Applying a Security Compliance Framework to Prepare Your Organization for Cyberwarfare and Cyberattacks

William F. Slater, III

January 14, 2013

Disclaimer

William F. Slater, III is an IT Security consultant who lives and works in Chicago, IL, United States of America. He has worked in Information Technology since 1977. In March 2013, he will complete his third graduate degree, an M.S. in Cybersecurity. Though he has prior experience as a computer systems staff officer serving at Strategic Air Command Headquarters from 1977 to 1980, and as an civilian IT service management Project Manager working with the U.S. from 2009 to 2010, and he has had a top secret clearance (1977 – 1980) and a secret clearance (2009 – 2011), he did not access any classified documents from the U.S military or the U.S. government to research and write this paper. This paper is therefore, is an unclassified document that was researched and written using resources that are available to the general public. Other information reflected in this paper is the professional opinion of Mr. Slater, who is solely responsible for the content of this paper.

Finally, Mr. Slater is a very patriotic American who always hopes for the best for the Republic of the United States of America and her Allies. This includes trying to do what is in his power as an IT professional, an educator, and a writer to make the use of Cyberspace and the Internet safe for everyone.

Introduction

On Monday, CNN posted a web article with this headline, ***Nations Prepare for Cyberwar,*** describing the inevitability of a cyberwar that is coming or is possibly already here (Goldman, 2013).

One of the main disadvantages of the hyper-connected world of the 21st century is the very real danger that countries, organizations, and people who use networks computer resources connected to the Internet face because they are at risk of cyberattacks that could result in anything ranging from denial service, to espionage, theft of confidential data, destruction of data, and/or destruction of systems and services. As recognition of these dangers, national leaders, business leaders, and the military leaders of most modern countries are now acknowledging that the potential and likely eventuality of cyberwar is very real. This article will introduce come concepts about the realities and weapons of cyberwarfare and discuss how an organization can use a security compliance framework of controls to mitigate the risks of cyberattacks and cyberwarfare.

The Simple Truths of this Article

1. Cyberwar is coming or could be already here. All the signs and news media coverage and publicly known actions of the U.S. Government confirm it

2. If you use have an IT infrastructure that is important to your business operations, you need to protect your business from Cyberattacks and Cyberwarfare

3. There are many things you can do, and things you cannot legally do if you are in the United States, to protect your business from Cyberattacks and Cyberwarfare.

Restrictions inside the U.S. Code, Title 10, and other various cyber legislation strictly prohibit retaliation or going on the offensive. But you can prepare and protect yourself from cyberattacks.

4. In any organization, Management Support is required to understand and allocate the resources to defend against cyberattacks.

5. Understanding risk identification, threats, vulnerabilities, controls, performing risk assessment, and risk management are essential to becoming an effective protector of IT assets.

6. Because of the complex nature of most IT infrastructures and assets and how they integrate with an organization's business operations, it is better to use some type of proven framework with which to assure that all the important aspects of compliance and infrastructure security have meet address and are being measured.

Cyberwar Concepts

Cyberattacks and cyberwarfare tactics, by some expert estimates, date back to the early 1980s when there was a set of suspicious explosions that were likely generated in control systems on some pipelines in Asia, though this has never been conclusively confirmed. However, the idea of using computers and software to attack another entity via networks dates back to the early 2000s and by some accounts, well before that. The diagram from Lewis University shows a brief graphic history between 2000 and 2009.

