e. applications. However, hardware plays a critical role in security and should be examined more closely as a tool for cyber security (Smith, 2004). Hardware includes various devices used within an organization that may be affected by cyber threats. Ensuring security of hardware devices is critical as this includes workstations and laptops containing organizational data as well as servers potentially containing customer data.

It is interesting to note that implementing hardware security is not simply configuring the hardware for access control – actually controlling the location of the hardware plays a role as well. Making sure that devices are physically secured (#23) plays a part. This is, obviously, made significantly more difficult due to the proliferation of mobile devices like smart phones that have enormous computing power, and incredible portability.

Security for hardware goes beyond how it is used. Security must be taken into account when hardware is being designed and built as well. There is a stream of research on how to design in security from the beginning with hardware (Smith, 2004). Clearly this isn't something that the average user will know about, but hardware plays a critical role in security and should be examined more closely as a tool for cyber security.

Table 3 shows the best practices that are related to software. Once again, the item numbering is the same as on the original table to facilitate comparisons between the different tables.

Some of these software best practices are items that are recommended for everyone (#8 Data Recovery – everyone should have a backup!), while others are oriented towards security professionals. This list again shows that there is a range of tasks that need to be done to secure software.

Item	Best Practice	Tech Type
2	Inventory of Authorized and Unauthorized Software	SW
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3
8	Data Recovery Capability	SW
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 3 – Software Related Best Practices

One of the things that these cyber security best practices for software shows is that we need to build these security practices into the software while it is being built. We believe that this is important both for practitioners and educators. The practitioners need to create software with security in mind. Educators need to teach students to think about security when building software.

Table 4 shows the networking related best practices for cyber security. Not surprisingly, this list is longer than it was for either hardware or software.

Security surrounding networks at organizations tend to be the primary focus of cyber security discussions. This is because attacks on networks tend to be the most publicized. Thus, as networks are at the heart of cyber space, their configuration plays a critical role in cyber security as well. Many of the recommendations for the networks deal with testing and remediation of issues for the network. This is to be expected as these threats evolve over time, and can change as hackers find new ways to breach security.

Item	Best Practice	Tech Type
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	NW
11	Limitations and Control of Network Ports, Protocols, and Services	NW
12	Controlled Use of Administrative Privileges	NW, P3
13	Boundary Defense	NW
19	Secure Network Engineering	NW
20	Penetration Tests and Red Team Exercises	AV, NW, P3
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 4 – Network related best practices

Table 5 shows the People Policies and Procedures best practices for cyber security. This is, by far, the longest list. What is interesting is that this seems contrary to expectations. Most people tend to focus on technology when cyber security is mentioned. However, when best practices are reviewed, it is policies and procedures that are most common.

This actually goes to something that has been noted in earlier research on security in general – your people are the weakest link (Ames, 2013). While part of this can be attributed to education and training for users, it also emphasizes the need for policies to be in place for enforcement. For example, many users continue to use weak passwords, despite the increase risk from hacking (Rashid, 2011), even though they are told not to. While we can't keep users from always doing this, we can put policies in place that force users to choose more secure passwords.

Item	Best Practice	Tech Type
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3
9	Security Skills Assessment and Appropriate Training to Fill Gaps	P3
12	Controlled Use of Administrative Privileges	NW, P3
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	P3
15	Controlled Access Based on the Need to Know	P3
16	Account Monitoring and Control	P3
18	Incident Response and Management	P3
20	Penetration Tests and Red Team Exercises	AV, NW, P3
21	Information System Security Systems Design and Planning	HW, SW, NW, P3
22	Top-Down Implementation is Essential	P3
23	Physical Facilities Security	HW, P3
24	Combine Major Cyber Security Frameworks	P3
25	Centralized InfoSec Design, Planning & Implementation	P3
26	InfoSec Department Separated from IT Department	P3
27	InfoSec Department Reports Directly to CISO	P3
28	Compliance with All Required or Applicable Regulations	P3
29	InfoSec Implementation must be Consistent w. the Organization's Culture	P3
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3

Table 5 – People, Policies and Procedures best practices.

Level of Implementation

While breaking out the best practices by area of impact is useful, it highlights something else about the best practices. Having a secure company requires the efforts of every employee. After all, it only takes a single person clicking on a malicious link to compromise security. However, these best practices are clearly not going to be approachable by everyone. For example, how likely is it that an individual will run penetration testing on their home network?

This leads us to a second way of approaching the best practices: By level of implementation. Specifically, is this something that individuals should realistically be concerned with doing? Or is this something that would require trained professionals? We present a suggested breakdown at two levels. The first is at the individual level (what should each person do) in table 6. The second is at the organizational level in table 7.

