Risk and the Five Hard Problems of Cybersecurity

Natalie M. Scala[1*], Allison C. Reilly[2], Paul L. Goethals[3], Michel Cukier[2]

[1]Towson University, Towson, MD, USA

[2]University of Maryland, College Park, MD, USA

[3]United States Military Academy, West Point, NY, USA

[*]Address correspondence to Natalie M. Scala, College of Business and Economics, Towson University, 8000 York Road, Towson, MD 21252, USA; tel: +1(410)704-2773; nscala@towson.edu

Appearing in *Risk Analysis*, *39*(10), pp. 2119-2126, 2019

ABSTRACT

This perspectives paper addresses risk in cyber defense and identifies opportunities to incorporate risk analysis principles into the cybersecurity field. The Science of Security (SoS) initiative at the National Security Agency seeks to further and promote interdisciplinary research in cybersecurity. SoS organizes its research into the Five Hard Problems (5HP): (1) scalability and composability, (2) policy-governed secure collaboration, (3) security metrics driven evaluation, design, development, and deployment, (4) resilient architectures, and (5) understanding and accounting for human behavior. However, a vast majority of the research sponsored by SoS does not consider risk, and when so, only implicitly. Therefore, we identify opportunities for risk analysis in each hard problem and propose approaches to address these objectives. Such collaborations between risk and cybersecurity researchers will enable growth and insight in both fields, as risk analysts may apply existing methodology in a new realm, while the cybersecurity community benefits from accepted practices for describing, quantifying, working with, and mitigating risk.

Keywords: Cybersecurity; the "Five Hard Problems;" system design; vulnerability mitigation

Social media summary:

How can risk models enhance cybersecurity? Drs. Scala, Reilly, Goethals, and Cukier identify opportunities and collaborations within the National Security Agency's Five Hard Problems framework.

1. INTRODUCTION

1.1. Cybersecurity and the Risk Perspective

Cybersecurity – the measures taken to protect network systems and their data against attacks or intrusions – is by definition a risk problem. There is significant uncertainty not only in how, where, and when attacks will occur, but also as to how vulnerable systems are to these attacks. While some intrusions are known to have occurred, others are not. Many attacks may simply go undetected, and those that are detected can wreak significant harm. Most systems are so complex that no solution can be fully guaranteed to prevent an intrusion. Thus, the cybersecurity problem space contains significant epistemic uncertainty.

In order to address the complexities of the cybersecurity problem, the National Security Agency (NSA) established the "Science of Security" (SoS) initiative to advance scientific practices in the field of cybersecurity and promote interdisciplinary work (U.S. National Security Agency, 2018a). In support of this, SoS created the *Five Hard Problems* (5HP) to provide structure for a comprehensive, government-driven research program and to encourage collaboration across disciplines by formalizing research needs (Nicol, Sanders, Scherlis, & Williams, 2012). Each of the 5HP sits squarely within the principles of risk, although the concept of risk itself, along with uncertainty, are discussed only implicitly in the 5HP. In fact, the term "risk" is only used 8 times in the entire 21-page document. All this suggests that risk concepts are only barely driving the research direction in a problem space that is inherently driven by risk. We argue that the 5HP can benefit from decades of research and development on general risk principles, extending existing theory to cybersecurity and presenting opportunities for additional involvement by the risk analysis community.

Even outside of the 5HP, the concept of risk is still grossly neglected in cybersecurity. In the past three decades, about two dozen papers in *Risk Analysis* pertain to cybersecurity, one-half of which were published just within the last few years. Table I outlines the specific cybersecurity focus area and approach for each of these papers.

Table I: Cybersecurity Research, *Risk Analysis* (by Year)