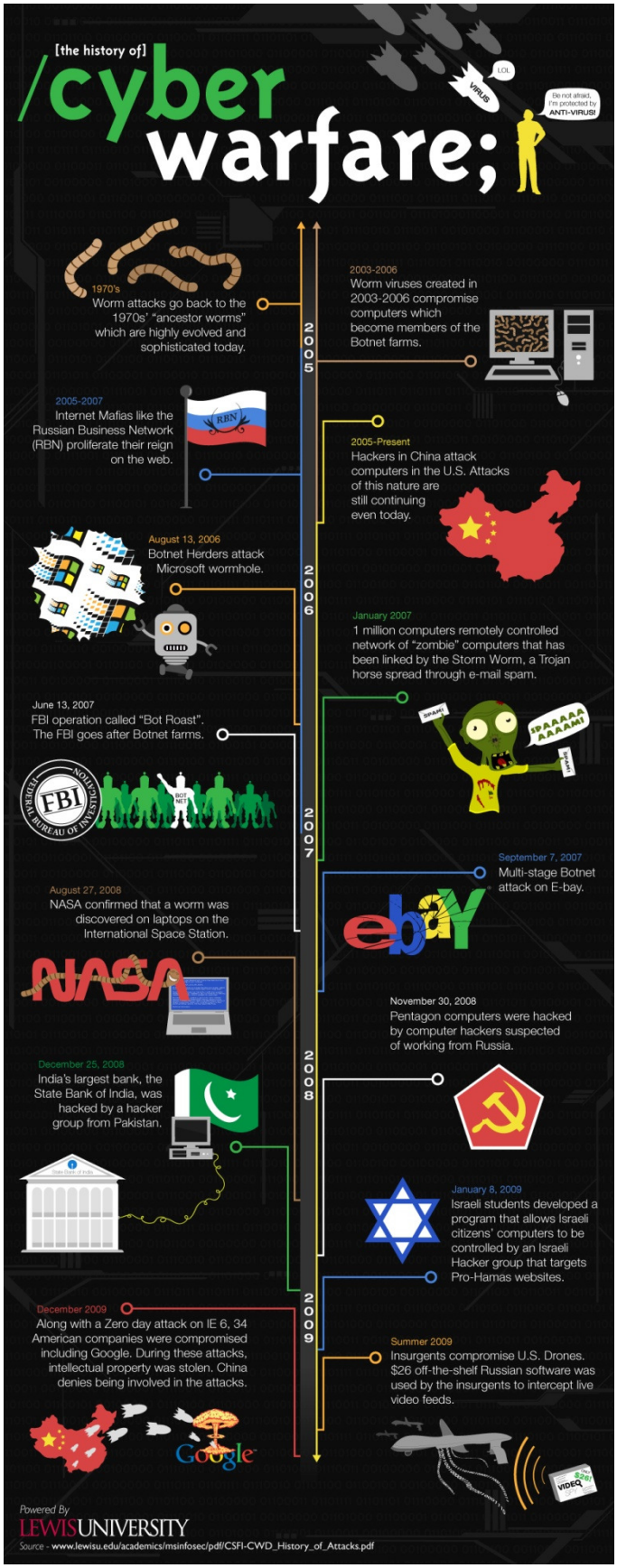
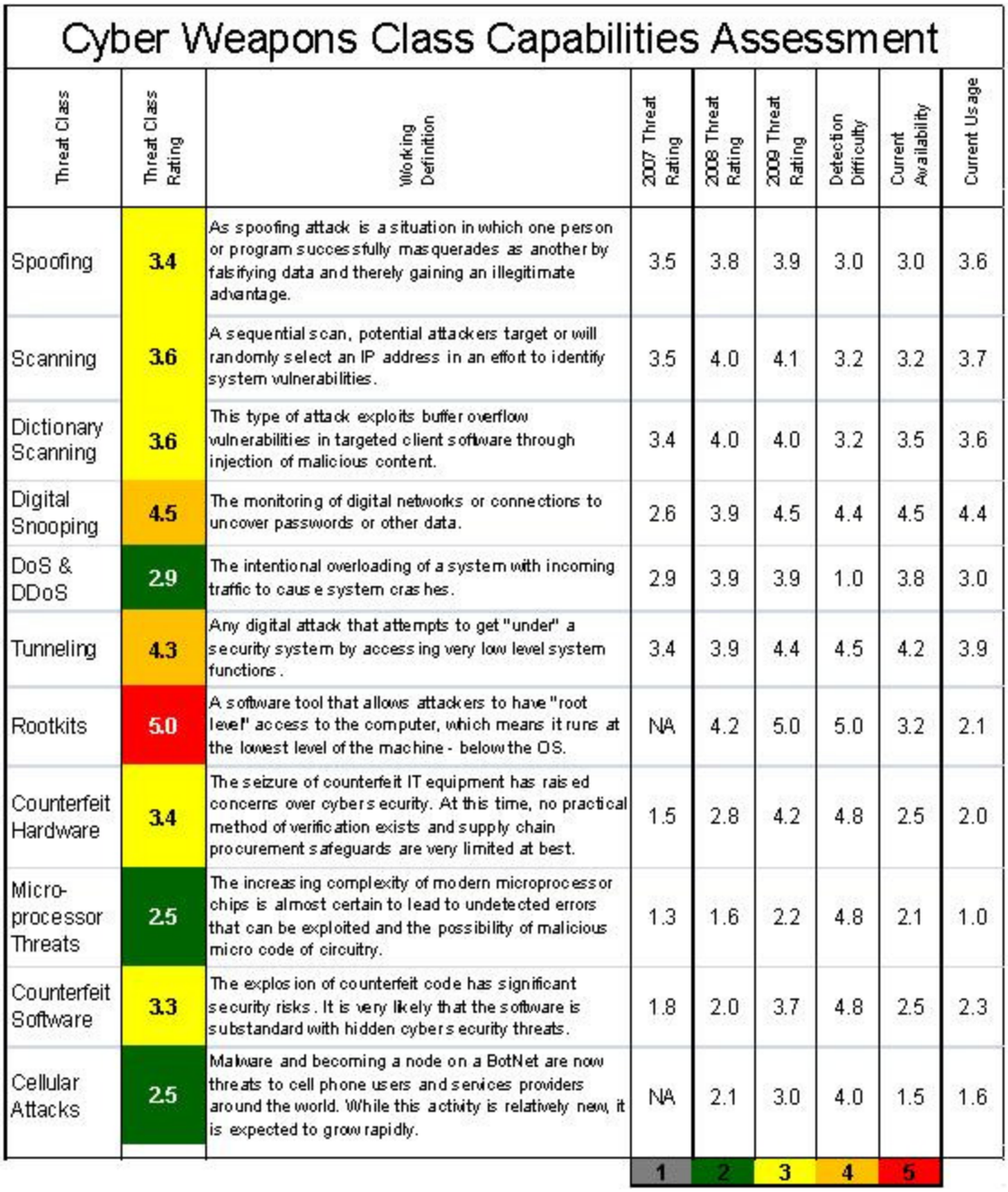


Figure 1 – A Brief History of Cyberwarfare by Lewis University, Romeoville, IL

Cyberweapons That We Know About

Cyberattacks and cyberwarfare tactics have typically been in the realm of Distributed Denial of Service (DDoS) attacks with some more sophisticated attacks as shown in the Technolytics diagram below.



Cyber Weapons Class Capabilities Assessment

Threat Class	Threat Class Rating	Working Definition	2007 Threat Rating	2008 Threat Rating	2009 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Spoofing	3.4	As spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	3.5	3.8	3.9	3.0	3.0	3.6
Scanning	3.6	A sequential scan, potential attackers target or will randomly select an IP address in an effort to identify system vulnerabilities.	3.5	4.0	4.1	3.2	3.2	3.7
Dictionary Scanning	3.6	This type of attack exploits buffer overflow vulnerabilities in targeted client software through injection of malicious content.	3.4	4.0	4.0	3.2	3.5	3.6
Digital Snooping	4.5	The monitoring of digital networks or connections to uncover passwords or other data.	2.6	3.9	4.5	4.4	4.5	4.4
DoS & DDoS	2.9	The intentional overloading of a system with incoming traffic to cause system crashes.	2.9	3.9	3.9	1.0	3.8	3.0
Tunneling	4.3	Any digital attack that attempts to get "under" a security system by accessing very low level system functions.	3.4	3.9	4.4	4.5	4.2	3.9
Rootkits	5.0	A software tool that allows attackers to have "root level" access to the computer, which means it runs at the lowest level of the machine - below the OS.	NA	4.2	5.0	5.0	3.2	2.1
Counterfeit Hardware	3.4	The seizure of counterfeit IT equipment has raised concerns over cybersecurity. At this time, no practical method of verification exists and supply chain procurement safeguards are very limited at best.	1.5	2.8	4.2	4.8	2.5	2.0
Micro-processor Threats	2.5	The increasing complexity of modern microprocessor chips is almost certain to lead to undetected errors that can be exploited and the possibility of malicious micro code of circuitry.	1.3	1.6	2.2	4.8	2.1	1.0
Counterfeit Software	3.3	The explosion of counterfeit code has significant security risks. It is very likely that the software is substandard with hidden cybersecurity threats.	1.8	2.0	3.7	4.8	2.5	2.3
Cellular Attacks	2.5	Malware and becoming a node on a BotNet are now threats to cell phone users and services providers around the world. While this activity is relatively new, it is expected to grow rapidly.	NA	2.1	3.0	4.0	1.5	1.6
			1	2	3	4	5	

Figure 2 – Classes of Cyberweapon Capabilities, by Technolytics.

