Proceedings of the 2018 Industrial and Systems Engineering Conference
K. Barker, D. Berry, C. Rainwater, eds.

Values and Trends in Cybersecurity

Lorraine Black and Natalie M. Scala
College of Business and Economics
Towson University, Towson, MD 21252

Paul L. Goethals
Department of Mathematical Sciences
United States Military Academy, West Point, NY 10996

James P. Howard, II
Information Technology Services Department
The Johns Hopkins Applied Physics Laboratory, Laurel, MD 20723

Abstract

This research examines values in cybersecurity and their applied impact on organizations. The Science of Security (SoS) initiative at the United States Department of Defense has identified five major research themes, or "hard problems," in cybersecurity, including a problem devoted to Security Metrics Driven Evaluation, Design, Development, and Deployment. Recent research has examined how both SoS-sponsored studies and best practices for metrics can be implemented in organizations, which varies by industry and by organization. In this paper, we examine how the sponsored research can be applied to increase the cybersecurity posture of organizations, given that no two scenarios are alike. First, we surveyed information technology professionals as well as small legal firms and solo practitioners to understand what they valued in a secure cyber system. Then, we investigated relationships between the respondents' identified values and their organizational history of attacks and breaches. Finally, we identified dichotomies in values between professionals trained in computer technology and those who are not. The research categorizes behaviors that can promote securing cyber systems as well as defines model inputs for identifying continuous improvement actions that increase security.

Keywords
Cybersecurity, metrics, value model, Five Hard Problems

1. Motivation

Concern for cybersecurity has greatly increased, as the quantity and severity of breaches continues to rise [1]. Cybersecurity is ever evolving, so to ensure security and protection, firms must successfully adapt to threats and adversaries. However, the actions one organization takes to adapt may be different from another organization. Hence, metrics and best practices are needed to help guide these institutions in making security decisions.

The Science of Security (SoS) initiative at the National Security Agency focuses on scientific cybersecurity foundations and promotes interdisciplinary research. SoS organizes cybersecurity research into five major veins, or hard problems: Resilient Architectures; Policy Governed Secure Collaboration; Security Metrics Driven Evaluation, Design, Development, and Deployment; Understanding and Accounting for Human Behavior; and Scalability and Composability [2]. Developing security metrics is particularly challenging, as systems are extremely complex, and small nuances may have significant impact on the overall security posture [2]. Furthermore, SoS research considers metrics as practices that can aid in preventing breaches, which does not align with the traditional metrics definition from analytics [3]. Generally speaking, metrics in cybersecurity are best practices for system management. The SoS initiative alone has indexed over 110 papers that develop metrics and best practices [4]; a good literature review of metrics papers outside the SoS realm can also be found in the literature [3]. Even though extensive research has been done to define candidate metrics and best practices, the literature lacks implementation advice. Therefore, as part of a larger research project, we develop a value model for metrics and best practices that enables an organization to identify preferred metrics and best practices to implement to secure their cyber systems. No organization can implement hundreds of metrics; this model customizes metrics according to how the organization approaches cybersecurity.

Attributes valued in cybersecurity are not consistent across organizations and should not be standardized. Companies that have dedicated information technology (IT) teams and large budgets can implement more and different controls versus a novice small business with a handful of computers and mobile devices. A recent Pew Research study concludes that Americans do not trust in cybersecurity and fail to implement best practices in their daily lives [5]. Understanding how and what is valued is essential to building decision models that accurately and continuously improve cybersecurity posture. Therefore, we seek to understand what organizations value in a secure cyber system, as well as how those values change based on the type of industry, size of firm, and cybersecurity maturity, among other factors. To examine this, we performed surveys of IT professionals and solo-practicing or small firm legal professionals. We considered these two groups, as IT professionals have formal training and career experience in cybersecurity, while legal professionals may not have such training. Furthermore, legal professionals at small firms or practicing independently may be considered as a proxy for small businesses, even though attorneys are held to additional ethical data security standards in order to maintain attorney-client privilege. Results from these surveys were then used as data inputs to the value model created as part of the overall research.