Year	Authors	Cybersecurity Focus Area / Approach
2006	Andrijcic and Horowitz (2006)	Macro-economic framework for theft of intellectual property / consequence analysis
2007	Santos, Haimes, and Lian (2007)	Critical infrastructure physical and economic interdependencies / measurement analytics
2009	Henry and Haimes (2009)	Risk management policies for process control networks / measurement analytics
2009	Davis, Garcia, and Zhang (2009)	Structural patterns of network traffic for online businesses / time series analysis
2010	Öğüt, Raghunathan, and Menon (2011)	Insurance risk management / measurement analytics
2014	Kaivanto (2014)	Behavioral decision making for phishing attacks / weighted probability model
2016	Rao et al. (2016)	Cyber risk management for critical infrastructure / game-theoretic methods for attack and defend models
2016	DiMase, Collier, Carlson, Gray, and Linkov (2016)	Supply chain risk management decision making / consequence analysis
2017	Busby, Green, and Hutchison (2017)	Internal and external threats to critical infrastructure control / principle of affordances, consequence analysis
2017	Allodi and Massacci (2017)	Infrastructure security from cyber attacks / risk quantification
2017	Gisladottir, Ganin, Keisler, Kepner, and Linkov (2017)	Effect of over- and under-regulation on organizational resilience for insider attacks / human factors modeling
2018	He, Devine, and Zhuang (2018)	Information sharing against cyber threats / cost-benefit analysis
2018	Paté-Cornell, Kuypers, Smith, and Keller (2018)	Cyber risk management for critical infrastructure / probability model
2018	Canfield and Fischhoff (2018)	Behavioral decision making for phishing attacks / cost-benefit analysis
2018	Ganin et al. (2017)	Cyber system threats, vulnerabilities, and consequences / decision analysis

The majority of the work in cybersecurity risk utilizes either a cost-benefit or consequence analysis approach rather than considering uncertainty, and only three of the papers examine the risk of an insider attack. Moreover, the risk literature lacks focus in key areas such as the effect of various mitigation techniques (encryption, resilient architecture, access control), the impact of the threat spectrum (software error to nation-state actor), modeling attacker decisions (targets, exploits, timings), and consequence analysis (direct costs, indirect costs, national security implications). So why are foundational and emerging risk principles absent in cybersecurity research? For decades, risk analysts have brought insight to other particularly intractable problems, such as terrorism (Zhuang & Bier, 2010), nuclear smuggling (Merrick & Leclerc, 2016), and natural disasters (Thompson, Garfin, & Silver, 2017). When researching these difficult challenges, risk analysts were able to collaborate with domain experts, learn and contextualize problems, and employ methods for working with little data and epistemic uncertainty. Cybersecurity is akin to many "typical" risk problems. However, the lack of literature in addressing the cybersecurity risk problem suggests a significant research gap.

In this perspectives paper, we explore the research agenda proposed by the 5HP and opportunities for the risk community within this framework. Specifically, we discuss the inherent components of risk to the 5HP and draw connections to research needs for rigorous risk assessment in cybersecurity. We argue that addressing risk in cybersecurity, either through the 5HP or another cybersecurity initiative, will advance both the cybersecurity community and the risk community. The cybersecurity community can benefit from applying accepted practices for describing, quantifying, working with, and mitigating risk; the risk community can address emerging challenges that are unique to cybersecurity, providing a platform for further research.

Furthermore, the risk community is adept at contributing to and contextualizing national security concerns; such relationships can continue and grow by examining cybersecurity, as the need to secure government and business systems is urgent and evolving.

1.2. Cybersecurity in Practice

Many organizations and institutions within industry, government, and academia work in extremely unpredictable and unstable cybersecurity environments. The dangers of operating in such a domain may come simply from connecting to a network. In 2016 alone, security companies such as Symantec estimated that an average of more than one million new pieces of malware, in the form of computer viruses or malicious software, were created each day (Symantec Corporation, 2016). The same environment is characterized in many ways by a low-level of understanding with respect to the security situation. IBM, in their annual cybersecurity study of 383 organizations worldwide, identified the average time to discover a breach from a malicious attack as being more than 200 days (Ponemon Institute, 2016). Even when an incident is discovered, many organizations are hesitant to share their breach or attack details, even though they are required to protect personal information or data. Fear of damage to an organization's reputation and a greater emphasis on privacy over security may prevent more attacks from being disclosed, contributing to a general lack of awareness in the severity of the problem.

Adding to the complexity of the cybersecurity problem is the asymmetric nature of the threat and how it could potentially affect an organization's network. The success of malware varieties such as ransomware and the proliferation of distribution methods such as social engineering attacks, suggest that cyber-criminals are likely to continue expanding their

influence. High profile breaches, such as with Sony and the Office of Personnel Management in 2015 as well as the Democratic National Committee in 2016, present evidence of potential state-sponsored actor involvement (Ponemon Institute, 2015; Hosenball, Volz, & Landay, 2016). Despite these apparent dangers outside one's network, recent analysis of cyber incident data suggests that more than 60% of all attacks are caused by insiders, either through malicious intent or inadvertent error (van Zadelhoff, 2016). The problem is more than just human-system interaction; networks may fail due to hardware and software incompatibilities, inadequate resources, gaps in policy management, insufficient training, or reductions in the quality of service.

