Proceedings of the 2016 Industrial and Systems Engineering Research Conference
H. Yang, Z. Kong, and MD Sarder, eds.

A Review of and Agenda for Cybersecurity Policy Models

Natalie M. Scala
Department of e-Business and Technology Management
Towson University, Towson, MD 21252

Paul Goethals
The Army Cyber Institute
United States Military Academy, West Point, NY 10996

Abstract

Recently, cybersecurity has received increased attention, as the quantity and severity of breaches continues to rise. Fundamental architecture and practices research exists in the computer science and policy domains, but research is lacking from a decision sciences perspective. This research reviews three policy models for cybersecurity. These models are from a policy perspective and focus on both heuristics and metrics. The general approach of these models limits predictive and prescriptive analysis by focusing on descriptive modeling and the static nature of system design. As a way forward, we present preliminary research of value focused modeling of cybersecurity metrics. This approach enables identification of the most critical metrics and supports prescriptive analytics for design and monitoring of cybersecurity systems.

Keywords
Cybersecurity, Policy, Value Focused Thinking, Metrics, Analytics

1. Introduction
Cybersecurity is evolving and increasingly becoming a forefront issue, as frequency and severity of attacks continue and grow. For example, 157 attacks and breaches were recognized in 2005, with 783 recognized incidents in 2014 [1]. Attacks continued against notable businesses in the last two years, and breaches occurred against organizations such as Neiman Marcus, University of Maryland, JP Morgan Chase, Home Depot, Staples, Morgan Stanley, Anthem, and Rutgers University [2].

In addition to the recognized attacks, hundreds or thousands of additional attacks went unrecognized. Cyber breaches can be invasive and damaging. Customer relations can be impaired and economic losses can be significant. Farahani, et al. [3] identify challenges companies face when hacked; those challenges are compounded by advancing technology, greater interconnectedness, and interdependent systems, which make securing data and systems from hacks even more difficult.

Most research in cybersecurity has been developed in the computer science or network infrastructure fields, generally ignoring the analytics and human elements of cyber systems. As a result, research from an Industrial Engineering perspective is generally undefined and unchartered. As a field, cybersecurity has not established a structured means to either measure performance of a system or predict the next breach with a degree of certainty. This is partly because cyber is a "reverse" problem, in that "success" is defined as the lack of a breach. Traditional risk models define "success" as a given activity actually occurring. Therefore, our overall research aims to establish a framework for prioritizing metrics and best practices for cybersecurity, allowing customizability by organization and/or economic sector. By employing Value Focused Thinking (VFT), we may rank relative importance of various metrics and best practices. In order to identify metrics and best practices for consideration in the model, we now review both established models for cybersecurity and the metrics literature as defined by "The Five Hard Problems."

2. Cybersecurity Models

In the last decade, researchers interested in the evaluation of cybersecurity programs have proposed a wide number of models. Specifically, we outline three distinct measurement techniques that clearly define the advancements made to the applicable body of knowledge.

2.1 The Three Tenets Model

In 2013, Cybenko and Hughes [4] described their early work on a vulnerability model for cyber-physical systems. The foundation of the model relied on three necessary and sufficient elements for an attack to be successful: (i) the presence of weaknesses in a system, (ii) the adversary having access to these weaknesses, and (iii) the adversary having the capability to exploit the weaknesses. A network of nodes representing components or devices would serve as the architecture for validating the model, whereby the "time to compromise" the network depended on both the diversity of security approaches offered by the organization and the number of parallel attackers. To model the "time to compromise" a system, the authors suggested various probability density functions based upon the robustness of the attack and the array of the defense.

In order to counter each of the three elements of a successful attack, the authors further identified measures of mitigation known as the "Three Tenets" that would serve as the framework for their proposed quantitative security metrics. The first tenet, *focus on what is critical*, called for minimizing the number of access points to critical system components. The premise of this rule is that all systems have design and process errors inherent in their operation; hence, only the mission critical components or information should be given the full attention of security professionals. The second tenet, *move key assets out-of-band*, suggests existing potential degrees of separation between the attacker and the desired target. Maximizing this separation then limits the adversary's access and reduces the probability of a successful attack. Finally, the third tenet, *detect, react, adapt*, calls for active defense measures that sense malicious behavior, integrate intrusion response mechanisms, and modify the nature of information environment. In doing so, a target may be presented that appears to be of little intrinsic value to the attacker. While the mathematical foundation of the "Three Tenets" model is not provided, there are some indications that a weighted scheme is employed. The authors discuss the tradeoffs that must be made between the confidentiality of the data, the integrity of the system, and the availability of the information. As part of the risk management process, decision makers may then prioritize one security condition over another.

