Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment

Mark A. Clark
Kogod School of Business
American University
mark.clark@american.edu

J. Alberto Espinosa
Kogod School of Business
American University
alberto@american.edu

William H. DeLone
Kogod School of Business
American University
wdelone@american.edu

Abstract

Cybersecurity governance is a critical issue for organizations engaged in a constant struggle to protect their data, brand, customers, and other assets from malignant actors. The nature of what constitutes successful cybersecurity practices and governance, however, is not yet clear, in part because an appropriate measure for cybersecurity success is not likely to be singular or simple. In this qualitative study, we explore perspectives of cybersecurity success through interviews representing various technical and non-technical roles across a variety of organizations, then provide a preliminary framework for understanding dimensions of cybersecurity success (financial, information integrity, operational, and reputational) as well as their associated knowledge domains and alignments.

1. Introduction

Cybersecurity incident response has become a nearly ubiquitous concern as attacks and breaches have struck organizations across business, not-for-profit, and governmental sectors. Indeed, the cost of cybercrime is estimated to reach $2 trillion dollars by 2019; and despite the increasing its severity, only 38% of companies reported in a survey that they were prepared to respond effectively to breaches and attacks (https://securityintelligence.com/20-eye-opening-cybercrime-statistics/). Organizations seeking to address such cybersecurity threats must develop governance policies which provide a goal framework for both technological and human systems, including managing the human performance and knowledge resources of the firm [1]. A significant challenge to such a framework is a lack of understanding of what constitutes success in the cybersecurity domain, especially beyond the information system itself. This understanding is needed to structure the knowledge required to inform cybersecurity governance policies that will support these broad forms of success. Once these areas are better understood, they can enact a comprehensive cybersecurity governance program, which we define as *"the sum total of an organization's efforts to protect its digital assets from unauthorized access and control, and by extension, protect further assets (e.g., people, intellectual property, finances) which could be compromised by unauthorized access."*

In contrast to the popular adage, both cybersecurity success and failure "have many fathers". In other words, a full understanding of what constitutes cybersecurity success for organizations is not likely to be singular or simple, reflecting the multiple components involved in governance systems (e.g., technology, decision structure, human behavior) as well as the variety of precipitating events and damages associated with data breaches (defined as *"unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data"* [2]. To this point, less than half of the reported data security breaches (48%) result from actual attacks by malicious agents; most such breaches are caused more by human errors and system failures [3]. With some exceptions, attempts to address cybersecurity breaches have generally relied upon technological solutions designed to scan incoming data for potential issues. However, organizational psychologists have recently begun to focus on the human psychosocial elements of cybersecurity, and particularly on the individual, team, and organizational factors that facilitate successful responses to cyber breaches. Because cybersecurity affects nearly every person and every role in an organization's structure, each with a perspective grounded in distinct knowledge, such a focus means identifying the collective processes and emergent states that contribute to more effective information sharing and application to what are often novel forms of attacks [1, 4, 5].

URI: https://hdl.handle.net/10125/64266
978-0-9981331-3-3
(CC BY-NC-ND 4.0)

Successful cybersecurity practice therefore requires alignment of knowledge among various individuals, roles and systems, such that a knowledge schema is formed at the organization level. To understand this cybersecurity-focused knowledge schema, we lean on team cognition research [6-8] which provides frameworks describing knowledge structure and content, such as degree of sharedness and related dimensions [9].

This study explores what constitutes cybersecurity success in organizations, in the perspective of organizational actors, through a qualitative inquiry using grounded theory method, including review of related literature, interviews with key informants, and thematic coding. We build upon the rich and established research literature on information systems (IS) success [10, 11], where proposed frameworks and empirically-tested constructs have focused on the data system itself. Cybersecurity, however, is a more complex endeavor going beyond technologies to also include people across varying roles within an organizational structure, and related processes that influence governance operation. Consequently, we propose that the appropriate definition and measure for cybersecurity success is not singular, but is tightly interrelated with multiple organizational structures, goals, processes and actors. Thus, the primary research questions for this study are:

1. *How do organizations conceptualize and measure their cybersecurity governance effectiveness?*
2. *How do such perspectives on cybersecurity success differ across organization level and roles?*

Once success is defined, effective cybersecurity governance is enacted through the content and structure of knowledge, including risk perspectives, held by the variety of internal and external stakeholders across roles and levels. These include board members exposed to risk and liability, executives monitoring financial returns, technical staff protecting hardware and software resources, middle managers ensuring continuity of their functional operations, and customers concerned with identity theft. Therefore, as a secondary focus, in this study we also investigate the content domains and alignment structure of knowledge associated with cybersecurity success.

3. *What knowledge domains and alignments are relevant to cybersecurity success?*

We investigate and further develop these questions through interviews with practitioners who fulfill varied roles across multiple levels of a diverse set of organizations in several industry sectors, informing our understanding of effective cybersecurity practices, measures, and governance. We then offer the findings from this qualitative approach as a preliminary framework for understanding cybersecurity success.