Since 2007, as the existence of well-orchestrated cyberwar attacks such as the DDoS attacks on Estonia (2007), Georgia (2008), and Kyrgyzstan (2009), as well as the Stuxnet (2010), Duqu (2011), and Flame (2012) have all become known to the world through security

researchers, their victims, and the media. As a result, it has become apparent most who are watching this area that cyberspace has now become the new realm onto which the field of international conflict has been extended, and that cyberwarfare is now no longer a theoretical issue that could one day threaten those participants and systems that rely upon connections to the Internet and Internet-connected networks. Unfortunately however, despite the emergence of a new breed of intelligent cyberweapons (i.e. Stuxnet, Flame, Duqu, and Shamoon) with the ability to strike with precision and accuracy, the present findings and research on cyberwarfare related events shows that the U.S. is playing catch-up and doing so badly (Turanski and Husick, 2012).

The diagram below shows the rapid evolution of cyberweapons over time. It is obvious that according to this diagram, starting in about 2008, until what is predicted to be about 2020, the evolution of the sophistication of cyberweapons will be be quite significant. This rapid rise in sophistication and capabilities of cyberweapons, coupled with their relative ease of use, proliferation and economic benefit, will make these weapons very compelling for military and strategic use, and make the likelihood of cyberwar increasingly significant for the foreseeable future.

Figure 3 – Evolution of Cyberweapon Capabilities, 1994 - 2020, by Technolytics.

Who Is the "Enemy" or the "Adversary?"

In the world of cyberattacks and cyberwarfare, the issue of who your adversary usually depended on your perspective. From the perspective of the U.S. and its allies, the adversary usually falls into one of these five categories: Russia, China, North Korea, Iran, or non-state actors. Much is already known about our potential adversaries, such as Russia, China, North Korea and Iran, but what is perhaps less understood is the degree to which they have been successful in integrating cyberwarfare and cyberdeterrence capabilities into their own national war plans. Nevertheless, due to the previous extensive experience of China, Russia and the U.S. with strategic war planning, it is more likely that each of these countries stand the greatest

chance of making integrating cyberwarfare and cyberdeterrence capabilities into their respective war plans. Yet, as far back as June 2009, it was clear that the U.S. and Russia were unable to agree on a treaty that would create the terms under which cyberwarfare operations could and would be conducted (Markoff, J. and Kramer, A. E., 2009).

DDoS as a Service, as low as US$20 Per Hour

We now live in a world where the Internet and malware have made it possible to buy services such as DDoS attacks against an enemy or a competitor for prices as low as $20 hour. When you consider the implications of this idea, the economic will make the idea of tactical cyberattacks more appealing to organizations. I know some of the URLs where these services are available, but rather than give them advertisement, I would just invite you to do an Internet search using your favorite search engine.

Understanding Risks and Threats and Vulnerabilities

To deal with the realities of cyberattacks and cyberwar, one must grasp a few simple concepts related to risk quantification, risk assessment, and risk management. Risk in the world of Information Technology is a calculation of the likelihood of an undesirable event based on the estimated severity of impact when the event occurs, the probability of the event's occurrence, and the ability to detect the event should it actually occur. Usually risk is usually explained and understood in terms of threats and vulnerabilities, and damages to assets. Risk is important to understand because risk reduction is usually accomplished by the application of one or more controls.

Examples of assets that could be impacted by risk in an organization include:

- Physical
- People
- Information (including documentation, strategy, business model, etc.
- Data and Databases
- Organization
- Websites
- Systems
- Servers, Computers, Network Infrastructure components, etc.
- Intangibles (brand, reputation, etc.)
- Services (Including power, cooling, backup power, and services provided to clients)

In addition, in the world of IT, you usually have four basic strategies to manage risk once it has been identified and assessed:

1. Mitigate it
2. Transfer it
3. Avoid it
4. Ignore it

I have included some diagrams to help readers understand the relationships between risk, vulnerabilities, threats, assets and controls that reduce risk.