2.2 The Attack Graph and Attack Surface Models

Graph-based models for identifying cybersecurity vulnerabilities have been in practice for the last thirty years. The Department of Defense employed the technique in the late 1980s; since then, the models have evolved into automatically generated platforms where advanced concepts, such as machine learning, are further incorporated [5]. The method takes into account the number of available paths that an attacker may take in reaching his/her target. Some researchers have proposed using attack graphs over other methodologies, due to their ease of implementation and the breadth of scientific work supporting the method [6].

In 2014, Abraham and Nair [7] proposed a variant of an attack graph model, where they incorporated a set of attack rules and security policy countermeasures into a network topology. The concept of the absorbing state for a Markov Chain was employed to simulate probabilities of network nodes becoming susceptible to an attack. At the heart of the methodology was an "exploitability score" and an attacker profile, which affected the time that an adversary took to transition from one network node to another. A similar construct of an attack graph Markov Chain model, proposed by Durkota et al. [8] in 2015, utilized honeypots as a deception mechanism and transition probabilities based upon principles from game theory.

A similar approach in the last decade involves what is known as an "attack surface," consisting of the targets, the devices and their policies, and access controls. The concept, which was introduced in 2003 by Howard, et al. [9] and further described by Manadhata and Wing [10], considered the exposure of an organization as the focus, whereby a larger number of access devices, data items, and paths equates to a larger adversarial attack surface. The representation in Figure 1 depicts the concept of an attack surface, an analogous depiction to that observed by Theisen, et al. [11] in 2015.

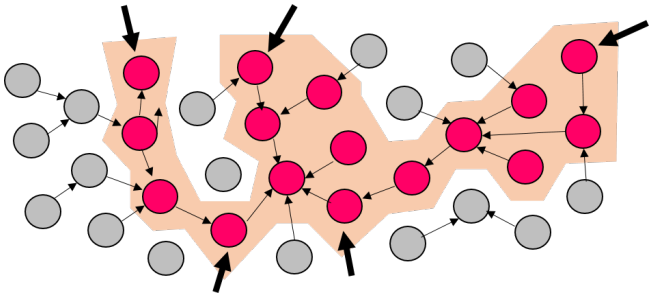

Figure 1: An Attack Surface Representation (Shaded Area)

In the last ten years, the concept has migrated to describing the architecture of both internal and external networks. Sun and Jajodia [12] proposed a surface metric that focuses on increasing the signature of the external network as a means to draw the attacker away from critical internal resources. The objective of minimizing an attack surface can also be found in the literature, so as to reduce the exposure of an organization to malicious activity [13] [14].

2.3 The Cybersecurity Heuristic Model

In 2015, Libicki, et al. [15] of the RAND Corporation published a research monograph titled, *The Defender's Dilemma*. The effort outlined the results of a vast survey of various senior security officials, offering evidence of effective tools or processes for defending against an information attack. Using the results of the survey as a basis for their study, the researchers then proposed a heuristic model for measuring cybersecurity effectiveness. While the model chose not to consider the effects of adversarial behavior or the choice of defensive techniques in its construct, it did put significant emphasis on the decisions made by organizations and the selection of security tools for protecting information. One of the survey findings was the clear intent of organizations to minimize their cybersecurity costs, in terms of the training and tools purchased, the restriction policies for devices, and the transparency of the network. This defined cost would serve as the tradeoff mechanism between bolstering one's defensive posture and facilitating attacker access.