2. Extant Theory

To better understand what constitutes cybersecurity success, we review the extant literature in this area.

2.1 Cybersecurity Success

The research literature suggests that IS project performance consists of two distinct dimensions: *process performance* and *product performance* [12-14]. Process performance has to do with the execution of the project and is typically measured by on-time/ on-budget project completion, user participation, and team member satisfaction and morale [13, 15, 16]. Product performance has to do with the actual information system developed, including system quality, functionality, impact, and user satisfaction with the system. Based on these studies and DeLone and McLean's [11] updated IS Success Model, our conceptualization and interview questions includes several measures of IS project success: on-time completion, within-budget completion, system costs/effort, meeting system requirements, system quality, user satisfaction, project team satisfaction, system use, and net system benefits.

In their seminal paper [10] and follow up 10-year review [11], DeLone and McLean [11] suggested measures of *system success*, including system quality, information quality, service quality, system use, user satisfaction, individual impact and organizational impact [10, 11]. This IS Success Model reports on the numerous measures that have been studied under each of these success dimensions. Organizational impact measures include such measures as improved organizational productivity, operating cost reductions, sales growth and increased profits. These measures can serve as a guide to identify potential outcomes of cybersecurity success.

The present study builds upon this body of research in IS success in several ways. First, cybersecurity is not a technological system per se, but an ongoing activity meant to protect not just systems and information, but also financial concerns, privacy, reputation, operations, processes and organizational outcomes. As such, it is a broader and more complex construct to define. Second, consistent with the standards set forth by the National Institute of Standards and Technology (NIST) [17] we view cybersecurity success as a two-phase endeavor: ***(1) Pre-Incident*** – aimed at managing risk and preventing breaches. This phase encompasses three NIST functions: *Identify*, *Protect* and *Detect*; and ***(2) Post-Incident*** – aimed at the expedient and effective restoration of normal operations. This phase

encompasses the other two NIST functions: *Respond* and *Recover*. Therefore, cybersecurity success must account for both, the extent to which breaches are prevented and the timely recovery of normal organizational systems and functions.

2.2 Shared Knowledge in Cybersecurity

While much has been written about cybersecurity practices, risk and governance, very little research has explored how the domain knowledge and its structural alignment across organizational members may influence risk exposure and potential business losses. Cybersecurity-related knowledge may be held differentially across organizational roles and levels; for instance, members of the information security team may share the basics of security protocols with product-line managers, but both roles would also have differentiated, unshared knowledge. Without an appropriate sharing of knowledge, decisions would be made in isolation, such as when cybersecurity protection resources are budgeted only to safeguard technical assets without regard for other perspectives. However, technical breaches, such as those suffered in recent years at the City of Baltimore, Starwood, Target and Sony, demonstrate that companies must account for risk of legal liability and loss of business value that were previously unimaginable. We argue that understanding the manner in which knowledge about cybersecurity is shared across organizational levels and entities is necessary to mitigate its associated risks and to deal more effectively with breaches when they occur. Thus, our research is designed to capture viewpoints which may reveal multiple perspectives on what constitutes cybersecurity success.

Cybersecurity incident response maturity models have generally focused on both the technical and individual capacities of in the incident response systems. For example, the National Cyber Security Centre in the Netherlands identified 5 areas of cyber security incident response maturity: foundation, tools, processes, organizational and human [18]. The foundation element refers to the creation and structural establishment of the incident response system. Tools and processes refer respectively to the automation and the technological infrastructure supporting incident response and the establishment of formal core services of the incident response system. The organizational element refers to formal governance structures guiding incident response. Finally, the human element refers to the incident responder's knowledge, skills and abilities.

Tetrick and colleagues [1] argued that this and similar incident response models fail to capture the key elements related to social functioning in incident response collectives. Along this line, Zaccaro and colleagues [5] noted that cybersecurity incident response typically entails collective knowledge work in which multiple analysts think and work together to make sense of incoming incidents and develop remediation solutions. Accordingly, Tetrick et al [1] specified social maturity as another key element in incident response models. They defined such maturity as the degree to which incident response teams and multiteam systems possess *"the capacity to collaborate well together in accomplishing [their] mission [and] to develop an effective synergy among…members"* (p. 48).

The effective sharing of information among cybersecurity stakeholders represents a critical element of incident response social maturity [5]. Information sharing about cyber incidents occurs not only within members of an incident response team, but also with other teams within a multi-team incident response system [see 4 for a description of such systems], as well as with teams in other partnering organizations. The speed, efficiency, and effectiveness of cyber incident remediation depends heavily on the quality of such information sharing and subsequent response coordination. In turn, information sharing quality is largely a function of the shared knowledge structures and networks established to guide and regulate such activities during incident response. As studies have shown [19], the extent and manner in which team members share knowledge has a strong impact on project success.