This research specifically seeks to identify values provided by survey respondents and examine any differences in values due to organization demographics and cybersecurity maturity. We discuss our survey protocol, analyze the collected data, and provide concluding insights. We begin with a discussion of the survey protocol.

2. Values of a Secure Cyber System

2.1 Survey Protocol

Two separate anonymous surveys were created: one tailored for IT professionals and another for legal professionals who are solo practitioners or at small firms. The survey for IT professionals began with demographics questions such as years of experience in cyber operations, industry that he or she supports, history of organizational breaches, and the size of firm. The legal professionals survey also began with demographics questions but with additional queries related to potential instances of fraud and insider abuse of data, as lawyers are held to attorney-client privilege standards. Because the legal professionals survey was targeted for small firms and solo practitioners, questions from a survey conducted by Ryan [6] were included, as that survey specifically addressed cybersecurity practices at small businesses. The overall goals of the surveys were to understand a respondent's level of cybersecurity understanding, any history dealing with breaches and data compromise, and what is valued in a secure cyber system.

The survey for IT professionals was administered online via Qualtrics during summer 2016 and advertised through professional listservs, social media, and authors' personal networks. In total, 98 responses were collected, with 79 responses being usable. The survey for legal professionals was administered both online and by paper mail during fall 2016 and advertised using both social media and contacts from the Bar Association directory for a mid-Atlantic state, as well as authors' personal networks. In total, 47 responses were collected, with 31 responses being usable.

For the IT professionals survey, 73% of respondents were from academia, with others from the following industries: computers and technology, engineering, banking, government, transportation and distribution, aerospace, energy utilities, entertainment and media, healthcare, military and defense, and retail and wholesale sales. The IT professionals were very experienced in cyber operations, as 52% of respondents reported more than 10 years of experience, 23% had 5-10 years of experience, 21% had less than 5 years of experience, and only 4% had no experience in that work role. A job title of Chief Information Officer or equivalent comprised 13% of the respondents, while 23% held the title of Director of Cyber Operations or equivalent, and 24% serve as the Manager of Cyber Operations or equivalent. The remaining respondents held other work roles. A perception of the organization's networks as very secure was reported by 5% of respondents, secure by 52%, neither secure nor unsecure by 27%, unsecure by 15%, and 1% did not specify. Finally, 52% of IT professionals reported a previous breach of the organization's systems (with 57% of academic professionals reporting a breach), 23% reported no breach, and the rest did not provide a response.

All respondents to the legal survey were attorneys. All but 3 respondents, or 90%, were solo practicing as small businesses, with 68% having no more than 10 employees. Comfort with technology varied, as 10% reported being moderately uncomfortable, 6% slightly comfortable, 10% neither comfortable nor uncomfortable, 39% moderately comfortable, and 35% extremely comfortable. A vast majority, 81%, have antivirus or antimalware software installed on their computers, with 6% each reporting either no such software or unsure of installation, and 7% not providing an answer. Only 16% of the respondents reported a breach, but 10% were unsure if one had occurred. The rest reported no breach or did not answer the question. Fraud was experienced by 7% of the respondents, while 13% were unsure if fraud had occurred. The rest reported no instance of fraud. An experience with insider abuse of data privileges was reported by 58% of the respondents, while 13% were unsure if abuse had occurred. The rest did not have such an experience or did not answer the question. Finally, 29% of the respondents experienced email phishing, 16% were unsure, and the rest reported no experience with phishing.

Although the sample size for each of the surveys are small, we deduce that many legal professionals at small firms and solo practitioners may not have a solid understanding of cybersecurity. IT professionals seem to have a stronger grasp of cybersecurity principles, which should be attributed to their training and career work in this area. This is an important (although obvious) point: those who do not have formal training or career experience in cybersecurity struggle with understanding, and therefore managing, the security of their networks and data. Accordingly, those without a background in cybersecurity or the support of someone with one are at greater risk of breach.