Although the frequency and severity of known attacks and breaches continue to rise (Farahani, Scala, Goethals, & Tagert, 2016), considering cybersecurity as a complex problem, with severe consequences, is still nascent. For example, cyber policy traditionally focuses on actions to take to prevent a breach. However, these recommendations are evaluated in a limited context. The impact of the recommendations on and the effect of compliance for other components of a system are typically not considered. Furthermore, consequences and the impact of breaches can be hard to quantify. Loss of organization goodwill and brand damage are of concern (Farahani et al., 2016; Whitler & Farris, 2017) , but research is mixed on the consumer or public effect of breaches. For example, in a survey conducted by Ablon, Heaton, Lavery, and Romanosky (2016), 26% of respondents recalled a recent breach notification of their data, whereby 32% of those respondents reported no cost or inconvenience from the breach and 11% of those respondents reporting a change in their behavior with the company. On the other hand, IBM proposes an average cost of a data breach to be $4 million (Ponemon

Institute, 2016). Reliable empirical data is limited. Clearly, more research is needed to better manage and quantify the magnitude of related impacts.

A holistic approach is one that not only focuses on components but one that also considers the interactions among those components, the system architecture, builders, users, those who wish to harm the system, as well as how interactions among these entities create additional vulnerabilities. Some systems approaches do exist that frame cybersecurity as a three-prong hardware, software, and human problem, but consequences in this space are not commonly discussed.

2. THE FIVE HARD PROBLEMS

The 5HP aim to organize and index research in cybersecurity with the goal of advancing scientific practice in the field. The initiative includes a community of practitioners and researchers across government, academia, and industry; to date, more than 500 publications that address one or more of the problems have been documented in various refereed journals or conference proceedings (U.S. National Security Agency, 2018a). Table II defines each of the problems, which serve as a framework for researching and assessing progress.

Table II: The 5 Hard Problems (Nicol et al., 2012)

Problem	Description
1. Scalability and Composability	Develop methods to enable the construction of secure systems with known security properties using components with known security properties, without a requirement to fully re-analyze the constituent components.
2. Policy-Governed Secure Collaboration	Develop methods to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains.
3. Security Metrics Driven Evaluation, Design, Development, and Deployment	Develop security metrics and models capable of predicting whether or confirming that a given cyber system preserves a given set of security properties in a given context.

4. Resilient Architectures	Develop means to design and analyze system architectures that deliver required service in the face of compromised components.
5. Understanding and Accounting for Human Behavior	Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties.

At the onset of developing the 5HP framework, the community of practitioners and researchers realized that making progress demanded a multidisciplinary effort, requiring "contributions from biology, economics and other social and behavioral sciences in addition to the traditional disciplines of mathematics, computer science, and electrical engineering "(U.S. National Security Agency, 2018b). An examination of the literature on the 5HP confirms that the context and motivation of the research is primarily written from the perspective of these various sciences, and, as discussed, risk approaches are largely absent. Given the uncertain and unstable nature of the cybersecurity environment and the potential for a costly network failure, the need for rigorous risk models is clear. In fact, when the 5HP are examined from a risk perspective, several research gaps are discovered. We outline these gaps below, highlighting the approaches and applications currently taken in the research for each hard problem, along with identifying open risk-related research questions and needs.

3. HOW ARE THE FIVE HARD PROBLEMS LINKED TO RISK?

3.1. Scalability and Composability

The *scalability and composability* hard problem addresses components that scale to large systems, are combined to form a new system, or augment an existing system. Connecting smaller components into a large system is of focus; however, the risk related to each individual component may not directly translate into total system risk. The goal is to ensure that when components integrate to form a new larger system, the system itself is secure. Examples of

research in this area include integrating syntax between components written in different programming languages, enforcing information flow constraints and permissions, and analyzing the complexity of attack surfaces (Nicol et al., 2015). Most of this research involves theoretical computer science-driven algorithmic analysis. The research goal is to enable determination of system level security by examining the security of the individual components, which is a more tractable problem due to lower complexity.