3. Methods

3.1 Qualitative Inquiry and Grounded Theory Method

Given the incomplete understanding and lack of a widely accepted model of cybersecurity success, we adopted grounded theory method, widely used in IS research [20, 21], to qualitatively explore the parameters of the success construct within its natural contexts, interviewing key informants and comparing their responses to discern themes and distinctions. Consistent with this method, we developed our basic interview questions from existing literature [22, 23]. We immersed ourselves in the extant knowledge of cybersecurity success, we read numerous secondary sources including scholarly works (e.g., ethnographies), business press, trade publications, and traditional media accounts. We then developed an initial coding scheme through open coding of the first few interview transcriptions aimed at uncovering general recurring themes of interest [24]. We then used the resulting themes once more, case by case, to contrast similarities and differences across roles and organizations [25], with consensus from three of the researchers involved in this study. We then analyzed the relationship among these themes.

This approach enabled us *"to uncover and understand what lies behind any phenomenon about which little is yet known"* and *"gain novel and fresh slants"* that build on existing theory [23, p.19]. We used a parallel processing approach to apply a key tenet of Grounded Theory – the iteration among new data, early data and existing research [26]. We then iterated informal and formal qualitative analyses with multiple raters, employing hand coding and software-supported analysis (i.e., NVivo©). Finally, we discussed the resulting themes and factors within our research team.

3.2 Sample

We interviewed a total of 17 experienced practitioners, drawn through a modified convenience sample technique which utilized cold calls and existing connections of the authors to contact a diverse array of organizations. The authors also developed connections through speaking at conferences and panels on cybersecurity-related topics. To gain perspectives of the variety of organizational roles who are jointly responsible for the cybersecurity of the organization, we targeted both technical and nontechnical interviewees across a variety of roles and organizational levels, including executives, members of boards of directors, managers, and line staff in organizations spanning several economic sectors, including insurance, consulting, healthcare, energy, and higher education. Our study sample is summarized in Table 1.

Table 1. Study Sample

Participant Role	Organization Type				Total
	Corporate	Government	Institution	Consulting & Services	
Board	2		1		**3**
Legal	1				**1**
Audit	1				**1**
CIO			1		**1**
CISO	1		1		**2**
Cybersecurity Specialist	1	1	1	5	**8**
Analyst				1	**1**
Total	**6**	**1**	**4**	**6**	**17**

All interviews were recorded and transcribed, resulting in over 120,000 words and 240 pages of material. The study reported in this paper is based on a preliminary analysis of these interviews by two of the three authors, who also conducted the interviews, and a separate in-depth analysis of the first 9 interviews by the remaining author and two research assistants.

3.3 Interview Protocol

The semi-structured interview protocol consisted of open-ended questions focusing on a set of related themes. The most relevant questions were the following 3 categories:

(1) conceptualization of cybersecurity success (e.g., What ends does your organization seek from your cybersecurity program?)

(2) classification of cybersecurity breach severity (e.g., Please give examples of what you consider to be a (i) critical; (ii) serious; (iii) minor cyber event. What factors lead you to classify these events?); and

(3) extent of organizational knowledge on pre-incident (identify, protect and detect) and post-incident (response and recover) phases of the NIST framework.

During the interviews we focused participants on contrasting what they knew, what others knew, and what colleagues should know about cybersecurity governance. Given the semi-structured nature of the interviews, interviewers were free to explore interesting themes in more detail and were not required to ask every question in the protocol.

3.4 Analysis

Following Miles and Huberman [27] and Strauss and Corbin [23], our literature review and research questions played a sensitizing role, suggesting the a priori constructs. Following the initial set of interviews, the two authors who conducted the interviews recorded their impressions, including development of an initial framework of cybersecurity success. In keeping with principles of qualitative inquiry, our analysis granted preliminary validity to all dimensions of cybersecurity success revealed in the interview process, as long as they increased the parameters of the construct. The frequency with which dimensions were mentioned was noted, although this did not necessarily further validate the dimension's utility. We then compared coding with the goal of attaining what Kvale terms "dialogical intersubjectivity," [28, p.154] a form of reliability via discussion regarding complex phenomena. Two authors, who conducted the interviews, pulled preliminary themes from the interviews. The third author and two research assistants, none of whom participated in the interviews, conducted separate coding and thematic analysis of the data by using NVivo© software. As a final step, the first two authors reviewed and refined the coded themes, identifying relations among them.