In order to establish a spectrum of measurement for information security, the researchers suggested more than two dozen parameters that might forecast the likelihood of an attack. Shown in Table 1 are just some of the factors incorporated into their heuristic model:

Table 1: Security Factors Affecting the Heuristic Metric

Measurement Factor	Characteristics and Effects
Organizational Size	Four size categories considered, based upon employee numbers (more than 100K, 10K, 1K, and 100). Larger organizations are more vulnerable (more entry points).
Organizational Value	Five categories of value, corresponding to the loss suffered by an attack.
Organizational Diligence	Five categories, related to the ability of an organization to enforce its security tools.
External Hardness	Determined by number of computers and mobile devices in an organization, their resistance to attack, the level of user training, and the restriction policies on devices.
Internal Hardness	Determined by the security tools that are purchased.
Air-Gapping	Isolating parts of an organization's network limits the losses from an attack.

To determine the quantity of loss from an attack, the researchers proposed using the product of the organizational value category, external hardness, and internal hardness. The level of training for employees, the quality of cybersecurity tools, and the degree of constraints used for mobile devices, all affect the measure of the network's internal and external hardness.

Upon performing a sensitivity analysis with select factors, the researchers prescribed lessons for both organizations and public policy with the aim of improving one's cybersecurity posture. Most importantly, organizations should have a firm understanding of what needs protection along with the degree of security required. Information management supervisors should know the access controls in place and what systems and applications are running on the network. Efforts should also be made to employ countermeasures at the organizational level, where and when feasible. In order to promote greater collaboration between government and industry toward addressing the cybersecurity problem, information sharing must be viewed as an endeavor to build a common picture of how

systems fail; hence, organizations may gain confidence in knowing that government agencies have an interest in protecting their information. Finally, the researchers noted that some defensive improvements may be achieved by advancing certain system protection policies, making it more difficult for attackers to employ typical approaches.

3. Science of Security: "The Five Hard Problems"

3.1 Definition

Generally speaking, current research in cybersecurity has primarily focused on system design and architecture. However, the nature and severity of recent breaches creates urgency to assess the strength of design and inherent risk in a cyber system. These needs led to the development of the Science of Security (SoS) initiative, led by the National Security Agency. SoS focuses on scientific cybersecurity foundations, promoting transdisciplinary research between fields such as computer science, mathematics, electrical engineering, psychology, economics, and the social and behavioral sciences [3]. SoS arranges current cybersecurity research into five major veins, called "The Five Hard Problems:" (i) *scalability and composability* examines combining secure components into a larger secure item, as vulnerabilities often lie in the gaps between two components; (ii) *policy-governed secure collaboration* develops methods and requirements to guarantee data protection while enabling information sharing and collaboration; (iii) *resilience* measures the ability of a system to resist an attack by unauthorized parties; (iv) *human behavior* researches unpredictability and complexity of human behavior which aids in the development of models that have increased accuracy while minimizing potential vulnerabilities from humans interacting, possibly unsecurely, with systems; (v) *security metrics* measure the security or vulnerability of a system. In general, metrics are especially challenging. Systems are extremely complex, and small nuances may have significant impact [16].

Most of the hard problems align with system design principles. The corresponding research in that area addresses structures in place to prevent breaches but does not measure how well a system is averting attack or how an IT department should manage cybersecurity on a daily basis. Specifically, the *security metrics* hard problem defines best practices for system management, but implementing all recommended metrics is impractical for organizations. For example, as of May 2015, 80 papers indexed by SoS propose metrics [17]. Farahani, et al. [3] highlight a small sample of the metrics and best practices associated with these papers, including honeybots, personalized application whitelisting, anonymization, CleanURL, probability a system is vulnerable, measuring attack surface area, and time system is vulnerable before a patch is deployed.

3.2 Descriptive vs. Predictive Metrics

In general, systems that have employed security properties are not immune to breaches. From an analytics perspective, metrics are descriptive and measure the current properties and performance of a system. A general challenge is to develop security metrics that are capable of confirming that a given cyber system preserves a given set of security properties. Metrics must be quantifiable, feasible, repeatable, and objective. However, metrics indexed by the SoS generally attempt to make an assessment or prediction about future events. Forecasts are a classic example of a predictive analytic, and best practices alone cannot measure the probability of future events. Thus, a research need exists to translate the descriptive nature of system assessment into a means of predicting future events. Furthermore, the SoS literature identifies practices and architectures but does not speak to guidelines for implementation of these best practices. The overall risk of a breach to the system is not currently measured within the hard problem environment; risk must be managed and quantified as part of predictive analytics.