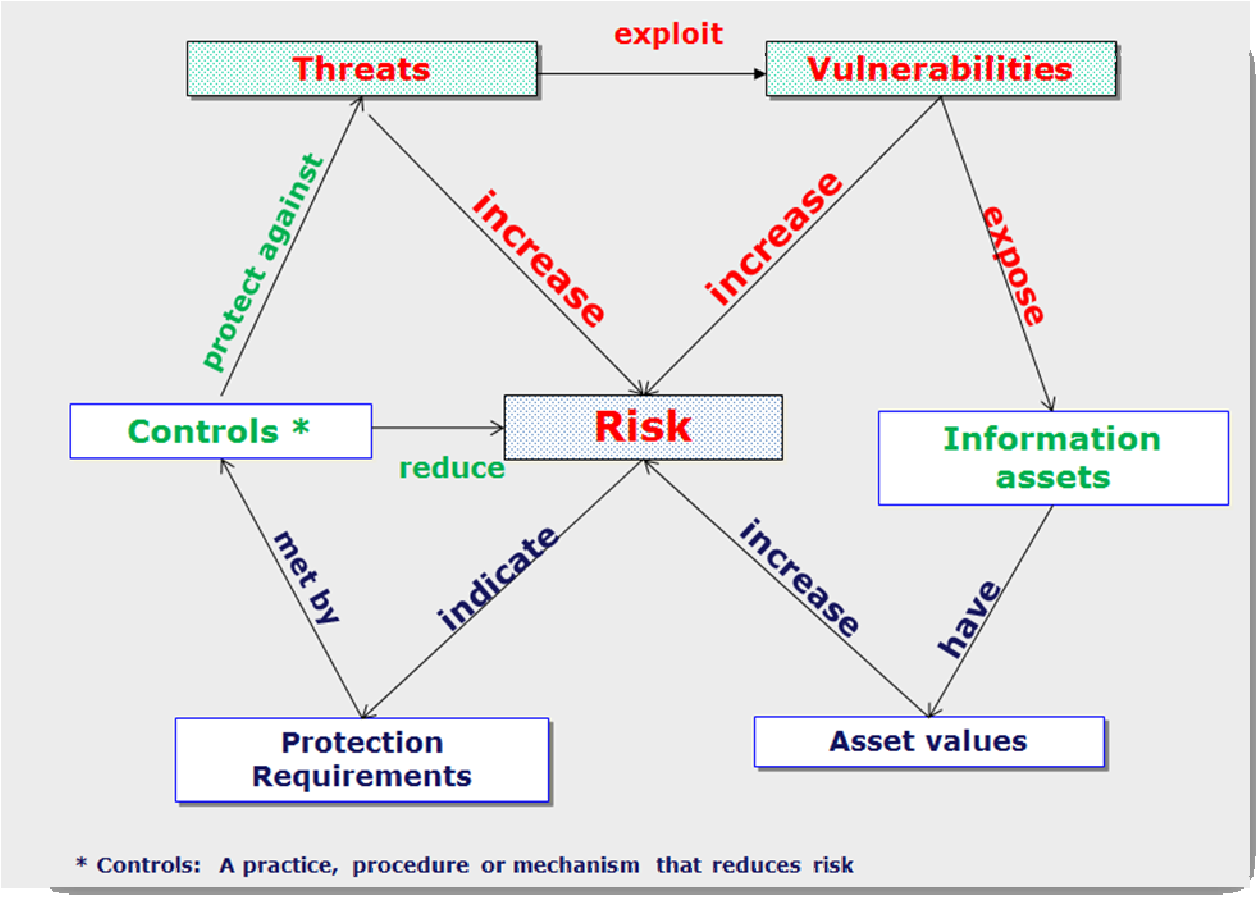


Figure 4 – Risk relationship diagram, from ISO27001.org.

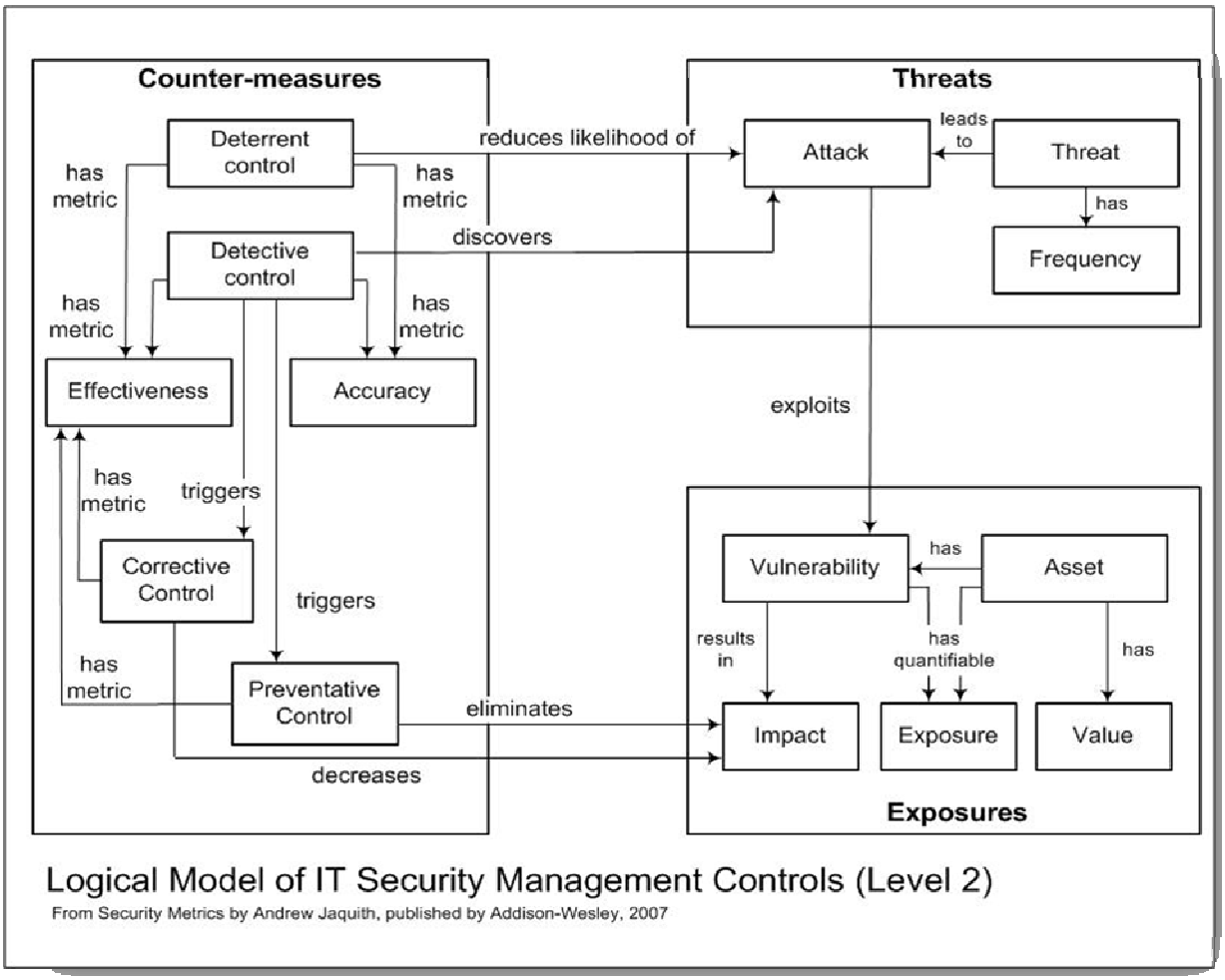


Figure 5 – Relationships between IT security management controls, Threats and Assets (Exposures), Jaquith, 2007

What Is an ISMS?