4. Findings

4.1 Cybersecurity Success

Our findings provided strong evidence that there are multiple dimensions of cybersecurity success which reflect the desire to achieve stable fulfillment of organizational goals, measured as size, depth, scope, or duration in one or more of these aspects of the system: financial, reputational, operational, and information integrity. This is consistent with prior arguments from DeLone & McLean [10, 11] and Jennex et al. [29]. These dimensions of cybersecurity success often seemed to fit with the strategic goals of their particular industry, and also the role of the person interviewed, with some overlap across these perspectives. This can be seen in the frequency that the dimensions were mentioned in the interviews: (1) financial impact (15 interviews, 29 references); (2) system integrity/ information protection (14 interviews, 33 references); (3) operational continuity or disruption (11 interviews, 21 references); (4) organizational reputation (12 interviews, 31 references); and (5) temporal or quantitative extent of a cybersecurity intrusion (7 interviews, 9 references). Next, we discuss these key dimensions, listed in Table 2, in more detail, and also refer to additional important success indicators mentioned by our interviewees, such as regulatory compliance, health outcomes, intellectual property, and others.

Table 2. Cybersecurity Success Dimensions

Key Dimensions (Impact Areas)	Impact Size, Scope, Temporality Examples
Financial Impact	Magnitude of revenue protection & cost avoidance; impact on earnings
System Integrity & Information Protection	Number and importance of personal records exposed to theft
Operational Continuity or Disruption	Extent and duration of disruption; Healthcare mortality
Organizational Reputation	Extent and duration of reputational damage

4.1.1 Financial

For private enterprises and many not-for-profit organizations, cybersecurity effectiveness was evaluated in terms of revenue protection and/or cost avoidance at some point in the sequence of organizational factors that comprise their value chains [30]. Even in not-for-profit organizations, financial considerations were important in providing and sustaining resources, in ultimate pursuit of stakeholder fulfillment [31]. For publicly traded companies this financial impact extended to the influence of cybersecurity incidents on stock price and shareholder value. Thus, when considering a given point in time, most success measures may have an impact, at least indirectly, on the financial bottom line, as this participant's comment illustrates: *"You know if I'm a pharma company then ... if somebody steals the secret formula ... that is a major loss. Or if it's a movie studio somebody … gets an early copy of the release … so in most cases it's a downstream financial loss."*

In this case, information integrity is compromised (i.e. intellectual property is stolen), which will result in lost revenue, ultimately limiting the ability of the organization to fulfill its mission.

Also, organizations that have experienced personal information breaches may pay out a per-person fee for credit monitoring. The impact of breaches, such as denial of service attacks or others with operational disruptions translate into lost revenues. Reputational damage (discussed below) can also be assessed by its impact on customer loyalty and ultimately by lost sales. Additionally, cybersecurity incidents often have associated costs of remediation (e.g., ransom payment) and recovery. Therefore, the overall measure of success is the avoidance of revenue loss plus response and recovery expenses.

It might be tempting to conclude that every factor and dimension related to cybersecurity success are subservient to, or at least leading to, the organization's financial outcomes. However, this view may fail to consider the important temporal, human and strategic dimensions. Financial outcomes often lag behind cybersecurity decisions and actions made at a given point in time. For instance, cybersecurity investments made at a given time might have differential financial outcomes later. An effective solution to a cybersecurity issue may require an investment that sacrifices shorter-term financials for longer-term viability.

The personal stake of cybersecurity governance decision-makers in terms of protecting their managerial or board positions, may not align directly with optimal financial outcomes. Additionally, satisfying stakeholders or achieving an organization's mission may supersede optimal financial decisions, especially for not-for-profits or government agencies. Our interviewees supported the need to look beyond financial considerations when defining cybersecurity success, as explained below.

4.1.2 System Integrity & Information Protection

The earliest and most publicized cybersecurity incidents have involved the theft of personal information, especially credit card data (identity theft). Examples include Marriott International, Target, Anthem, Equifax, Facebook, the City of Baltimore's ransomware attack, and the U.S. Office of Personnel Management (OPM). These cybersecurity events gained prominence for the sheer volume of records (millions) that were compromised. Large companies and/or their cyber insurance companies have incurred costs per compromised record, amounting to millions of dollars in remediation costs. As a result, the corporate risk management spotlight has often been focused on

the protection of personal information of customers and employees.

Personal information protection has been further heightened by the recent rollout of the European Union's General Data Protection Regulation (GDPR) with its massive fine potential for non-compliance. Naturally, publicized data breaches can impact customer trust and future purchases; resulting in further revenue loss. For example, one participant noted that *"cybersecurity integrity is certainly paramount … what made that major was because of the information access to everything else. … privacy involves the third or fourth on our list of importance."*

4.1.3 Operational Continuity or Disruption

One important goal of a cybersecurity governance program is to maintain continuity of business operations. Denial of service attacks, ransomware incidents and viruses like WannaCry are examples of cyberattacks meant to disrupt or shut down organizational operations. These are among the more devastating cybersecurity incidents resulting in significant revenue loss and in the case of healthcare systems, the potential loss of life, as a participant articulated: *"I would say a critical event would be an intrusion into an operating plan or an operating system and losing control of that for some period of time…completely disrupting a bank or insurance company, and actually disrupting their operations, is a much more serious event."*