4. Research Design

Value models can assist with the definition of risk and value. VFT is a creative process, with decision makers brainstorming all possible objectives and alternatives, regardless of feasibility. A model then evaluates each alternative against the objectives, identifying the preferred course of action. Throughout the process, the decision maker focuses on value and is proactive in identifying that which is cared about within the problem space. The reader is referred to [18] [19] for further details on the VFT process.

Multiple objective decision analysis (MODA) is a decision analysis technique for evaluating a decision under multiple objectives or criteria; the objectives may be conflicting [20–22]. MODA is a utility approach and frequently used with VFT. Objectives are defined into attributes, which are organized into a value hierarchy. Then, for each attribute on the hierarchy, a value function is defined; alternatives are then scored by creating an additive value function across the value objectives and attributes for each alternative [21]. The alternative with the highest

score is deemed preferred. Further details on the MODA process can be found in [20-22]. A step-by-step outline of the process, with best practices for defense applications, can be found in Dillon-Merrill, et al. [23].

Our overall research aims to address inherent risk in cyber architectures and provide an implementable methodology for cyber metrics and best practices. Our research will construct a framework to identify metrics and best practices that are most appropriate for various organizations and industries, based on their current cybersecurity posture, needs, and operating climate. VFT will be used with MODA to build a model of metrics; the metrics will be scored by using value functions. Engineering managers can then assess the importance of these metrics against the specific cybersecurity needs of their organization. The output of the model will be a rank-ordered list of metrics and best practices; the higher scoring metrics would be those of greater importance to the organization. Cost vs. benefit analyses of metrics and best practices implementation versus improved cybersecurity posture can then be done, creating a complete organizational strategy to secure cyber assets.

The MODA process will be used to build the value model, which begins with the identification of objectives and attributes. Development of the value hierarchy has begun using the gold standard [24] where source texts, policy documents, and related research are reviewed, including documents provided and research indexed by SoS. From that review, we identify objectives in cybersecurity metrics and corresponding best practices that may measure the objective or mitigate risk. These metrics and practices are presented in Table 2. Our research goal is to contribute a value model framework that organizations can use with their data and corresponding values to identify appropriate metrics for their cyber systems.

Table 2: Value focused objectives with corresponding metrics and best practices

Objectives	**Metrics / Best Practices**
Minimizing cyberattacks on internal infrastructure	Firewall, intrusion prevention systems
Minimize data loss	Data at rest/transit encryption, verify encryption certificates
Maximize detection & intrusion of unauthorized person	Anomaly behavior analysis
Minimize malware downloaded from Internet	Web content filters
Maximize the catch of unauthorized people in a system	Honey pots
Maximize securing the system	Air-gap
Minimize identity theft	Limit storage of personally identifying & sensitive data
Minimize intrusions and system failures	Dynamic execution environment & protection, sandbox
Reduce the opportunity for attack persistence	Dynamic platforms
Maximize user awareness of possible attacks	User awareness defense
Minimize the installation of malware	Application whitelisting
Maximize the awareness of unprotected systems	Real time monitoring, accounting, & identifying all network devices
Maximize the awareness of possible attack areas	Measuring attack surface area
Minimize the time of being vulnerable	Automated patch deployment
Minimizing the response time of protecting system	Automated response using predetermined responses
Minimize successful attacks of individuals at home	Home user training, secure default configurations for software

5. Conclusion

The opportunities for applying Industrial Engineering principles in the cybersecurity realm are vast. Most research has been focused on network infrastructure and computer science, and the field can benefit from continuous improvement principles, application of best practices, and dedicated operations research modeling. We identify current cybersecurity models and summarize the hard problems framework. Clearly, there is room for Industrial Engineers to contribute to each of the hard problems. We identify needs in the metrics realm and present an agenda for research in value models to prioritize metrics and best practices. Such models can help to shape an organization's cybersecurity policy and provide an implementable action plan to improve cybersecurity posture.

Acknowledgements

The authors thank Jasmin Farahani for her help with compiling Table 2. The views expressed in this paper are those of the authors and do not reflect official policy of the U.S. Army, Department of Defense, or the U.S. Government.