The fast-paced, electronically-enabled business environment of the 21st century is characterized by the tactical and strategic uses of information as business enablers. In practically every organization, information is now seen as a primary asset and as such, it must be protected. Yet the proliferation and reliance on information in an organization also introduces responsibilities and risks which if not addressed, can subject the organization to extraordinary

risks that could severely impact the viability of the business. The best strategy for an organization to manage these new business realities is to adopt a strong compliance management posture in the area of Information Security to ensure that its information assets are protected in the most comprehensive, standardized manner possible. Presently, the best tool to manage the challenges of Information Security is an enterprise Information Security Management System (ISMS). The ISMS is a centralized system of policies, procedures, and guidelines that when created and uniformly applied will provide the best practices to help ensure that an organization's Information Security is being managed in a standardized way using documented best practices. The introduction of an ISMS into an organization's business operations will serve to identify, document and classify information assets and risks and then document the mitigation of risks using established, documented controls. When an organization has chosen the standardized ISO 27001 Security Management Framework the key benefits to implementing an ISMS would be:

- The implementation of a standardized Information Security Management System into the organization
- Better management and fulfillment of the Information Security requirements from the organization's Clients
- Reduction of risks related to cyberattacks and cyberwarfare
- Reduction of risk of loss of existing customers
- Increased opportunities for new business
- Reduction of risk to regulatory penalties
- Reduction of risk reputational damage
- The creation of an Information Security-aware culture at the organization

- Enabling ISO27001-compliant offices to communicate and conduct business in areas affected by Information Security in a standard way
- Better management of IT assets and their associated risks
- The ability to have an Information Security Management System that is based on the Deming model of Plan – Do – Check – Act for continuous process improvement
- The adoption of the most widely recognized internal standard for implementing an ISMS

Note that the Information Security has rapidly risen to the forefront as a serious business issue. Because of its rapid rise to prominence and the dynamic and evolving nature of threats and the associated risk management efforts, the models to measure and quantify the value of such projects can often seem frustrating at best. So while this ISMS project may difficult to quantify using traditional methods such as return on investment, it is clear that the benefits of continued customer relationships as well as the ability to attract future customers through a demonstrated strong and continually improving posture of Information Security compliance management will far outweigh the costs associated with an ISO 27001project.

Indeed, after implementing the ISMS under ISO 27001 standards, an organization will have better control of the Information that is the lifeblood of its business, and it will be able to demonstrate to its customers and its business partners that it too has adopted a strong posture of compliance in the area of Information Security.

What is ISO 27001?

ISO 27001 is an international standard with 133 controls in 11 domains which provide structured standard for the creation of an Information Security Management System based on

strongly focused risk management and continuous process improvement under the Plan – Do – Check- Act model. The present version was developed in 2005 and an updated version is expected to be published by ISO sometime in 2013. This version is predicted to have several additions that will focus on Cloud Computing and also standardized IT services and service management as described under ITIL and ISO 20000. In fact, in October 2012, the ISO 27013 standard was published and it demonstrates how to integrate an ISO 2000—based Service Management System with an ISO 27001-based Information Security Management System.

What Cyberattack / Cyberwarfare Risk Remediation Project Using ISO 27001 Might Look Like

It is possible to create and implement an ISMS using a fast-track method as shown in figure 6 below. Note that management must support such a project in terms of resources (monetary, people, and assets) and politically in order for it to be successful. Nevertheless, it is possible to accomplish such a project if management and the project team have the will and resources to succeed.

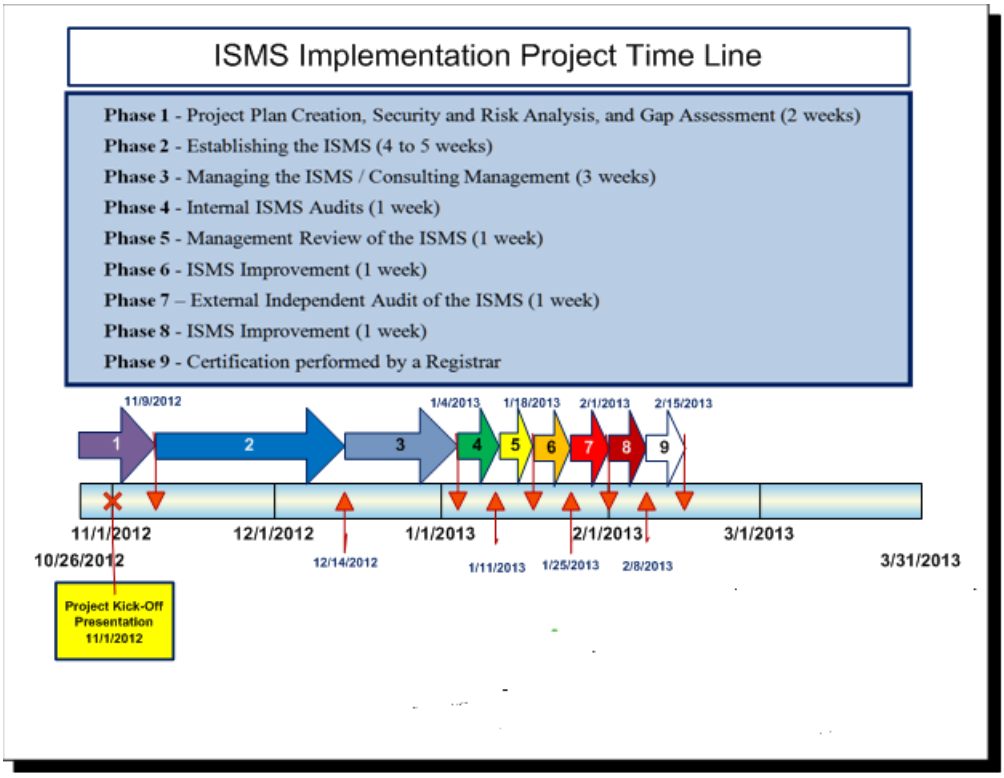


Figure 6 – A Fast-track ISMS Implementation Project Timeline, William Slater, 2012

Should You Get Your Organization Certified in ISO 27001?

Should you get your organization certified in ISO 27001 if you make the effort to remediate your cyberattack and cyberwarfare risks using an ISO 27001 ISMS control framework? The quick answer is, it depends. Currently, there are less than 9000 ISO 27001 ISMS certificate holders worldwide. Despite the apparent emphasis on security and risk reduction, quite often, organizations will pursue the ISO 27001 certification either to comply with regulatory requirements (as is required in India), or as a business enabler, because their business partners and/or customers expect it or have greater confidence in an organization that has an ISO 27001 certification. Though is not easy or inexpensive in terms of resources to earn or maintain and ISO 27001 certification, the return on investment, particularly in areas like the

North America and South America where the ISO 27001 certification is still relatively rare, can be quite significant.

Figure 7 below shows the numbers of ISO 27001 ISMS Certificate Registrants by continent as of 2011. Note that according the PECB, a certification body that trains and certifies ISO 27001 implementers and auditors, the number of ISO 27001 ISMS Certificate Registrants is expected to double each year in North America for the foreseeable future.