2.2 Reported Values

Both populations were asked to identify values or characteristics of a secure cyber system. Respondents were given opportunities to identify multiple values. The goals of this exercise were to collect an inventory of values to use as a dataset for the overall value model and to analyze if reported values differ between and/or within the populations. In summary, 74 unique values were provided by the IT professionals, and 44 unique values were provided by the legal professionals. The question was freeform response, and no examples of values or prompts were given, so that respondents would not be biased in their response. As a result, a mix of responses was elicited. Many respondents provided the same values or values with related definitions. Therefore for ease of analysis, we grouped the values into themes. Table 1 presents the cybersecurity themes and the corresponding values assigned to each theme; note that all values provided in the surveys are listed in Table 1, and each value is assigned to one and only one theme. Each value is listed once, even if multiple survey respondents within the same population provided it. Note that the values reported from the IT professionals in Table 1 are also included in another study [3], and are listed here for ease of reference.

3. An Analysis of Values Between Populations

Critically analyzing the values in Table 1 leads to identifying similarities and differences among not just the themes but also the values reported within the themes. Some of these points, which are qualitative in nature, can be deduced from the current sample but may be extended to larger samples or the overall population. Other analytical points are identified via quantitative evaluation.

3.1 Qualitative Analysis

Each of the 15 themes reflects components of or attributes to consider in a secure cyber system. An interesting point in comparing the two populations and the values they chose for their respective cybersecurity domains is the prevalence of their word choice. For example, legal respondents did not provide values related to automation, awareness, training, or policy. They also completely avoided the terms “control,” “governance,” and “monitoring” in their open description of favored attributes, language that is used consistently throughout each of the themes by the IT professionals. In contrast, legal professionals frequently noted the words “data,” “information,” “privacy,” and “protection,” verbiage that cannot be found in any of the IT professional responses. This qualitative comparison seems to suggest that IT professionals are more concerned with *prevention* by means of a centralized process where the emphasis of security is on the system, whereas legal professionals place greater importance on *protection* and *privacy* via the security of the data itself. This may also suggest a more proactive versus reactive policy when it comes to the organization’s cybersecurity posture.

Table 1: Values Organized by Theme (Adapted from [3])

Theme	Values Provided by IT Professionals	Values Provided by Legal Professionals
Access Controls	(i) Administrative controls, (ii) Control of information assets, (iii) Authenticated access, and (iv) Controlled access to personalized data	(i) Protection of client information, (ii) Confidentiality of information, (iii) Privileged data, (iv) Client files, (v) Protection of data, (vi) Protecting attorney-client communication, (vii) Confidentiality/Security, (viii) Ease of appropriate access, (ix) Confidentiality, (x) Sharing of info, (xi) Safeguarding client data, (xii) Privacy of data, and (xiii) Maintenance of privacy
Automation	AI driven (Artificial Intelligence)	N/A
Awareness	(i) Awareness, (ii) Employee awareness, (iii) Informed user base, (iv) Phishing awareness, (v) Security awareness, and (vi) User awareness	N/A
Consistency	Consistent	N/A
Monitoring	(i) Continuous monitoring, (ii) Event monitoring, (iii) Flow monitoring, (iv) Scanning, (v) Network monitoring, and (vi) Reduces false positive rate	(i) Constantly monitoring online site, (ii) Discovery, (iii) Hacking, (iv) Blocking unsecure external email, and (v) Preventing access to potentially harmful websites
Human Behavior	(i) Behavior based, (ii) Communication with community, (iii) People, and (iv) Skilled staff or team	(i) Employee misuse, and (ii) Insider access abuse
Other	(i) Identity management, (ii) Non-invasive, (iii) PeopleSoft, (iv) Technology, (v) Tooling, (vi) Dependence, (vii) Contextual data, and (viii) Exercises	(i) Data breaches, (ii) That the system can be breached, and (iii) Software problems
Policy	(i) IT security governance, (ii) Procedure to policy authority document linkages, (iii) Process, (iv) Risk posture, (v) Risk assessment, and (vi) Comprehensive security program	N/A
Prevention	(i) Encryption, (ii) IDS (intrusion detection systems), (iii) Intrusion prevention, (iv) IPS (intrusion prevention systems), (v) Prevention, (vi) Strong two factor authentication, (vii) Secure authentication and certificates, (viii) Identification of vulnerabilities, (ix) IAST and RASP (interactive application security testing and runtime application self-protection), and (x) Validated inputs	(i) Virus protection, (ii) Data protection, (iii) Anti-virus, (iv) Data loss, (v) Security of data, (vi) Virus and malware, (v) Viruses, (vi) Protection from viral attacks and phishing, (vii) Virus attacks, and (viii) Viruses
Resilience/Design	(i) Design, (ii) Firewall, (iii) Multiple defensive layers, (iv) Next-generation firewall (NGFW), (v) Red forest, (vi) Red team, (vii) Multi-factor authentication, (viii) Integrity, (ix) Most of security features in AWS, (x) Pen test (penetration testing), (xi) Resilience, and (xii) Secure data APIs (application programming interfaces)	(i) Constantly updating online site, (ii) Business interruption, (iii) Integrity of data, (iv) Data sabotage, (v) Data availability, (vi) Protection from destruction, (vii) Preventing disruptions, (viii) Uninterrupted operation of systems, and (ix) Ability to access systems remotely while maintaining security
Robustness	Robustness in the face of attack	N/A
Threat Detection	(i) Event management, (ii) Ability to separate network traffic, (iii) Defense in depth, (iv) Detection, (v) Early threat detection, (vi) Threat detection, (vii) Threat modeling, and (viii) Unique tools that recognize threats	(i) Theft of data, and (ii) Data theft
Training	(i) Training, (ii) User training, (iii) Developer training, and (iv) Administrator training	N/A
Usability/Transparency	(i) Transparent to users, (ii) Alerts/notification, and (iii) Usability	N/A
Fraud	N/A	(i) Fraud, and (ii) Identity fraud

