The Economics of Cybersecurity Part II: *Extending the Cybersecurity Framework*

AFCEA Cyber Committee[1]

Background

While organizations in the United States spend an estimated $15 billion/year on cybersecurity, the economic impact of cyberattacks continues to grow to over $100 billion/year. At the 2014 World Economic Forum, McKinsey launched a new report[2] that recognized increased cybersecurity can save the global economy trillions. Michael Daniel, the President's cyber czar, recently confirmed that the economics of cyber security were out of balance favoring the attacker.[3]

Our previous paper, *The Economics of Cyber Security: A Practical Framework for Cybersecurity Investment* introduced a practical framework for guiding investment in cybersecurity. [AFCEA Cyber Committee 2013] The investment framework was based in part on the observation that the majority of damaging cyberattacks has little sophistication and documented evidence that a baseline of security controls can be effective against most of these attacks. That paper presented an easily understood graphical model that helped explain the key factors that should influence cybersecurity investment.

[1] This paper is the result of collaboration among the members of the Economics of Cybersecurity Subcommittee of the AFCEA Cyber Committee and a set of outside advisors. The principal author is John Gilligan. Other contributors include: Kenneth Heitkamp, Robert Dix, Charles Palmer, Jeffrey Sorenson, Tom Conway, Wray Varley, Gary Gagnon, Robert Lentz, Phillip Venables, Alan Paller, Jane Holl Lute and Franklin Reeder.

[2] "Risk and Responsibility in a Hyperconnected World" World Economic Forum 2014 http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf.

[3] Amber Corrin, "The economics of a national cyber immune system", http://fcw.com/Articles/2014/01/29/cyber-immune-system.aspx?s=fcwdaily_300114&Page=1

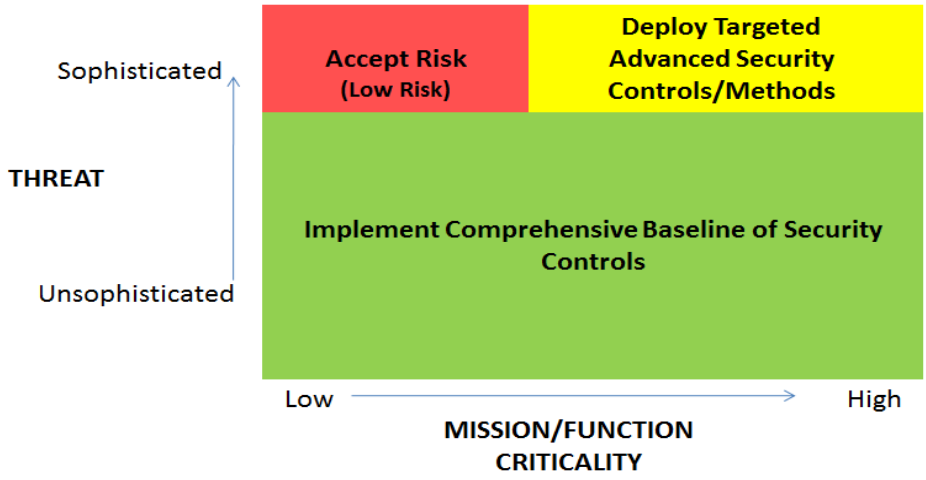

Figure 1: Cybersecurity Economic Framework

That paper also provided the following three investment principles:

Investment Principle #1: Implementation of a comprehensive baseline of security controls that address threats that are of low to moderate sophistication is essential and is economically beneficial.

Investment Principle #2: Focus security investment beyond the baseline controls to counter more sophisticated attacks against the functions and data that are most critical to an organization.

Investment Principle #3: For sophisticated attacks, an organization should accept the security risk of not protecting functions and data that are of lowest impact to the organization's mission and where cost exceeds benefits.