Figure 7 – ISO 27001 ISMS Registrants by Continent as of 2011 (source unknown)

Is Compliance with the ISO 27001 Standard or Some Other Security Compliance Framework Still Important Even If Your Organization Doesn't Get Certified?

Personally, I believe that the chief responsibility of the leadership of organization is to recognize risks and reduce them, as cost effectively as possible to manageable levels, and to comply with the laws and regulations that impact its operating environment. Even if an

organization does not seek or achieve a certification under a security compliance standard such as ISO 27001, the organization can embrace and comply with the security controls of a security compliance standard, and thereby significantly reduce its business and security risks. The value in each of these security compliance frameworks (i.e. ISO 27001, PSC DSS. FISMA, HIPAA, etc.) is that each offers a set of well defined controls that are structured in a way to allow the organization that adopts then to visibly demonstrate its efforts to reduce risks to its assets and its operating environment.

Mapping to Achieve Compliance with Two or More Security Compliance Frameworks

When an organization is required to comply with two or more security compliance frameworks, a process known as "mapping" using a table showing the similarity of various controls is used to understand and communicate the specific controls of each standard, and usually on a one to one basis. Typically, the standard that is already in place or the one that is the most familiar is represented on the left column, and the newer standard that is required for a new compliance initiative is located on the right column. An example is shown in figure 8 below.

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS *
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	SA-9, SC-8, SC-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
A.10.9.2 On-line transactions	SC-3, SC-7, SC-8, SC-9, SC-14
A.10.9.3 Publicly available information	SC-14
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12

Figure 8 – Mapping ISO 27001 Annex A controls to NIST 800-53 Controls (FISMA)

Using ISO 27001 Controls to Defend Against Cyberwarfare and Cyberattacks

Of the 133 controls defined in Annex A of the ISO 27001 standard, not all of these are required to reduce the risk of cyberattacks and cyberwarfare. However, using my knowledge of the ISO 27001 standard framework of 133 controls, and my knowledge of the various characteristics and aspects of cyberattacks and cyberwarfare, I created the table in Appendix A that can be used to understand how these various defined controls can be used to mitigate the risks associated with cyberattacks and cyberwarfare. The right-most column gives a simple yes or no to indicate the usefulness of the control in the mitigation of risks associated with cyberattacks and cyberwarfare.

Recommendations

The section has been divided into recommendations for four distinct groups of people that will probably comprise the population of this magazine's readers. I deliberately omitted government officials and military officials because they have their own elite teams of cyberwarfare experts to advise them on these issues. In addition, they have a perspective of cyberattacks and cyberwarfare in which they must consider battle plans and strategies that include both offensive and defensive operations. To best understand the true nature of cyberdeterrence and cyberwarfare, everyone would be well advised to read many of the materials in the reference section of this article, and in particular, read Martin Libicki's book, Cyberdeterrence and Cyberwar, because I consider it to be the best unclassified reference on the market.

For IT Professionals:

1. Educate yourself, continually about Cyberwarfare.
2. Stay abreast of the threats and vulnerabilities associated with your infrastructure and the information technologies that you work with.
3. Stay abreast of the security controls required to mitigate the risks associated with the information technologies that you work with.
4. Where possible, get professional training and certifications associated with IT security and your job positions.

For IT Managers:

1. Learn the security compliance standard or standards that will enable you to help your organization effectively lower risk to acceptable levels.
2. Learn risk management in the IT world.
3. Learn what your teams do and keep them motivated to be the best at what they do.

For Executives and Business Owners:

1. Remember your responsibilities to the Board of Directors, your shareholders and other stakeholders in your organization: Cyberattacks and cyberwarfare represent serious threats that can obliterate an organization's ability to function (see the 2007 cyberattacks in Estonia, or the 2008 attacks in Georgia

if you require more proof). If you plan for your organization to be an ongoing concern for the foreseeable future, you have no alternative than to ensure it is protected from cyberattacks and the effects of cyberwarfare.

2. Learn the security compliance standard or standards that will enable you to help your organization effectively lower risk to acceptable levels.
3. Learn risk management in the IT world.
4. Learn what your managers and your teams do and keep them motivated to be the best at what they do.

For Hackers:

1. Consider becoming legitimate because the need for experienced cybersecurity professionals to defend organizations and countries has never been greater and in the long run, the compensation will probably be much more lucrative.
2. Make sure that if you do join a team that it is a winning team.

Conclusions

This article has covered some of the better known aspects of cyberattacks and cyberwarfare, and attempted to show that risks can be managed by applying security compliance frameworks such as ISO 27001. While this has only been an introduction, because scores of books have been written on these topics since 2005, it is important to understand these basic concepts and take them seriously. The future of your business, the satisfaction and confidence of your stakeholders, business partners, and your customers all depend on your ability to protect your business and its operations capabilities in the day and age of cyberattacks and cyberwarfare.

Resources:

Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.

Brewer, D. and Nash, M. (2010). Insights into the ISO/IEC 27001 Annex A. A paper written published by Dr. David Brewer and Dr. Michael Nash to explain ISO 27001 and Risk Reduction in Organizations. Retrieved from http://www.gammassl.co.uk/research/27001annexAinsights.pdf on March 10, 2011.

Bush, G. W. (2008). Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House January 2008. Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on January 5, 2012.

Calder, A. and Watkins, S. (2012). IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 5th edition. London, U.K.: IT Governance Press.

Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.

Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HarperCollins Publishers.

Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf on October 10, 2012.

Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.

Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retrieved from http://www.infracritical.com/papers/nstb-2481.pdf on December 20, 2011.

Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf on September 30, 2012.

Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillan.

Gerwitz, D. (2011). The Obama Cyberdoctrine: tweet softly, but carry a big stick. An article published at Zdnet.com on May 17, 2011. Retrieved from http://www.zdnet.com/blog/government/the-obama-cyberdoctrine-tweet-softly-but-carry-a-big-stick/10400 on September 25, 2012.

Gjelten, T. (2010). Are 'Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.

Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.

Gjelten, T. (2011). Security Expert: U.S. 'Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.

Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.

Goldman, D. (2013). Nations prepare for cyber war. An article published at CNN on January 7, 2013. Retrieved from http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html?hpt=hp_c3 on January 7, 2013.

Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare. Cambridgeshire, U.K.: IT Governance.Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.

ISO. (2005) "Information technology – Security techniques – Information security management systems requirements", ISO/IEC 27001:2005. Retrieved from http://www.ansi.org on February 1, 2011.