Analyzing individual components is contrary to risk analysis practices, as only focusing on component reliability lacks a systems perspective (Garvey, 2008). Individual component approaches may fail to address concepts like threat shifting (i.e., fortifying one component may simply "shift" the threat to another component) and component-adversary-system interactions (i.e., modifications at the component-level creating vulnerabilities at the system-level). The inability to take a more holistic approach adds a level of uncertainty with respect to the integrity and reliability of these structures. There are clear opportunities for risk analysts to contribute to a systems-based approach, identifying risks and proposing mitigations that may arise when the components are joined or merged together. Furthermore, the scientific approaches taken in the cybersecurity community towards evaluating individual components of a system could provide new thinking and approaches to the risk field. These approaches include "combining or hybridizing models" to differentiate between trusted and less-trusted components, developing new programming languages that contribute to overall assurance estimates, and producing adaptive structural designs to account for more sophisticated system architecture (Nicol et al., 2012).

3.2. Policy-Governed Secure Collaboration

Policy involves developing recommendations and guidelines to promote the secure operation of systems and the protection of information. This includes methods for enforcing normative requirements and standards as well as practices for handling system interactions among users with various authorities and permissions (Nicol et al., 2015). SoS research to date addresses algorithms and programming language to set system priorities, developing models to both evaluate if requirements are consistent amongst the system and manage collaborations between users with different authorities; the research also examines if policies capture stakeholder requirements and/or social architecture needs (Nicol et al., 2015). However, policy is typically frustrating to cyber operations and information technology professionals, as the actual enforcement of rules and regulations can be difficult at best. SoS research identifies tensions between security policies and organizational objectives, specifically when the honest user seeks solutions to mitigate the security policy (Koppel, Smith, Blythe, & Kothari, 2015). Strong consequences for a failure to comply with policies are needed, as lack of compliance exposes risk.

The risk community has a rich history of risk governance, with the premise that many systems, such as nuclear power plants, have a level of regulatory control. Policy-related cyber risk assessments must consider each of these cyber networks as decentralized but interconnected entities, often controlled by different organizations or departments. Good risk governance has cognizance of how individuals make decisions, and with this knowledge, encourages better decision-making. There are many examples of this in different risk contexts, including hazard science (Collins, 2008) and energy conservation (Frederiks, Stenner, & Hobman, 2015). However, unique to the security and cybersecurity realm, policy must allow for

dynamic decision-making that is adaptive to an evolving adversary. There are some efforts underway to develop governance guidelines for reducing cyber risk. For example, government entities such as the National Institute of Standards and Technology (NIST) suggest cybersecurity policies (National Institute of Standards and Technology, 2014), but organizations are not legally mandated to follow the guidelines. Furthermore, current guidelines are not optimal, as they are generally based on current best practices rather than rigorous scientific study. For example, Lee, Geng, and Raghunathan (2016) argue that implementing cybersecurity standards may not translate into increased security.

3.3. Security Metrics Driven Evaluation, Design, Development, and Deployment

The *security metrics* hard problem addresses measuring the extent to which various security properties are present in a system; SoS research statistically analyzes vulnerabilities and exploits, measures how users perceive security, and develops metrics to predict vulnerabilities or assess the effectiveness of countermeasures (Nicol et al., 2015). Note that SoS research includes metrics as a form of prediction. This is a clear deviation from the traditional analytics definition of a metric, which is a variable of interest, populated by data from the past and present only (nothing about the future) (Evans, 2013). A probabilistic prediction of the future is not necessarily a metrics question in the traditional risk or analytics sense. However, models that address the probability of attack and the degree of vulnerability are clearly needed and one of the main open research questions in cybersecurity.

Traditional probability models address the likelihood of some event occurring as a success. In contrast, cybersecurity offers the complement of this concept, whereby a success is something not occurring. This approach is analogous to risk research applications of other

intelligent adversaries. In cybersecurity, successful attacks may occur, without the system being breached. In this case, system security is the complement of the probability of a breach, a definition of success that may be acceptable to some and not others. For example, Mission Oriented Risk and Design Analysis is a model that assesses system risk by scoring attacks based on adversary preference and impact on mission (Nicol et al., 2012). An organization's focus on prevention, detection, or reaction will lead to different standards of effectiveness and system security. As a result, metrics remains a challenging problem within risk.