We concluded with the strong recommendation that organizations implement the Framework, along with a set of critical security controls such as the 20 Critical Controls (CSC) [CSIS 2013][4] or the Australian Government Department of Defense Top 35 "Strategies to Mitigate Targeted Cyber Intrusions" (DND 35) [DND 2012],[5] as a practical and economical first step to improving their cybersecurity posture. This Paper provides an extended version of the Cybersecurity Economic Framework and specifically provides guidance to organizations regarding how they should address more sophisticated cyber

[4] http://www.councilonycybersecurity.org/practice-areas/technology; http://www.tripwire.com/state-of-security/featured/prioritizing-top-20-critical-security-controls/.
[5] http://www.asd.gov.au/publications/Top_35_Mitigations_2012.pdf.

threats.[6] The resulting Extended Cybersecurity Framework provides a maturity model with more fine-grained guidance that can be effectively used by organizations to guide their investment strategies.

Extended Cybersecurity Framework

The Cybersecurity Economic Framework (shown in Figure 1) and the three Investment Principles provide a solid basis for organizational decisions about cybersecurity investments. However, addressing sophisticated threats can be quite costly and, therefore, requires a more nuanced approach. This Paper extends the initial Cybersecurity Economic Framework by adding additional granularity, specifically focused on addressing sophisticated threats.

In developing the extensions to the Framework, a number of cybersecurity models and methodologies were examined for possible insights. [CERT 2010; SEI 2013: NICE 2012; DOE 2012] Some of the models defined a progression of security investments (*i.e.,* a maturity model) for cyber defenses. In general, these models recommended implementing additional controls to enhance security protection at higher maturity levels and did not provide insight into evaluating the economic benefits of investment decisions. In some cases, the models were tailored for specific domains (*e.g.,* the electricity domain).

One model, developed by Robert Lentz, former Director of Cybersecurity for the U.S. Department of Defense, proved particularly helpful in guiding extensions to the Cybersecurity Framework. [Lentz 2011] Lentz's model paralleled the Cybersecurity Framework recommendations for relatively unsophisticated threats (*i.e.,* implement a baseline of critical controls). In addition, Lentz's model predicted the economic benefits of security countermeasures for addressing sophisticated threats, referred to in the model as Advanced Persistent Threats (APT) and Nation State threats. Specifically, Lentz's model recommended ways to reduce overall cost to an organization in addressing sophisticated threats. Lentz introduced the concept of tracking of evolving behavior and pattern of threats as a primary method for addressing more sophisticated threats and making appropriate additional investments in cyber security.

Lentz's recommendation to focus on attack patterns in order to address sophisticated threats aligned with insights gained from discussions during this research with the Chief Information

[6] A threat to cyber systems refers to persons who attempt unauthorized access to a cyber system device and/or network. This access can be directed either from within an organization by trusted users, or from remote locations by unknown persons using the Internet. Threats can come from numerous sources, including hostile governments, terrorist groups, disgruntled or poorly trained employees, and malicious intruders.

Security Officers (CISOs) of several large companies, each of whom appeared to have a highly advanced cyber defense capability. [Gilligan 2013] In one case, the initial claim by the organization was that their cyber defenses were totally based on dynamic threat response, and specifically not based on a foundation of baseline security controls following Investment Principle #1. Upon further discussion, it became clear that, as shown in the Cybersecurity Framework above, the organization had actually implemented a core set of baseline security controls to address the less sophisticated threats. However, this organization, as well as others contacted, strongly asserted that a static defense based on additional "layers" of controls on top of the baseline found in the DND Top 35 and CSC was neither economically feasible, nor effective in countering sophisticated threats.

The common characteristic between Lentz's model and the industry experiences was complementing the implementation of baseline security controls with the employment of a real- time, threat-based security protection strategy (consisting of highly focused automated controls, as well as human analysts for identifying and countering more sophisticated threats). What the organizations shared was that beyond a certain point, the cost to implement an increasing number of automated controls became economically and practically counterproductive. When sophisticated attackers are obstructed by static controls, they rapidly alter attack techniques. Therefore, the return on investment for additional controls beyond those that could be implemented with very modest cost did not justify the additional investment. Moreover, the organizations often found that layers of controls resulted in conflicting interaction among controls that actually reduced the overall security posture of the organization.

Common characteristics of the cyber defense strategies among these companies were the following: 1) increased reliance on real time information sharing and collaboration with high caliber government and industry consortia to rapidly recognize, and then respond to, emerging or changing attack patterns; and 2) the use of automated, as well as human, analysis of attack patterns to develop a continuously evolving set of countermeasures for sophisticated threats.