Jaquith, A. (2007). Security Metrics. Boston, MA: Addison Wesley.

Kaplan, F. (1983), The Wizards of Armageddon: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.

Kerr, D. (2012). Senator urges Obama to issue 'cybersecurity' executive order. An article published at Cnet.com on September 24, 2012. Retrieved from http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/ on September 26, 2012.

Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.

Langer, R. (2010). A Detailed Analysis of the Stuxnet Worm. Retrieved from http://www.langner.com/en/blog/page/6/ on December 20, 2011.

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.

Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all on June 28, 2009.

Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at Poltix.Topix.com. Retrieved from http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war on September 22, 2012.

McBrie, J. M. (2007). THE BUSH DOCTRINE: SHIFTING POSITION AND CLOSING THE STANCE. A scholarly paper published by the USAWC STRATEGY RESEARCH PROJECT. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA423774 on September 30, 2012.

Obama, B. H. (2012). Defense Strategic Guidance 2012 - Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf on January 5, 2012.

Obama, B.H. (2011). INTERNATIONAL STRATEGY for Cyberspace. Published by the White House on May 16, 2011. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf on May 16, 2011.

Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.

Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.

Radcliff, D. (2012). Cyber cold war: Espionage and warfare. An article published in SC Magazine, September 4, 2012. Retrieved from http://www.scmagazine.com/cyber-cold-war-espionage-and-warfare/article/254627/ on September 7, 2012.

Saini, M. (2012). Preparing for Cyberwar - A National Perspective. An article published on July 26, 2012 at the Vivikanda International Foundation. Retrieved from http://www.vifindia.org/article/2012/july/26/preparing-for-cyberwar-a-national-perspective on October 14, 2012.

Sanger, D. E. (2012). Confront and Coneal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.

Schmidt, H. S. (2006). Patrolling Cyberspace: Lessons Learned from Lifetime in Data Security. N. Potomac, MD: Larstan Publishing, Inc.

Schmitt, E. and Shanker, T. (2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. An article published in the New York Times on October 17, 2011. Retrieved from http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html on October 17, 2011.

Slater, W. F. (2013). ISO 27001 Resource Page. Retrieved from http://billslater.com/iso27001 on January 12, 2013.

Stiennon, R. (2010). Surviving Cyber War. Lanham, MA: Government Institutes.

Strohm, C. and Engleman, E. (2012). Cyber Attacks on U.S. Banks Expose Vulnerabilities. An article published at BusinessWeek.com on September 28, 2012. Retrieved from http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability on September 30, 2012.

Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.

The ISO 27000 Directory. (2012). An Introduction to ISO 27001, ISO 27002....ISO 27008. Retreived from http://www.27000.org/index.htmhttp://idcontent.bellevue.edu/content/CIT/cyber/615/compliance on December 7, 2012.

Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html on October 25, 2012.

U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf on November 3, 2012.

U.S. Department of Defense, JCS. (2006). Joint Publication (JP) 5-0, Joint Operation Planning, updated on December 26, 2012. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf on October 25, 2012.

Waters, G. (2008). Australia and Cyber-Warfare. Canberra, Australia: ANU E Press.

Appendix A – ISO27001 Domains, Control Objectives and Controls

ISO 27001:2005 Controls			
Clause	**Section**	**Control Objective/Control**	**Does It Apply to Defending Against Cyberattacks and Cyberwarfare?**
Security Policy	**5.1**	**Information Security Policy**	
	5.1.1	Information Security Policy Document	**Yes**
	5.1.2	Review of Information Security Policy	**No**
Organization of Information security	**6.1**	**Internal Organization**	
	6.1.1	Management Commitment to information security	**Yes**
	6.1.2	Information security Co-ordination	**No**
	6.1.3	Allocation of information security Responsibilities	**Yes**
	6.1.4	Authorization process for Information Processing facilities	**No**
	6.1.5	Confidentiality agreements	**No**
	6.1.6	Contact with authorities	**No**
	6.1.7	Contact with special interest groups	**No**
	6.1.8	Independent review of information security	**No**
	6.2	**External Parties**	
	6.2.1	Identification of risk related to external parties	**No**
	6.2.2	Addressing security when dealing with customers	**No**
	6.2.3	Addressing security in third party agreements	**No**
Asset Management	**7.1**	**Responsibility for Assets**	
	7.1.1	Inventory of assets	**Yes**
	7.1.2	Ownership of Assets	**Yes**
	7.1.3	Acceptable use of assets	**Yes**
	7.2	**Information classification**	
	7.2.1	Classification Guidelines	**Yes**
	7.2.2	Information Labeling and Handling	**Yes**

Human Resource Security	**8.1**	**Prior to Employment**	
	8.1.1	Roles and Responsibilities	**Yes**
	8.1.2	Screening	**Yes**
	8.1.3	Terms and conditions of employment	**No**
	8.2	**During Employment**	
	8.2.1	Management Responsibility	**Yes**
	8.2.2	Information security awareness, education and training	**Yes**
	8.2.3	Disciplinary process	**No**
	8.3	**Termination or change of employment**	
	8.3.1	Termination responsibility	**No**
	8.3.2	Return of assets	**Yes**
	8.3.3	Removal of access rights	**Yes**
Physical and Environmental Security	**9.1**	**Secure Areas**	
	9.1.1	Physical security Perimeter	**Yes**
	9.1.2	Physical entry controls	**Yes**
	9.1.3	Securing offices, rooms and facilities	**Yes**
	9.1.4	Protecting against external and environmental threats	**Yes**
	9.1.5	Working in secure areas	**Yes**
	9.1.6	Public access, delivery and loading areas	**Yes**
	9.2	**Equipment security**	
	9.2.1	Equipment sitting and protection	**Yes**
	9.2.2	Support utilities	**Yes**
	9.2.3	Cabling security	**No**
	9.2.4	Equipment Maintenance	**No**
	9.2.5	Security of equipment off-premises	**Yes**
	9.2.6	Secure disposal or reuse of equipment	**Yes**
	9.2.7	Removal of Property	**Yes**
Communications and Operations Management	**10.1**	**Operational Procedures and responsibilities**	
	10.1.1	Documented operating Procedures	**Yes**
	10.1.2	Change Management	**Yes**
	10.1.3	Segregation of Duties	**Yes**