References

1. Identity Theft Resource Center, n.d., "Data Breaches," retrieved from http://www.idtheftcenter.org/id-theft/data-breaches.html
2. Goethals, P. L., 2015, "Operations Research Initiatives in Cyber Defense," INFORMS Annual Meeting, November 1-4, Philadelphia, Pennsylvania.
3. Farahani, J., Scala, N.M., Goethals, P., and Tagert, A., 2016, "Best Practices in Cybersecurity: Processes and Metrics," Baltimore Business Review, 28-32.
4. Hughes, J., and Cybenko, G., 2013, "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity," Technology Innovation Management Review, retrieved from http://timreview.ca/article/712.
5. Phillips, C., and Swiler, L., 1998, "A Graph-Based System for Network Vulnerability Analysis," Proceedings of the Workshop on New Security Paradigms, 71-79.
6. Yee, G., 2012, "The State and Scientific Basis of Cyber Security Metrics," Defence Research and Development Canada-Ottawa.
7. Abraham, S., and Nair, S., 2014, "Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains," Journal of Communications, 9(12), 899-907.
8. Durkota, K., Lisy, V., Kiekintveld, C., and Bosansky, B., 2015, "Optimal Network Security Hardening Using Attack Graph Games," Proceedings of the 24th Int'l Conference on Artificial Intelligence, 526-532.
9. Howard, M., Pincus, J., and Wing, J., 2003, "Measuring Relative Attack Surfaces," retrieved from http://www.cs.colostate.edu/~malaiya/635/09/Howard03.pdf
10. Manadhata, P., and Wing, J., 2011, "An Attack Surface Metric," IEEE Transactions on Software Engineering, 37(3), 371-386.
11. Theisen, C., Krishna, R., and Williams, L., 2015, "Strengthening the Evidence that Attack Surfaces Can Be Approximated with Stack Traces," Department of Computer Science, North Carolina State University.
12. Sun, K., and Jajodia, S., 2014, "Protecting Enterprise Networks through Attack Surface Expansion," Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation, 29-32.
13. Soule, N., Simidchieva, B., Yaman, F., Watro, R., Loyall, J., Atighetchi, M., Carvalho, M., Last, D., Myers, D., and Flatley, B., 2015, "Quantifying and Minimizing Attack Surfaces Containing Moving Target Defenses," 3rd Int'l Symposium on Resilient Cyber Systems, August 18-20, Philadelphia, Pennsylvania.
14. Atighetchi, M., Soule, N., Watro, R., and Loyall, J., 2014, "The Concept of Attack Surface Reasoning," June 22-26, Sevilla, Spain, 39-42.
15. Libicki, M. C., Ablon, L., and Webb, T., 2015, The Defender's Dilemma: Charting a Course Toward Cybersecurity, RAND Corporation, Santa Monica, California.
16. Nicol, D. M., Scherlis, W. L., Williams, L. A., and Katz, J., 2015, "Science of Security Lablets Progress on Hard Problems, " retrieved from http://cps-vo.org/node/21590
17. Science of Security, 2015, "SoS Documents: By Topic," retrieved from http://cps-vo.org.
18. Keeney, R. L., 1992, Value-focused Thinking: A Path to Creative Decision Making, Harvard University Press, Cambridge, Massachusetts.
19. Keeney, R. L., 2008, "Applying Value-focused Thinking," Military Operations Research, 13(2), 7-17.
20. Parnell, G., 2007, "Value-Focused Thinking Using Multiple Objective Decision Analysis," appears in Methods for Conducting Military Operational Analysis: Best Practices in Use throughout the Department of Defense, Loerch, A. G. and Rainey, L. B. (eds.), Military Operations Research Society, Alexandria, Virginia, 619-656.
21. Keeney, R. L., and Raiffa, H., 1976, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, Wiley, New York, New York.
22. Kirkwood, C. W., 1997, Strategic decision making: Multiobjective Decision Analysis with Spreadsheets, Duxbury Press, Belmont, California.
23. Dillon-Merrill, R. L., Parnell, G. S., Buckshaw, D. L., Hensley, W. R., and Caswell, D. J., 2008, "Avoiding Common Pitfalls in Decision Support Frameworks for Department of Defense Analyses," Military Operations Research, 13(2), 19-31.
24. Parnell, G. S., Bresnick, T. A., Tani, S. N., and Johnson, E. R., 2013, Handbook of Decision Analysis, Wiley, Hoboken, New Jersey.