In general, metrics are needed in all risk fields and are particularly hard to develop. Metrics should be robust and meaningful, informed by objectives. Consider the *community resilience* field within risk: hundreds of metrics have been proposed to evaluate community resilience in a predictive sense, but once evaluated in practice, many lack predictive ability (Cutter, Ash, & Emrich, 2014). Interestingly, the 5HP approach metrics as a predictive tool. This disconnect leads to a pressing need for risk modeling. Objective-driven analysis is extremely important for cybersecurity metrics, as it provides insight into what is valued by organizations, which in turn sheds light on what should be measured. Such analysis may include metrics for consequence, such as valuation, preference models, indirect consequences, and damage assessments. Taxonomies for collecting and sharing data are also relevant; an example of such comes from Bishop and Bailey (1996). Other opportunities for research include vulnerability metrics with attacker-defender games. An analysis of the range of consequences is important for better understanding the impact of cyber breaches, which includes how users value potential consequences and the corresponding effect on decision-making.

3.4. Resilient Architectures

Resilience has three main attributes in the SoS literature: (1) robustness and the ability to withstand attack, (2) continuing system service during an attack, and (3) restoring a system to full function following an attack (Nicol et al., 2015). SoS research in this area includes identifying the properties of resilience, deploying policies that can absorb, mitigate, and adapt to adversarial traffic, and understanding how well the system is performing during disruption. Robustness includes understanding how the degree of severity of cyber attacks could be affected by the physical system components as well as game theory approaches for human system involvement.

Opportunities for incorporating risk concepts in a resilient architecture include quantifying the probability and severity of attacks, building a knowledge base for how the system might respond, and prioritizing system services during an attack. Attacks are driven by adversaries, so models that consider adaptive response can contribute to the cybersecurity community's resilience.

The risk and resilience field has developed significantly in the past decade and offers research for resilient systems that can be applied to the hard problems. Specifically, the SoS approach to resilience lacks (1) temporal dimension and (2) principles such as robustness, rebound, flexibility, extendibility, and adaptability, as found in the literature (Woods, 2015). Beyond applying existing research, risk analysts are needed to build new methodologies to address instances where intrusions occur but are undetected. Intrusion detection is reactive, as all mitigations or corrective actions occur once a breach to the system is discovered. Modeling the probability of intrusion is a more difficult problem but is necessary for developing proactive approaches to managing the risk of an intrusion. Resilience research may also develop services

that cyber systems enable. Many systems of systems rely on online-based communication and the value of the cyber component to those systems; in particular, with respect to system service, robustness and functionality are of interest.

The risk concepts that are implicit in the other four hard problems (i.e., problems 1, 2, 3, and 5) have strong ties to resilient architectures. For example, to maintain a robust system, metrics and understanding how people make decisions under uncertainty are needed (problems 3 and 5). Also, managing risk and incorporating resilience principles more universally, either at a corporation, sector (e.g., finance), or national level requires good risk governance (problem 2) that is cognizant of how systems are generally designed, their threats (especially the different types of threats), and how people behave under uncertainty (problem 5). In general, systems need to be built to manage risks. Understanding risks, including uncertainties, allows for prioritization to mitigate risks effectively.

3.5. Understanding and Accounting for Human Behavior

The *human behavior* hard problem addresses ways humans interact with cyber systems. Systems may be built with security measures, but those measures may be compromised by human behavior. That behavior can be accidental, in that a person misuses a system inadvertently but still exposes a vulnerability, or that behavior can be malicious, in that a person interacts with a system with the intent of inflicting harm. Research in this area includes identifying actions taken by users that lead to malware infections, scoring/ranking system requirements and controls to determine potential impact on security, examining the impact of social and cognitive factors of phishing scams, applying persuasion research to classify phishing

emails to predict the likelihood of falling victim to social engineering, and processing biometrics to distinguish between an ordinary and malicious user (Nicol et al., 2015).

In many systems, human behavior drives the degree of inherent risk in the security problem. The emergence of organization insiders that have malicious intent has driven the need to examine the risk of human behavior beyond error and ignorance. Furthermore, the nature of intent is also of concern and divides the human behavior problem space. Risks and subsequent mitigations will differ for malicious and non-malicious actors. Regardless, a system must be adaptive to threats from both types of actors, and the corresponding risks must become better defined and formally addressed in the literature. Understanding actors' objectives and motivations, capabilities, how they make decisions under uncertainty (which includes both highly risk-averse and non-rational behavior) will enable more resilient systems and better governance. As a result, applications and principles of decision-making under uncertainty are essential in this hard problem. This includes the study of what people value in cybersecurity (Black, Scala, Goethals, & Howard, 2018) as well as methods to elicit value judgments for cyber risk. Defining what users value may also lead to models that enable the setting of priorities, which further supports decision-making processes.