Another point that seems to resonate in an analysis of the values among the two populations is with respect to the human dimension. Values or themes such as training, awareness, encryption, authentication, and access control are all mechanisms established to reduce or eliminate the possibility of human error. It is realistic to deduce that IT professionals overseeing or managing computer security for a host of employees are more likely to be attuned to the impact of human factors than that of the legal professionals. The survey responses appear to account for this behavior based upon the clear presence or absence of these expressions among each population.

Finally, two themes - *Prevention* and *Resilience/Design* - seem to illustrate how much the two populations differ in their position, knowledge, and perspective of cybersecurity. The legal professionals take a one-dimensional perspective for *Prevention*, with a focus primarily on protecting information from loss due to viruses and malware. In contrast, the IT professional perspective considers threats entering the system (for which IDS and IPS are used to detect and prevent), as well as the information departing the system or organization (for which encryption, authentication, and validation would support). A similar posture is observed with regard to the *Resilience/Design* theme. The legal professional focus is on avoiding disruption and interruption to both the data and the system, while the IT professional is concerned with internal defense mechanisms (such as a firewall) and the external means for protecting information (such as authentication). These points suggest that one population tends to see the cybersecurity threat more as a symmetric problem – the organization against an external adversary, versus that of an asymmetric threat, where the hazards may be both internal and external to the institution.

3.2 Quantitative Analysis

Experiencing the breach of a cyber network may be a traumatic event for an organization. Customer and corporate data may be compromised; as a result, breaches can lead to customer lack of trust [1]. Public relations may attempt to repair the trust, but the systems themselves must be secured. As a result, we hypothesize that organizations that have experienced breaches or other forms of data compromise approach values differently.

To investigate further, we consider Fisher's exact test, which identifies information on the significance of observed differences between two proportions and insights as to categories or demographics that account for the differences [7]. While the chi-square test is appropriate for large sample sizes, a Fisher's exact test is used for small sample sizes. The size of each sample proportion may differ, as this does not affect the outcome of the analysis. We tested whether values and corresponding themes identified in our survey are contingent upon if an organization was breached. Therefore, for each theme, we consider reported values, separated by respondents reporting breaches or no breaches. We then compare those counts to the total number of values reported. For example, 5 legal respondents reported a breach, and 22 respondents did not report a breach. Four respondents were either unsure or did not provide a response. Thus, for the 27 respondents who clearly reported a breach or lack thereof, we identified the number of respondents who reported a value within each theme. For each theme and each population, we then employed the Fisher's exact test for evaluating the hypotheses H_0: No difference in values between breached and not breached respondents, versus H_1: A statistical difference in value exists between breached and not breached respondents. Table 2 depicts the tests that yielded significant *p*-values.