Another participant also noted how dramatic losing operational control can be: *"A critical event would be an intrusion into an operating plan or an operating system and losing control of that for some period of time. … to take Shell or Exxon or one of those guys, the deepwater platforms, one of them produces 200,000 barrels a day of oil. If you lost control of that because somebody hacked into your system, your skater system and your control system, and you've lost control of that. That would be a major event."*

Thus, one of the major dimensions of an effective cybersecurity program is avoiding or limiting any disruption to operations, as exemplified by this comment from an informant: *"If you have some sort of type of system outage that we have seen that have impacted some airlines where they've had significant outages where there were several clients that had issues arising from the Mirai botnet… that impacted their organization where they did quite a bit of business online … where clients weren't able to access the sites and they ended up incurring quite a bit of expense with it as well as a loss of income."*

4.1.4 Organizational Reputation

Many senior executives and board members worry most about the risk of reputational damage resulting from a publicly reported cybersecurity attack that might result in the theft of personal information or reveal damaging internal communications, as this participant comment illustrates: *"the best outcome is never have anything embarrassing happen."* This seems to be a most salient theme, particularly at higher levels of the organization, as this comment illustrates: *"One is where information is pulled out and then that breach is made public so that somebody not only pulls information out which is damaging enough or money out, but they actually demonstrate in public that they've done it. And then there's an impact on your brand potentially."*

Another participant also noted that *"as a security person I didn't care about denial of service, I would categorize it as minor. But for an insurance carrier, that would be major because, for example, imagine the business interruption, the business impact and effect on your insurance policy if delta.com got knocked offline".*

Reputational or brand damage can result in loss of customer trust, purchases and loyalty. Furthermore, these impacts can be longer lasting than a disruption in operations that has a discrete time limitation, as this comment about the Sony breaches illustrates: *"the Sony attack from a couple of years ago; part of the novelty there is that the threat … specifically wanted to target e-mail communications of the top leadership to bear. They say they stole a lot of other information too. But part of what they went after was e-mails where they found company executives talking negatively about Hollywood stars."* On the flip side, positive cybersecurity performance may enhance a company's image as a trusted partner dedicated to protecting customer information and privacy.

4.1.5 Other Important Success Measures

Our participants mentioned additional measures and indicators of success. Regulatory compliance was another frequently mentioned success issue. As one board member put it: "*there's a whole bunch of regulatory … things that can create some huge problems*." Organizations are concerned about large government fines related to failure to protect personal information or failure to report breaches that might impact an organization's operational and/or financial performance materially. The large fines being meted out by the European Union under the new General Data Protection Regulation (GDPR) are emerging as a significant issue. Thus, avoiding such fines is a meaningful success measure. Potential SEC fines for misleading filings represent both unwanted costs and reputational damage. One senior executive stated that *"we have to be very careful … because of SEC filings. There are certain things, depending on how much they cost and the impact as defined by the SEC and it affects your ratings so companies have to be sure that, if they*

classify an attack … adjusting their 10K to reflect the cost of those systems (breaches)."

Similarly, organizations want to avoid the overhead costs and productivity loss associated with governmental compliance audits. Regulatory issues can extend the impact of a cybersecurity breach by adding costs and/or reputational damage to other foundational impacts. Good cybersecurity governance reduces financial and reputational risks by avoiding regulatory action.

Interestingly, some cybersecurity success measures are industry specific. For example, quality of care and mortality metrics are critical in the healthcare industry. Environmental impacts are key to success in the oil and gas industry. One representative of the oil and gas industry stated: *"But if something happened and it caused an oil spill, that would be huge."*

Responses from board members and executives are more representative of enterprise success measures. For example, an important measure for senior managers is intellectual property protection, a significant competitive advantage issue. As one respondent put it: *"(the theft of) intellectual property … is the most dangerous to our organizations and organizations have not figured out what to do with that*."

Finally, it is also important to acknowledge that individuals at all levels of the organization identified success measures that may be in conflict with enterprise cybersecurity success measures. Therefore, those individuals may take cybersecurity actions that are not in the best interest of the organization as a whole. Job preservation is a prime example. IT managers and/or executives may choose not to disclose serious breaches for fear of termination. As documented in the business press, multiple Chief Information Security Officers, Chief Information Officers and Chief Executive Officers have lost their jobs due to serious cybersecurity intrusions. Board of Directors' satisfaction with an organizational cybersecurity governance program is an important factor in managerial job security. For example, one board member commented that management will disclose cybersecurity breaches to the board only when approved by legal counsel. Most companies will have thresholds or committees to decide when to disclose particular information to the board.