4. CONCLUSIONS

Overall, many opportunities exist for risk analysis within the cybersecurity realm. The 5HP provide structure and a framework to the field of cybersecurity as the approach is centered around structure, design, and physical security. Aside from *human behavior,* the other hard problems mainly focus on design, instead of the risks associated with interaction with the systems. This is mostly due to the lack of probabilistic approaches in the 5HP literature and risk

not being explicitly addressed. In this paper, we argue that a formal risk approach is needed in the 5HP literature, and we outline opportunities to incorporate risk into each hard problem. Risk is a natural fit to the 5HP, as the analysis is applied to and relevant for various fields. SoS is and intends to be interdisciplinary and has a strong modeling component. Although risk may be somewhat removed from the current literature, it is welcome and appropriate for the 5HP. Cyber risk models should be a mix of system design principles and mitigation, identifying which data to protect and when, while taking a continuous improvement approach.

To realize these objectives, several approaches are needed. Examples include a value model for cybersecurity metrics, with the goal of identifying the preferred metrics and best practices for an organization to implement based upon what is valued in a secure cyber system (Scala & Goethals, 2018). What organizations value are unique and may be dependent on their demographics, such as size of firm, industry sector, previous history of attacks, etc. (Black et al., 2018). The identification of values span both the metrics and security hard problems. In addition, the effects of encryption, increased resilience, access control, and the type of attack should be investigated to determine their impact on a risk assessment. Finally, policy and human behavior can be addressed in examining system integrity and vulnerability to attack; consequences are high in government systems, such as voting processes. The opportunities are abound, and risk analysis is greatly needed to advance the field of cybersecurity.

ACKNOWLEDGMENTS

The views expressed in this paper are those of the authors and do not represent the official policy or position of the United States Military Academy, the United States Army, or the United States Department of Defense.

REFERENCES

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. (RR-1187-ICJ). Santa Monica, CA: RAND Corporation.

Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis: An International Journal*, *37*(8), 1606–1627.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis: An International Journal*, *26*(4), 907–923.

Bishop, M., & Bailey, D. (1996). *A critical analysis of vulnerability taxonomies*. Retrieved on July 15, 2018 from http://www.dtic.mil/dtic/tr/fulltext/u2/a453251.pdf

Black, L., Scala, N. M., Goethals, P. L., & Howard, J. (2018). Values and trends in cybersecurity. In K. Barker, D. Berry, & C. Rainwater (Eds.), *Proceedings of the Institute of Industrial and Systems Engineering Conference*.

Busby, J. S., Green, B., & Hutchison, D. (2017). Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. *Risk Analysis: An International Journal*, *37*(7), 1298–1314.

Canfield, C. I., & Fischhoff, B. (2018). Setting priorities in behavioral interventions: An application to reducing phishing risk. *Risk Analysis: An International Journal*, *38*(4), 826–838.

Collins, T. W. (2008). What influences hazard mitigation? Household decision making about wildfire risks in Arizona's White Mountains. *The Professional Geographer*, *60*(4), 508–526.

Cutter, S. L., Ash, K. D., & Emrich, C. T. (2014). The geographies of community disaster resilience. *Global Environmental Change*, *29*, 65–77.

Davis, G., Garcia, A., & Zhang, W. (2009). Empirical analysis of the effects of cyber security incidents. *Risk Analysis: An International Journal*, *29*(9), 1304–1316.

DiMase, D., Collier, Z. A., Carlson, J., Gray Jr, R. B., & Linkov, I. (2016). Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems. *Risk Analysis: An International Journal*, *36*(10), 1834–1843.

Evans, J. R. (2013). *Business analytics: Methods, models, and decisions*. Upper Saddle River, NJ: Pearson Education.

Farahani, J., Scala, N. M., Goethals, P. L., & Tagert, A. (2016). Best practices in cybersecurity: Processes and metrics. *Baltimore Business Review: A Maryland Journal,* 28-32.