Individual	
Item	**Best Practice**
5	Malware Defenses
6	Application Software Security
7	Wireless Device Control
8	Data Recovery Capability
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
15	Controlled Access Based on the Need to Know

Table 6 – Individual Level best practices

Many best practices for cyber security are suggested across multiple levels making it difficult for the layman user to understand what he/she should implement. While not everyone is a technical expert, everyone who has devices that connect to the internet is impacted by concerns with cyber security. This was the mindset that the authors used when trying to determine which best practices could reasonably be implemented by individuals.

For example, as most best practices would suggest, everyone should be running antivirus and antimalware software (practice #5) and you should always keep your software patched and up to date (practice #6). In addition, users should run frequent backups (#8), make sure their home wireless network are password protected (# 7 and 10) and passwords are not

Organization	
Item	**Best Practice**
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
4	Continuous Vulnerability Assessment and Remediation
9	Security Skills Assessment and Appropriate Training to Fill Gaps
11	Limitations and Control of Network Ports, Protocols, and Services
12	Controlled Use of Administrative Privileges
13	Boundary Defense
14	Maintenance, Monitoring, and Analysis of Security Audit Logs
16	Account Monitoring and Control
17	Data Loss Prevention (DLP)
18	Incident Response and Management
19	Secure Network Engineering
20	Penetration Tests and Red Team Exercises
21	Information System Security Systems Design and Planning
22	Top-Down Implementation is Essential
23	Physical Facilities Security
24	Combine Major Cyber Security Frameworks
25	Centralized InfoSec Design, Planning & Implementation
26	InfoSec Department Separated from IT Department
27	InfoSec Department Reports Directly to CISO
28	Compliance with All Required or Applicable Regulations
29	InfoSec Implementation must be Consistent w. the Organization's Culture
30	Maximize Use of Automation in InfoSec Implementations

Table 7 – Organizational level best practices

lying around as well as access to files are limited to the user (#15). This provides a very reasonable list that even individuals without extensive technical knowledge can perform on most modern operating systems fairly easily. If each individual followed these practices, there will be fewer security breaches at organizations, and fewer horror stories from users. Many of the other practices, however, are best left to the experts.

It should be noted that the assumption made here is that if the individuals should be doing it, then the organizations should as well. Thus, table 7 represents those best practices that should be implemented by organizations. Here, the authors tried to divide out those practices that were identified that should be done, but that are not reasonable to assume an individual user could or should do. While it is reasonable to assume that a large organization would audit their security procedures to ensure compliance with regulations (#28), it's probably not reasonable to assume that an individual could do this.

As noted in the previous section, many of these best practices are policies and procedures that the organization should put into place. This is to be expected, but it also is indicative of a need within organizations to have someone or some group that is responsible for creating these policies and monitoring their implementation. While this has been a constant recommendation, the sheer number of cyber security failures that make the news indicates that it is not a suggestion that is always followed by organizations.

4. CONCLUSIONS AND FUTURE RESEARCH

This article has pulled together suggested cyber security best practices from multiple sources and given two possible frameworks to examine them in. It is believed that this gives both researchers and practitioners a good base to build on when either teaching or implementing cyber security programs.

While conducting this research, we noticed a few gaps in the cyber security literature. One of the current gaps in cyber security research is that there is no theoretical basis on which to build upon. The research in this area has, to date, been primarily applied. While this makes sense, as cyber security is a very applied area, we also believe that this creates a problem for research in the area.

We believe that this is something that should be addressed by future research: the creation of a theoretical base for cyber security research to build on. This theoretical base could potentially be used to help organizations understand which cyber security practices would be most applicable to them. In the current research, we have provided a framework to categorize many of the best practices provided by practitioners.

Also, while this paper has presented a dividing line between organizations and individuals in this paper, additional refinement is required. After all, high net worth individuals, or those in great positions of responsibility, would likely need to implement additional security measures beyond the suggested individual measures presented here. Further research should be done to develop more of a "sliding scale" approach to determining when a given best practices should be put into place both for individuals and for organizations. This could potentially be linked with the theoretical basis for research that was mentioned earlier, thus providing theoretical justification for the sliding scale.

5. REFERENCES

Ames, J. (2013). Cyber security: Lawyers are the weakest link. [Article]. Lawyer, 27(44), 1-1.

Gorman, S. (2008). NSA's Domestic Spying Grows As Agency Sweeps Up Data. [Article]. Wall Street Journal - Eastern Edition, 351(57), A1-A12.