4.2 Incident Severity

In order to understand how knowledge alignment can affect cybersecurity success, we first had to understand how participants classified the severity of cybersecurity incidents as either severe, serious, or minor.

Critical Events: were those associated with irreparable financial or reputational damage. One participant referred to these as *"business-ending"* events. However, most participants were less dramatic, but indeed referred to events of broader scope that could seriously compromise things like critical infrastructure, personal identities, intellectual property and service delivery. For example, one participant discussed the adverse effects that a breach of hospital patient records could have. Another participant commented on the irreparable damage that massive breaches of identity in organizations can, as this participant comment illustrates: *"when many federal employees now have their fingerprints potentially compromised and that's something that cannot be regenerated because it is acute and specific. So those people have the possibility of having some level of compromise or inability to have non-repudiation of their identity for the rest of their lives".*

Serious Events: are somewhat similar in nature to critical events, but narrower in scope and with more limited reputational and financial impact. There was general agreement that these affect individual systems, small groups of individuals or single departments, non-critical infrastructure and non-critical services, among other entities.

Table 3. Cybersecurity Incident Severity Examples

	Incident Severity: Examples from Interviews		
	Minor	**Serious**	**Critical**
Financial Impact	Ransomware attack on a limited number of computers with a small financial loss relative to company size.	Paycheck redirection to a malicious actor of a large group of employees (hard or non-repayable money loss).	Theft of a drug formula from a pharmaceutical company that reduces ability to recoup development investments.
Systems Integrity & Information Protection	An individual's social network account hack.	Starwood, Sony, Home Depot, Target hacks that took significant financial resources to recover.	A lobbyist's phone hack when a foreign government gets access to sensitive US government information.
Operational Continuity or Disruption	DDoS attacks (for an IS specialist)	Ukrainian power grid in summer of 2015 with no human lives lost.	Intrusion of an operating system of an oil and gas company, losing control for a time.
Organizational Reputation	Change a homepage of a company's website.	Customers' payment card information, social security numbers, ID breach that a company must acknowledge.	Equifax breach with non-recoverable reputation loss.

Minor Events: there is some consensus among participants that minor events are those that need to be

addressed, but that they are mostly nuisance issues with limited financial or reputational impact, and very narrow in scope. Some examples of this include identity theft of single individuals, viruses and malware affecting one or few users, and minor phishing breaches.

Interviewees mentioned further examples of cybersecurity events of varying severity, from their own organizations and references to incidents known from the popular press or their own contacts. We include some of these examples in Table 3.

4.3 Knowledge Alignment

The primary purpose of the present study, and the focus of the first two research questions, was to develop the construct of cybersecurity success. Once this is defined, our third research question can help explore the domains and alignment of knowledge among the multiple cybersecurity actors and roles, necessary to achieve cybersecurity success in organizations. From our interviews, we are able to sketch out some preliminary findings of interest. One important thing to note is that most participants responded to our questions from one of three perspectives: what they themselves knew; what others in different roles knew; and what people should really know. Another interesting finding to note is that the NIST Framework is not necessarily widely adopted, but when participants discussed cybersecurity knowledge areas, a great deal of the policies and procedures they mentioned fitted within the NIST Framework functional categories, even if not classified that way verbatim by them.

Perhaps the most interesting thing to note is the differences in perceptions about knowledge and information across roles. For example, participants in cybersecurity technical roles were typically confident that the critical cybersecurity practices were in place and that their organizations were well protected against breaches. They tended to rate their knowledge of pre-incident aspects (i.e., identify, detect, protect) as very high and were also confident that policies and procedures were in place for effective post-incident response and recovery.

This perspective was not always shared by others who were more focused on risk management than on specific cybersecurity checklists and policy compliance. Middle to upper management respondents reported more concern about governance and the appropriate level of information sharing with the board. Indeed, some of our interviewees noted that information sharing cannot be widespread in every instance because it can create panic situations, and it was necessary to be very careful about which incidents to escalate to the upper management or to the governing board. One study participant in a cybersecurity management role commented: *"I would say that the number one thing is that the board is happy, and we are not having to notify on data breaches over a long period of time. That's a beautiful thing for sure. That's a number one no data breach is awesome. That doesn't mean that they're not happening right?"* The same participant noted that before even declaring an event as a cybersecurity incident, a substantial evaluation and discussion was required: "…*so it's not necessarily a cybersecurity incident, but it could be and we are going to report out our next report will be in 30 minutes. Our next report might be in an hour. Our next report may be in four hours because it's inherently* [sic] *and we're not going to have anything that is really appreciably different than the time before. [*The report would state:*] Please do not share this information beyond this group. No need to escalate yet. This is confidential as we're still in the investigation stages*."