Table 2: Significant Fisher's exact tests

	Prevention: IT		**Monitoring: Legal**		**Other: Legal**	
	Value Included	Not Included	Value Included	Not Included	Value Included	Not Included
Beached	2	7	3	2	2	1
Not Breached	39	11	2	20	3	21
p-value	0.0022		0.0300		0.0790	

Regarding the theme of *Prevention*, IT professionals are concerned with preventing their cyber systems from internal and external attacks. With regard to *Monitoring,* legal professionals worry about outside forces breaching their data and email; breached professionals especially seek protection from harmful websites and email links. For legal professionals, the *Other* theme includes data breaches, that the system can be breached, and software problems. These choices support the idea that legal professionals may be more concerned with data and email breaches, a connection that is natural, given that legal professionals need to maintain attorney-client privilege. Overall, surveyed legal professionals want secure email and web via monitoring of systems for breaches, while IT professionals want protection from breaches by working to prevent them before they occur. Legal professionals address breaches after they occur; in contrast, IT professionals work to prevent breaches before they occur. This may suggest that legal professionals either experience less breaches or are not fully aware of cyber breaches that may have occurred. It seems reasonable that those who have experienced a cyber intrusion put greater emphasis and awareness on themes such as *Monitoring* and *Prevention*.

Moreover, some tests may indicate additional findings associated with the null hypothesis. For instance, we found no difference in values for organizations that had or had not been breached and attributes such as demographics or the size of industry. It has been suggested by various cybersecurity reports that both small and large organizations are at risk of a cyber breach, one reporting that 71% of data breaches occur in businesses with less than 100 employees [8]. Although there are clearly more small businesses than large businesses in the U.S., our results provide support for this same conclusion. In addition, the absence of any correlation between how secure the respondents rated their organization and whether they experienced a breach or not tends to bolster the notion that no institution is truly removed from the cybersecurity problem. Even large organizations with a greater monetary capacity for defending their infrastructure are experiencing data breaches.

4. Conclusions and Future Work

In summary, organizations value different attributes when securing their cyber systems. We are developing a value model for best practices in cybersecurity and, in this paper, show its application to two different organizational classes of participants. Further, this model can be customized to the organization to accommodate differences in capability and risk. In addition to the value model, an analysis of the responses to the survey instrument shows how those risks differentiate across industries. Finally, we have observed that risk management and defensive capability are not necessarily indicative of the preventing breaches. Future work includes examining how risk affects cybersecurity decisions, especially in high consequence scenarios such as voting systems. What organizations care about should directly affect their risk profile and that profile, along with a model to support best practices, leads to holistic management and understanding of cyber systems.

Acknowledgements

The authors would like to thank Rachael Artes, Jasmin Farahani, Rachel Fredman, and Alexander Thierer for their help with collecting and managing the survey data. 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 Department of Defense.

References

1. Farahani, J., Scala, N.M., Goethals, P.L., and Tagert, A.C., 2016, “Best Practices in Cybersecurity: Processes and Metrics,” Baltimore Business Review: A Maryland Journal, 28-32.
2. 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
3. Scala, N.M., and Goethals, P.L., 2018, “A Model for and Inventory of Cybersecurity Values: Metrics and Best Practices,” working paper for journal submission.
4. Science of Security, 2016, “SoS Documents: By Topic,” retrieved from http://cps-vo.org.
5. Olmstead, K., and Smith, A., 2017, “Americans and Cybersecurity,” retrieved from http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.
6. Ryan, J.J.C.H., 2000, “Information Security Practices and Experiences in Small Businesses,” Ph.D. dissertation, The George Washington University.
7. McHugh, M. L., 2013, “The Chi-square Test of Independence,” Biochemia Medica, 23(2), 143-149.
8. Verizon Enterprise, 2017, “2017 Data Breach Investigations Report,” retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/