Invensys. (2012). Cyber Security Best Practices. Retrieved June 4, 2014, from http://iom.invensys.com/EN/pdfLibrary/ServicesProfile_Invensys_CyberSecurityBestPractices_06-12.pdf

ISACA. (2014). COBIT 5. Retrieved June 4, 2014, from https://cobitonline.isaca.org/about

Nicho, M. E. (2013). An Information Governance Model for Cyber Security Management. In D. Mellado, L. E. Sanchez, E. Fernandez-Medina & M. Piattini (Eds.), Cyber Security Governance Innovations: Theory and Research (pp. 155-185): AISPE.

Ortbal, J. (2010). Best Practices for Managing Information Security. ITpolicycompliance.com, 22. Retrieved from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-best_practices_for_managing_information_security-february_2010_OR_2876547.en-us.pdf

Panchak, P. (2014). American CyberSecurity is a Big, Dangerous Deal for Business, IndustryWeek.

Rashid, F. Y. (2011). Password Security Remains the Weakest Link Even After Big Data Breaches. [Article]. eWeek, 28(11), 38-39.

Rawlings, N. (2013). Data Breach at Target Impacts Up to 40 Million Customers. [Article]. Time.com, 1-1.

Rembiesa, B. (2013). How to reduce IT security risk with IT asset management. Retrieved June 4, 2014, from http://searchsecurity.techtarget.com/tip/How-to-reduce-IT-security-risk-with-IT-asset-management

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. The Information Management Journal, 39(4), 6.

Smith, S. (2004). Magic Boxes and Boots: Security in Hardware. [Article]. Computer, 37(10), 106-109.

Team, V. R. (2013). 2013 Data Breach Investigations Report. 63. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Turner, M. J., Oltsik, J., & McKnight, J. (2008). Security Management Survey: ISO, ITIL and COBIT Triple Play Fosters Optimal Security Management. Retrieved June 4, 2014, from http://www.bsmreview.com/security_best_practice_survey.shtml

Whitman, M. E., & Mattord, H. J. (2010). Management of Information Security (3rd ed.). Boston, MA: Course Technology.

Appendix

Item	Best Practice	Cite
1	Inventory of Authorized and Unauthorized Devices	(Rembiesa, 2013)
2	Inventory of Authorized and Unauthorized Software	(Team, 2013)
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	(Rembiesa, 2013; Team, 2013)
4	Continuous Vulnerability Assessment and Remediation	(Invensys, 2012; Ortbal, 2010; Saint-Germain, 2005; Team, 2013)
5	Malware Defenses	(Invensys, 2012; Team, 2013)
6	Application Software Security	(Rembiesa, 2013; Team, 2013)
7	Wireless Device Control	(Rembiesa, 2013)
8	Data Recovery Capability	(Nicho, 2013; Team, 2013)
9	Security Skills Assessment and Appropriate Training to Fill Gaps	(Rembiesa, 2013; Team, 2013)
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	(Invensys, 2012; Team, 2013)
11	Limitations and Control of Network Ports, Protocols, and Services	(Invensys, 2012; Team, 2013)
12	Controlled Use of Administrative Privileges	(Saint-Germain, 2005; Team, 2013)
13	Boundary Defense	(Team, 2013)
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	(Invensys, 2012; Team, 2013)
15	Controlled Access Based on the Need to Know	(Rembiesa, 2013; Team, 2013)
16	Account Monitoring and Control	(Team, 2013)
17	Data Loss Prevention (DLP)	(Invensys, 2012; Team, 2013)
18	Incident Response and Management	(Saint-Germain, 2005; Team, 2013)
19	Secure Network Engineering	(Team, 2013)
20	Penetration Tests and Red Team Exercises	(Team, 2013)
21	Information System Security Systems Design and Planning	(Saint-Germain, 2005)
22	Top-Down Implementation is Essential	(Saint-Germain, 2005)
23	Physical Facilities Security	(Saint-Germain, 2005; Team, 2013)
24	Combine Major Cyber Security Frameworks	(Nicho, 2013; Turner, et al., 2008)
25	Centralized InfoSec Design, Planning & Implementation	(Ortbal, 2010)
26	InfoSec Department Separated from IT Department	(Ortbal, 2010)
27	InfoSec Department Reports Directly to CISO	(Ortbal, 2010)
28	Compliance with All Required or Applicable Regulations	(Saint-Germain, 2005; Turner, et al., 2008; Whitman & Mattord, 2010)
29	InfoSec Implementation must be Consistent w. the Organization's Culture	(Nicho, 2013; Ortbal, 2010)
30	Maximize Use of Automation in InfoSec Implementations	(Ortbal, 2010)

Table 1 – Summary of Cyber Security Best Practices