In some cases, the differentiation of cybersecurity knowledge extended beyond the boundaries of the focal organization. Our interviewees reported that this outsourced knowledge may come through a specialized consultant, an estimate for insurance (often according to its own set of cybersecurity standards), or an interpretation of industry or government guidelines, such as in the form of a scorecard. These cases include variation in both content of knowledge, in that the outsiders bring in new information or perspectives, and the knowledge structure of in terms of who holds that particular expertise.

Interestingly, high-level managers discussed the importance of communication protocols related to cybersecurity incidents, and that it is a matter of deciding when to escalate an issue to the board, but a board member commented that the flow of information from upper management to the board is often controlled and filtered by legal counsel, as this comment by a board member illustrates: *"management filters the story to shift the narrative … just to clarify that a little bit more which is why the general counsel ultimately gets involved is the general counsel typically prepares the agenda for the board. And if they don't want to speak much then there's five minutes on cybersecurity. If you're going to say something you must rehearse it with the general counsel prior go into the board … cybersecurity is highly controversial. Therefore, the role the general counsel serves as a gatekeeper to decide whether or not they will let the board hear the information or not."*

Overall, our preliminary results suggest that people in more technical roles within cybersecurity are more knowledgeable about pre-incident areas and they tend to have confidence in their ability to protect the organization, at least publicly. Management is more concerned with risk mitigation and effective response and recovery plans and may carefully select what

knowledge and information is shared with the board. The board is more concerned with understanding their liability and exposure, and how incidents may impact shareholders.

One more interesting issue emerging from the data is about the type of knowledge that needs to be shared. The team cognition literature differentiates the various team knowledge constructs into ***durable*** – i.e., knowledge acquired over time, which remains relevant over time (e.g., procedures, tools, policies) and ***fleeting*** – i.e., situational knowledge that is relevant while a situation is in progress (e.g., presence awareness, task awareness, etc.), which becomes irrelevant when the situation passes [32]. In this regard, there seems to be a parallel with other domains like in sports and military operations, in which teams need to train and learn over long periods of time, acquiring durable knowledge to be able to perform effectively and efficiently during games or operations. Similarly, our data suggests that cybersecurity actors need to share substantial amounts of durable knowledge during pre-incident phases, but then need to share fleeting knowledge during post-incident phases, in a timely and efficient manner, fostering effective situational awareness [33].

5. Conclusions

This study explores the construct of cybersecurity success, grounded in a set of qualitative interviews with professionals who fulfill varied roles across levels of organizations in multiple industry sectors. Our findings indicate that cybersecurity success is multifaceted, including financial, information integrity, operational, and reputational dimensions, each with varying relevance to differing organizations and roles. This multidimensional view of cybersecurity success is important for both research and practical considerations. Defining an array of cybersecurity success dimensions allows organizations to clarify connections of their governance policies and practices with specific outcomes meaningful to their line of business. Similarly, organizational researchers can use such connections to model relationships, build theory, and test hypotheses to deepen understanding of effective cybersecurity governance.

Additionally, we find preliminary evidence that knowledge domains related to particular dimensions of cybersecurity outcomes are differentially distributed across organizational roles and levels. Technical and non-technical roles, as well as executive and functional managers, hold dissimilar knowledge content. However, this knowledge needs to be aligned in terms within and across job roles, both in terms of durable and situational awareness knowledge of where to turn in the case of cybersecurity breaches or threats. Further examination, such as through policy-capturing or survey research, may help to reveal optimal distributions of specific knowledge domains to achieve varied forms of cybersecurity success without expecting all organizational members to become experts in every aspect of cybersecurity.

Finally, it is evident that organizations vary in their ratings of severity thresholds for critical, serious, and minor cybersecurity incidents. This variance seems related to the line of business, such as healthcare institutions rating illicit access to patient data as a more critical breach than would a retail company whose customer preferences were released, which might be a serious but not necessarily critical breach for that company. This, again, can help to build meaningful predictive models for particular businesses or industry sectors.

Overall, this research is an important step toward understanding the many ways that organizations may define cybersecurity success, as well as to enact effectiveness through knowledge application within their cyber governance systems. Our framework of the success of cybersecurity governance systems, although preliminary, provides rich grounds for further research in this area. These research efforts can assess the validity of our preliminary cybersecurity success dimensions, refining connecting success outcomes to particular knowledge domains, structural alignments, and organizational practices.

6. References

[1] L. Tetrick, S. Zaccaro, R. Dalal, J. Steinke, K. Repchick, A. Hargrove, *et al.*, "Improving social maturity of cybersecurity incident response teams," *Fairfax, VA: George Mason University*, 2016.

[2] R. Sen and S. Borle, "Estimating the contextual risk of data breach: An empirical approach," *Journal of Management Information Systems*, vol. 32, pp. 314-341, 2015.