One CISO remarked that from an economic perspective, the organization found that the best return on investment was to employ countermeasures beyond the "baseline" only in response to recognized specific attack patterns from sophisticated adversaries. However, the desire of the organization was also to improve the cost effectiveness of countermeasures so that over time they can be, in the words of the CISO, "pushed down" to be part of the baseline set of security controls.

Lentz predicted in his model that employment of these techniques (*i.e.,* sharing of threat information and employing proactive analysis and focused response to evolving attack patterns) would permit an organization to successfully counter sophisticated attacks and,

therefore, improve the return on investment of cyber defenses to an organization. His prediction is based on anecdotal data rather than a detailed economic analysis of actual cost and benefits, but he does point out that the cost to an organization of a successful attack by a sophisticated attacker can be very large. There are numerous well-publicized examples, including the recent attack on Target in November 2013 that has Target's Chief Financial Officer, John J. Mulligan, appearing as the first witness before the Senate Judiciary Committee on February 4, 2014: "In addition to an investigation of the breach by the Secret Service, the Justice Department and several state attorneys general, the Senate Judiciary Committee has asked Target for documents related to its cybersecurity efforts and the malware used in the attack."[7]

The insight provided by the Lentz model, as well as the company sources, provides the basis for our Extended Cybersecurity Framework and for identifying these additional Investment Principles:

Investment Principle #4: The economic benefit of participating in multiple, high quality cyber security information sharing exchanges regarding the dynamic characteristics of sophisticated threats is very high.

Investment Principle #5: Additional Investments to address sophisticated threats should be specifically tailored to the (evolving) threat characteristics.

Investment Principle #6: Effective countering of the most sophisticated threats (e.g., Nation State) requires investment in current technology controls and human capabilities to be able to effectively predict and respond to attack patterns.

Investment Principle #5 (which we'd like to particularly emphasize) reflects our finding that ***broad*** application of additional controls beyond the foundational set of critical controls is not a sound economic investment—as stated above, additional controls should be ***specifically tailored*** to the evolving threat characteristics.

Interaction with CISOs from organizations with industry-leading cyber capabilities highlighted that, in most cases, implementation of additional layers of controls is expensive. Moreover, in their experience, sophisticated attackers are very agile in successfully developing alternative attack vectors when confronted with effective static controls. This Investment Principle does not align with guidance from the US government in publications from the National Institute of Standards and Technology (NIST) that recommends implementation of additional controls is the

[7] Elizabeth A. Harris, Nicole Perlroth and Nathaniel Popper, "Neiman Marcus Data Breach Worse Than First Said" *The New York Times* (January 23, 2013) http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?smid=tw-share.

primary method for an organization to achieve an improved security posture. [NIST 2009; NIST 2010]

The Extended Cybersecurity Framework addresses the additional insights and principles from Lentz and the companies surveyed to produce a more granular perspective of cyber investments and respective focus areas. In particular, each of the broad areas of the Framework depicted in Figure 1 can be subdivided into what is referred to in this Paper as 'levels' reflecting progressive investment and associated actions that describe an evolutionary path for investment and improved security effectiveness.

The lower portion of the original Cybersecurity Economic Framework can be viewed as having two gradations or levels as shown below in Figure 2. The levels reflect a prioritization of focus and investment for organizations in implementing a comprehensive [set of] security controls.

Enhanced Descriptor	*Employment of Security Controls*	*Security Tailored to Mission*	*Participate in Information Sharing (threat and vulnerabilities)*
Managed	CSC Integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs
Performed	Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs

Figure 2: Expanding the Baseline of Security Controls

The lower or first level in implementing a comprehensive baseline of security controls, **Performed**, reflects implementation of the baseline set of controls. However, the implementation does not include information sharing, automated continuous monitoring, or partitioning of architecture to focus protection on mission critical capabilities and data.