	10.1.4	Separation of development and Operations facilities	**Yes**
	10.2	**Third Party Service Delivery Management**	
	10.2.1	Service Delivery	**No**
	10.2.2	Monitoring and review of third party services	**No**
	10.2.3	Manage changes to the third party services	**No**
	10.3	**System Planning and Acceptance**	
	10.3.1	Capacity management	**Yes**
	10.3.2	System acceptance	**Yes**
	10.4	**Protection against Malicious and Mobile Code**	
	10.4.1	Controls against malicious code	**Yes**
	10.4.2	Controls against Mobile code	**Yes**
	10.5	**Back-Up**	
	10.5.1	Information Backup	**Yes**
	10.6	**Network Security Management**	
	10.6.1	Network controls	**Yes**
	10.6.2	Security of Network services	**Yes**
	10.7	**Media Handling**	
	10.7.1	Management of removable media	**Yes**
	10.7.2	Disposal of Media	**Yes**
	10.7.3	Information handling procedures	**Yes**
	10.7.4	Security of system documentation	**Yes**
	10.8	**Exchange of Information**	
	10.8.1	Information exchange policies and procedures	**Yes**
	10.8.2	Exchange agreements	**Yes**
	10.8.3	Physical media in transit	**Yes**
	10.8.4	Electronic Messaging	**Yes**
	10.8.5	Business Information systems	**Yes**
	10.9	**Electronic Commerce Services**	
	10.9.1	Electronic Commerce	**Yes**
	10.9.2	On-Line transactions	**Yes**
	10.9.3	Publicly available information	**Yes**
	10.1	**Monitoring**	
	10.10.1	Audit logging	**Yes**
	10.10.2	Monitoring system use	**Yes**
	10.10.3	Protection of log information	**Yes**
	10.10.4	Administrator and operator logs	**Yes**
	10.10.5	Fault logging	**Yes**

	10.10.6	Clock synchronization	**Yes**
Access control	**11.1**	**Business Requirement for Access Control**	
	11.1.1	Access control Policy	**Yes**
	11.2	**User Access Management**	
	11.2.1	User Registration	**Yes**
	11.2.2	Privilege Measurement	**Yes**
	11.2.3	User password management	**Yes**
	11.2.4	Review of user access rights	**Yes**
	11.3	**User Responsibilities**	
	11.3.1	Password Use	**Yes**
	11.3.2	Unattended user equipment	**Yes**
	11.3.3	Clear Desk and Clear Screen Policy	**Yes**
	11.4	**Network Access control**	
	11.4.1	Policy on use of network services	**Yes**
	11.4.2	User authentication for external connections	**Yes**
	11.4.3	Equipment identification in networks	**Yes**
	11.4.4	Remote diagnostic and configuration port protection	**Yes**
	11.4.5	Segregation in networks	**Yes**
	11.4.6	Network connection control	**Yes**
	11.4.7	Network Routing control	**Yes**
	11.5	**Operating System Access Control**	
	11.5.1	Secure Log-on procedures	**Yes**
	11.5.2	User identification and authentication	**Yes**
	11.5.3	Password Management system	**Yes**
	11.5.4	Use of system utilities	**Yes**
	11.5.5	Session Time-out	**Yes**
	11.5.6	Limitation of connection time	**Yes**
	11.6	**Application access control**	
	11.6.1	Information access restriction	**Yes**
	11.6.2	Sensitive system isolation	**Yes**
	11.7	**Mobile Computing and Teleworking**	
	11.7.1	Mobile computing and communication	**Yes**
	11.7.2	Teleworking	**Yes**
Information	**12.1**	**Security Requirements of Information Systems**	

Systems Acquisition Development and Maintenance	12.1.1	Security requirement analysis and specifications	**Yes**
	12.2	**Correct Processing in Applications**	
	12.2.1	Input data validation	**Yes**
	12.2.2	Control of internal processing	**Yes**
	12.2.3	Message integrity	**Yes**
	12.2.4	Output data validation	**Yes**
	12.3	**Cryptographic controls**	
	12.3.1	Policy on the use of cryptographic controls	**Yes**
	12.3.2	Key Management	**Yes**
	12.4	**Security of System Files**	
	12.4.1	Control of Operational software	**Yes**
	12.4.2	Protection of system test data	**Yes**
	12.4.3	Access control to program source library	**Yes**
	12.5	**Security in Development & Support Processes**	
	12.5.1	Change Control Procedures	**Yes**
	12.5.2	Technical review of applications after Operating system changes	**Yes**
	12.5.3	Restrictions on changes to software packages	**Yes**
	12.5.4	Information Leakage	**Yes**
	12.5.5	Outsourced Software Development	**Yes**
	12.6	**Technical Vulnerability Management**	
	12.6.1	Control of technical vulnerabilities	**Yes**
Information Security Incident Management	**13.1**	**Reporting Information Security Events and Weaknesses**	
	13.1.1	Reporting Information security events	**Yes**
	13.1.2	Reporting security weaknesses	**Yes**
	13.2	**Management of Information Security Incidents and Improvements**	
	13.2.1	Responsibilities and Procedures	**Yes**
	13.2.2	Learning for Information security incidents	**Yes**
	13.2.3	Collection of evidence	**Yes**
Business Continuity Management	**14.1**	**Information Security Aspects of Business Continuity Management**	
	14.1.1	Including Information Security in Business continuity management process	**Yes**
	14.1.2	Business continuity and Risk Assessment	**Yes**

	14.1.3	developing and implementing continuity plans including information security	**Yes**
	14.1.4	Business continuity planning framework	**Yes**
	14.1.5	Testing, maintaining and re-assessing business continuity plans	**Yes**
Compliance	**15.1**	**Compliance with Legal Requirements**	
	15.1.1	Identification of applicable legislations	**Yes**
	15.1.2	Intellectual Property Rights (IPR)	**Yes**
	15.1.3	Protection of organizational records	**Yes**
	15.1.4	Data Protection and privacy of personal information	**Yes**
	15.1.5	Prevention of misuse of information processing facilities	**Yes**
	15.1.6	Regulation of cryptographic controls	**Yes**
	15.2	**Compliance with Security Policies and Standards and Technical compliance**	
	15.2.1	Compliance with security policy	**Yes**
	15.2.2	Technical compliance checking	**Yes**
	15.3	**Information System Audit Considerations**	
	15.3.1	Information System Audit controls	**Yes**
	15.3.2	Protection of information system audit tools	**Yes**

(ISO, 2005)