[3] B. Laberis. (2016). *Eye-Opening Cybercrime Statistics*. Security Intelligence. Available: https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

[4] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab, "An organizational psychology perspective to examining computer security incident response teams," *IEEE Security & Privacy*, vol. 12, pp. 61-67, 2014.

[5] S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and J. A. Steinke, *Psychosocial dynamics of cyber security*: Routledge, 2016.

[6] J. A. Cannon-Bowers and E. Salas, "Reflections on Shared Cognition," *Journal of Organizational Behavior*, vol. 22, pp. 195-202, 2001.

[7] J. A. Cannon-Bowers, E. Salas, and S. Converse, "Shared Mental Models in Expert Team Decision-Making," in *Individual and Group Decision-Making: Current Issues*, J. Castellan, Ed., ed Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., 1993, pp. 221-246.

[8] R. J. Klimoski and S. Mohammed, "Team Mental Model: Construct or Metaphor," *Journal of Management*, vol. 20, pp. 403-437, 1994.

[9] J. A. Espinosa and M. A. Clark, "Team Knowledge: Dimensional Structure and Network Representation," in *Theories of Team Cognition: Cross-Disciplinary Perspectives*, E. Salas, S. M. Fiore, and M. Letsky, Eds., ed New York, NY: Psychology Press/Routledge, Taylor & Francis Group, 2011, pp. 289-312.

[10] W. H. DeLone and E. R. McLean, "Information Systems Success: The Quest for the Dependent Variable," *Information Systems Research*, vol. 3, pp. 60-95, 1992.

[11] W. H. DeLone and E. R. McLean, "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems*, vol. 19, pp. 9-30, 2003.

[12] J. G. Cooprider and J. C. Henderson, "Technology-Process Fit: Perspectives on Achieving Prototyping Effectiveness," *Journal of Management Information Systems*, vol. 7, pp. 67-87, 1991.

[13] S. R. Nidumolu, "The Effect of Coordination and Uncertainty on Software Project Performance: Residual Performance Risk as an Intervening Variable," *Information Systems Research*, vol. 6, pp. 191-219, 1995.

[14] B. H. Wixom and H. J. Watson, "An empirical investigation of the factors affecting data warehousing success," *MIS Quarterly*, vol. 25, pp. 17-41, 2001.

[15] C. Deephouse, T. Mukhopadhyay, D. R. Goldenson, and M. I. Keller, "Software Processes and Project Performance," *Journal of Management Information Systems*, vol. 12, pp. 187-205, 1996.

[16] R. F. Powers and G. W. Dickson, "MIS Project Management: Myths, Opinions, and Reality," *California Management Review*, vol. 15, pp. 147-156, 1973.

[17] (2018). *NIST Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[18] "CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity," 2015.

[19] J. A. Espinosa and M. A. Clark, "Team Knowledge Representation: A Network Perspective," *Human Factors*, vol. 56, pp. 333 - 348, March 2014.

[20] A. Bryant, "Re-Grounding Grounded Theory," *Journal of Information Technology Theory and Application*, vol. 4, pp. 25-42, 2002.

[21] W. Orlikowski, "Knowing in Practice: Enacting a Collective Capability in Distributed Organizing," *Organization Science*, vol. 13, pp. 249-273, May-June 2002.

[22] B. G. Glaser and A. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Hawthorne, NY: Aldine de Gruyter, 1967.

[23] A. Strauss and J. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Second Edition ed. London: Sage Publications, Inc, 1998.

[24] C. Cassell and G. Symon, "Qualitative Research in Work Contexts," in *Qualitative Methods in Organizational Research: A Practical Guide*, G. Symon and C. Cassell, Eds., ed Thousand Oaks: Sage Publications, 1999, pp. 1-13.

[25] R. K. Yin, *Case study research: Design and methods*. Newbury Park: Sage Publications, 1994.

[26] K. Charmaz, *Constructing grounded theory*: Sage, 2014.

[27] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*. Beverly Hills: Sage Publications, 1994.

[28] S. Kvale, "Dominance through interviews and dialogues," *Qualitative inquiry*, vol. 12, pp. 480-500, 2006.

[29] M. E. Jennex, S. Smolnik, and D. T. Croasdell, "Towards a Consensus Knowledge Management Success Definition," *VINE Journal of Information and Knowledge Management Systems*, vol. 39, pp. 174-188, 2009.

[30] R. S. Kaplan and D. P. Norton, "Linking the Balanced Scorecard to Strategy," *California Management Review*, vol. 39, pp. 53-79, 1996.

[31] R. S. Kaplan, "Strategic Performance Measurement and Management in Nonprofit Organizations," *Nonprofit Management and Leadership*, vol. 10, pp. 353-370, 2001.

[32] N. J. Cooke, E. Salas, J. A. Cannon-Bowers, and R. J. Stout, "Measuring Team Knowledge," *Human Factors*, vol. 42, pp. 151-173, 2000.

[33] M. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, 1995.