The upper or second level in implementing a comprehensive baseline of security controls, **Managed**, does provide continuous, automated monitoring of the baseline controls; information sharing to identify new profiles that should be implemented by the foundation critical controls; process metrics such as those found in the Critical Security Controls [CSIS 2013]; and, at least, partial focus on discriminating additional protection investments toward the most critical mission capabilities. The overall economic benefits of implementing a baseline set of controls are significantly enhanced by an organization moving to the **Managed** level. The additional cost is relatively small, but the implementation of additional processes, controls, tools and management disciplines requires a more mature organizational approach.

Figure 3 below shows the refinement of the portion of the Extended Cybersecurity Framework that addresses more sophisticated threats.

Enhanced Descriptor	Employment of Security Controls	Security Tailored to Mission	Participate in Information Sharing (threat and vulnerabilities)
Resilient	Augment CSC Based on Mission and Threats	Investments are Mission Assurance Focused	Tools and Staff to Response to Shared Threat Information
Dynamic	Augment CSC Based on Mission and Threats	Investments are Mission Protection Focused	Tools and Staff to Response to Shared Threat Information

Figure 3: Expanding Targeted Advanced Security Controls/Methods/Tools

Figure 3 shows two gradations or levels: **Dynamic** and **Resilient**. The lower level, **Dynamic**, calls for augmentation of the foundation of critical security controls based on the organization's mission and real time knowledge of threats gained through high quality cybersecurity and threat information sharing arrangements. Organization would implement selective controls, complemented by human surveillance, to counter Advanced Persistent Threats (APTs). This level of implementation of controls is ***dynamic*** to reflect the evolution of threats. This Dynamic Level also calls for investments to deliberately protect the ability to operate and preserve critical mission functions and data. Typically, this can be done by appropriately architecting the cyber environment into logical or physical protection enclaves reflecting different mission criticality of the information and capabilities in the enclave. Finally, the Dynamic level would recommend an investment in the capability provided primarily by skilled humans, as well as information sharing agreements, to rapidly identify and respond to actual cyberattacks from sophisticated sources.

The upper level, **Resilient**, builds on the investments of the Dynamic level by focusing on the ability to effectively counter very sophisticated threats (*e.g.,* threats from Nation States and their proxies) and permit an organization to continue mission critical operations with minimal disruption despite the persistent presence of sophisticated cyberattacks. The key additional investments at this level are both automated and human capabilities to perform real time analysis of attack patterns thereby permitting an organization to actually anticipate these threats and to be prepared to rapidly respond to highly sophisticated threats, including pre-planned packages that can be tailored to respond to actual attacks. Organizations exhibiting Resilient Level characteristics were adept at recognizing threat trends and the common characteristics of specific threats and their mutations over time. They were, thus, able to predict, with good certainty, where and how the threat would likely evolve in the next few hours and days. In addition, in the Resilient Level, an organization invests in building protected enclaves, implementing selective redundancy for highly critical capabilities, and the ability to operate in a degraded or contested mode during an attack. These investments in automation, planning and human capabilities result in an organization being able to assure mission continuity that persists through sophisticated cyberattacks.

These refinements creating the Extended Cybersecurity Framework permit organizations to appropriately focus and prioritize investments. Clearly, some organizations will believe they are not the target of threats that have the sophistication of a Nation State and their proxies so will conclude that the types of investments required for the Resilience Level or even Dynamic Level may not be economically beneficial. In other cases, organizations that have begun implementing a baseline set of critical security controls found in the CSIS or Australian DND references can begin to plan for implementing the recommended progression of cybersecurity investments [CSIS 2013; DND 2012; DND 2013].

Figure 4 provides a summary of the Extended Cybersecurity Framework with the respective element of the initial Framework shown in the right column of the figure. The progression of levels in the Extended Cybersecurity Framework reflects a maturity model that organizations can use to focus, prioritize and phase their investments in cybersecurity protection capabilities.