Frederiks, E. R., Stenner, K., & Hobman, E. V. (2015). Household energy use: Applying behavioural economics to understand consumer decision-making and behaviour. *Renewable and Sustainable Energy Reviews*, *41*, 1385–1394.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis: An International Journal*. Retrieved on July 15, 2018 from https://doi.org/10.1111/risa.12891.

Garvey, P. R. (2008). *Analytical methods for risk management: A systems engineering perspective*. Boca Raton, FL: Chapman and Hall/CRC.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over-and Underregulation. *Risk Analysis: An International Journal*, *37*(9), 1644–1651.

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis: An International Journal*, *38*(2), 215–225.

Henry, M. H., & Haimes, Y. Y. (2009). A comprehensive network security risk model for process control networks. *Risk Analysis: An International Journal*, *29*(2), 223–248.

Hosenball, M., Volz, D., & Landay, J. (2016). U.S. formally accuses Russian hackers of political cyber attacks. *Reuters*. Retrieved on January 2, 2018 from https://www.reuters.com/article/us-usa-cyber-russia/u-s-formally-accuses-russian-hackers-of-political-cyber-attacks-idUSKCN12729B

Kaivanto, K. (2014). The effect of decentralized behavioral decision making on system-level risk. *Risk Analysis: An International Journal*, *34*(12), 2121–2142.

Koppel, R., Smith, S. W., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient? *Studies in Health Technology and Informatics, 208,* 215–220.

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70-86.

Merrick, J. R., & Leclerc, P. (2016). Modeling adversaries in counterterrorism decisions using prospect theory. *Risk Analysis: An International Journal*, *36*(4), 681–693.

National Institute of Standards and Technology (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved on January 1, 2018, from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Nicol, D. M., Scherlis, W. L., Katz, J., Scherlis, W. L., Dumitras, T., Williams, L. M., & Singh, M. P. (2015). *Science of Security lablets: Progress on hard problems*. Retrieved July 15, 2018, from Science of Security and Privacy Virtual Organization: from http://cps-vo.org/node/21590

Nicol, D., Sanders, W., Scherlis, W., & Williams, L. (2012). *Science of Security hard problems: A lablet perspective.* Retrieved January 1, 2018, from Science of Security and Privacy Virtual Organization: https://cps-vo.org/node/6394

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis: An International Journal*, *31*(3), 497–512.

Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis: An International Journal*, *38*(2), 226–241.

Ponemon Institute. (2015). *The rise of nation state attacks*. Ponemon Institute, CounterTack, Inc., and MCSI.

Ponemon Institute. (2016). *2016 Cost of Data Breach Study: Global Analysis*. Ponemon Institute and IBM Corporation.

Rao, N. S., Poole, S. W., Ma, C. Y., He, F., Zhuang, J., & Yau, D. K. (2016). Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. *Risk Analysis: An International Journal*, *36*(4), 694–710.

Santos, J. R., Haimes, Y. Y., & Lian, C. (2007). A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies. *Risk Analysis: An International Journal*, *27*(5), 1283–1297.

Scala, N., & Goethals, P. (2018). *A model for an inventory of cybersecurity values: metrics and best practices.* Working paper.

Symantec Corporation. (2016). *Internet Security Threat Report* (Volume 21). Mountain View, CA: Symantec Corporation. Retrieved on January 1, 2018, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Thompson, R. R., Garfin, D. R., & Silver, R. C. (2017). Evacuation from natural disasters: a systematic review of the literature. *Risk Analysis: An International Journal*, *37*(4), 812–839.

U.S. National Security Agency. (2018a). *Science of Security and Privacy: List of publications.* Retrieved January 1, 2018, from https://cps-vo.org/group/sos/lablet/reporting/ncsu

U.S. National Security Agency. (2018b). Science of Security and Privacy: Goals of the Science of Security virtual organization. Retrieved July 17, 2018, from https://cps-vo.org/group/SoS/about

van Zadelhoff, M. (2016). The biggest cybersecurity threats are inside your company. *Harvard Business Review*. Retrieved January 1, 2018, from https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Whitler, K. A., & Farris, P. W. (2017). The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, *57*(1), 3–9.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5–9.

Zhuang, J., & Bier, V. M. (2010). Reasons for secrecy and deception in homeland-security resource allocation. *Risk Analysis: An International Journal*, *30*(12), 1737–1743.