Enhanced Descriptor	*Employment of Security Controls*	*Security Tailored to Mission*	*Participate in Information Sharing (threat and vulnerabilities)*	*Response to Cyber Threats*	*Cybersecurity Framework Area*
Level 4: Resilient Operate Through Sophisticated Attack	Augment CSC Based on Mission and Threats	Investments are Mission Assurance Focused	Tools and Staff to Response to Shared Threat Information	Analytical Capabilities to Anticipate Threats	**Additional Investments to Deploy Targeted Advanced Security Controls/Methods**
Level 3: Dynamic Able to respond to Sophisticated Attack	Augment CSC Based on Mission and Threats	Investments are Mission Protection Focused	Tools and Staff to Response to Shared Threat Information	Capabilities for Rapid Reaction To Threats	
Level 2: Managed Protection against Unsophisticated Attack	CSC Integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs	Respond to Attacks After the Fact	**Implement Comprehensive Baseline of Security "Good Hygiene"**
Level 1: Performed Some Protection Against Unsophisticated Attacks	Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs	Respond to Attacks After the Fact	

Figure 4: Extended Cybersecurity Framework

An important objective for most organizations is the ability to measure the value of investments, in this case the return on investment (ROI) in terms of fewer cyber breaches and less economic impact. The authors of this paper gave some preliminary thought to the type of measures that could be used in conjunction with this Extended Cybersecurity Framework.

These are admittedly preliminary and have been included in Appendix A. As this Extended Framework is implemented, it is hoped that appropriate measures can be refined to guide organizations as they make detailed ROI assessments.

Summary

The objective of *The Economics of Cyber Security: A Practical Framework for Cybersecurity Investment* was to answer the following questions:

1. Is the investment by the United States in cybersecurity being appropriately applied?
2. Should organizations invest more or less in order to provide adequate security?
3. Where should organizations invest to gain the biggest economic return?

That paper, supported by the observation that the vast majority of attacks originate from unsophisticated threats and a straightforward baseline of security controls is effective against such attacks, concluded that much of the approximately $15 billion spent could be better focused. In short, implementing a baseline of controls reflects sound economics.

With regard to whether organizations should invest more, the Cybersecurity Economic Framework provided a "roadmap" for incremental investments. Most organizations do not need to invest significant additional resources to implement a comprehensive baseline of security controls. In fact, most organizations have already purchased commercial tools that effectively implement such controls with minimal additional investment other than normal maintenance/upgrades. Effective implementation of the baseline security controls requires increased management discipline and strong leadership to ensure that they are effectively used with effective processes and metrics.

The Extended Cybersecurity Framework and Investment Principles provide economic advice to organizations wishing to focus additional investments to address more sophisticated threats while producing sound return on investment. It reflects the practices of leading organizations to focus investments by leveraging knowledge of the specific and evolving attack patterns being observed inside and outside a particular organization. More granular identification of incremental cybersecurity investments results in a "maturity model" that can be followed by organizations as they seek to evolve to an improved cybersecurity posture.

While both papers focus primarily on technical measures for cyber security, such controls must be a part of a comprehensive cybersecurity program that continuously addresses trained people, adequate policies and appropriate processes. The Extended Cybersecurity Framework requires an organization to have adequately trained cybersecurity staff. This requirement is especially important for Levels 3 and 4. Similarly, appropriate policies and procedures must govern an organizations' investment strategy (especially policies and procedures addressing

how an organization: responds to attacks; deals with potential loss of mission capabilities, and goes about reconstitution after attack).

This paper defined a set of principles of an economic framework for cybersecurity. Additional efforts should focus on collecting both cost and benefit data from representative organizations. This will permit validation of the principles in this effort and provide more granular economic insights for organizations with regard to investments in cybersecurity.

Appendix A: Possible Metrics for the Cybersecurity Framework

Several reviewers of this Paper commented on the need to provide quantifiable metrics for determining the effectiveness and economic benefits of cybersecurity measures. Candidly, the research conducted did not focus in this area and this is a much-needed area for further exploration. Nevertheless, the Extended Cybersecurity Framework does lend itself to an initial set of metrics. These are summarized in the figure below and can be the focus of annual or more frequent inspections. It is noted that these metrics should also be examined and updated as a focus of future research.

Enhanced Cybersecurity Framework Descriptor	*Employment of Security Controls*	*Security Tailored to Mission*	*Participate in Information Sharing (threat and vulnerabilities)*	*Response to Cyber Threats*
Level 4: Resilient Operate Through Sophisticated Attack	Metric: Capability for real time deployment of controls in response to changing threat profile	Metric: 1) Deployed protection architecture based on assuring mission continuity; 2) Regular exercise of ability to operate through attack	Metric: 1) Robust network of information exchange partners monitored on real time basis; 2) Staff capable of extending threat data to predict threat evolution.	Metric: Established policies and practices as well as experienced staff able to permit real time response to sophisticated threats
Level 3: Dynamic Able to respond to Sophisticated Attack	Metric: Implement threat monitoring capabilities to support identification and deployment of additional controls	Metric: 1) Identification of mission critical capacities; 2) Deployment of (partial) architecture and controls to protect mission critical capabilities	Metric: 1) Robust network with information exchange sources; 2) Experienced staff capable of rapid response to sophisticated threats	Metric: Organic staff capable of recognizing sophisticated threat and recommending response actions
Level 2: Managed Protection against Unsophisticated Attack	Metric: 1) Ensure baseline controls are consistently applied across the enterprise; 2) Controls are implement with (continuous) automated monitoring with a goal of hourly or single digit minute cycle times	Metric: Formal identification of mission critical capabilities	Metric: 1) Established relationship with one or more information sources for cyber threat and vulnerability information; 2) Standard processes for rapidly responding to threat/vulnerability updates	Metric: Organization staff able to respond after the fact to attack
Level 1: Performed Some Protection Against Unsophisticated Attacks	Metrics: 1) Implement DND Top 4 Controls; 2) Implement some additional CSC or DND 35 Controls	Metric: None	Metric: Threat/Vulnerability Information pushed to organization but inconsistently reviewed or applied	Metric: Attack response prompted from outside the organization

Figure A1: Metrics for Enhanced Cybersecurity Framework

Appendix B: The Cybersecurity Investment Principles

Investment Principle #1: Implementation of a comprehensive baseline of security controls that address threats that are of low to moderate sophistication is essential and is economically beneficial.

Investment Principle #2: Focus security investment beyond the baseline controls to counter more sophisticated attacks against the functions and data that are most critical to an organization.

Investment Principle #3: For sophisticated attacks, an organization should accept the security risk of not protecting functions and data that are of lowest impact to the organization's mission and where cost exceeds benefits.

Investment Principle #4: The economic benefit of participating in multiple, high quality cyber security information sharing exchanges regarding the dynamic characteristics of sophisticated threats is very high.

Investment Principle #5: Additional Investments to address sophisticated threats should be specifically tailored to the (evolving) threat characteristics.

Investment Principle #6: Effective countering of the most sophisticated threats (e.g., Nation State) requires investment in current technology controls and human capabilities to be able to effectively predict and respond to attack patterns.

References

AFCEA Cyber Committee: *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, Armed Forces Communications and Electronics Association. October, 2013.

CSIS 2013: *CSIS: 20 Critical Controls: Critical Controls for Effective Cyber Defense* – Version 4.1. March, 2013.

DND 2012: *Strategies to Mitigate Targeted Cyber Intrusions*, Australian Government, Department of Defence Intelligence and Security, October 2012.

CERT 2010: *CERT Resilience Management Model, Version 1.0*, CMU/SEI-2010-TR-012.

SEI 2013: SEI Innovation Center Report: *Cyber Intelligence Tradecraft Project: Summary of Key Findings*, Software Engineering Institute, January 2013.

NICE 2012: *Cybersecurity Capability Maturity Model (White Paper), National Initiative for Cybersecurity Education (NICE)*, October 3, 2012.

DOE 2012: *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, Department of Energy and Department of Homeland Security, May 31, 2012

Lentz 2011: Robert Lentz, Cyber Security Maturity Model, PowerPoint presentation, wwwdintel.org.

DND 2013: *Top 4 Strategies to Mitigate Targeted Cyber Intrusions*, Australian Government, Department of Defence Intelligence and Security, April 2013

Gilligan 2013: Discussions with Chief Information Security Officers of four large companies. The companies have not approved release of their identities.

NIST 2009: SP 800-53, Rev 3. *Recommended Security Controls for Federal Information Systems and Organizations*. August 2009.

NIST 2010(2): SP 800-53 A, Rev 1. *Guide for Assessing the Security Controls of Federal Information Systems and Organizations, Building Effective Security Assessment Plans*.