Regulatory Facilitators and Impediments Impacting Cybersecurity Maturity

Jeffrey Proudfoot
Bentley University, jproudfoot@bentley.edu

Stuart Madnick
CAMS, smadnick@mit.edu

Regulatory Facilitators and Impediments Impacting Cybersecurity Maturity

Completed Research

Jeffrey G. Proudfoot
Bentley University /
MIT Sloan School of Management
jproudfoot@bentley.edu

Stuart Madnick
MIT Sloan School of Management /
MIT School of Engineering
smadnick@mit.edu

Abstract

Due to society's increasing reliance on technology (e.g., financial transactions, critical infrastructure, globally-integrated supply chains, etc.), technological disruptions from cyberattacks can have profound implications for virtually all organizations and their stakeholders. In an effort to minimize cyber threats, governments and regulators have been deploying an increasingly comprehensive and complex landscape of regulations; however, the extent to which regulations actually facilitate, or harm, cybersecurity maturity remains nebulous. This research reports the findings of a qualitative study designed to help illuminate this problem space. We interviewed 12 high-ranking experts, associated with a variety of organizations and industries, and analyzed their responses to identify key factors emerging from the data. These factors were found to operate as either facilitators or impediments of cybersecurity maturity. In addition to identifying these factors, we discuss the implications of our findings, limitations, and avenues for future research.

Keywords

Regulation, cybersecurity, compliance, qualitative, rich description.

Introduction

A growing priority of organizations operating in our increasingly hostile digital world is the advancement of their cybersecurity maturity[1]. Governments and other regulating entities are increasingly involved in efforts to compel organizations to improve their cybersecurity maturity. Generally, this means that a regulator will establish a set of regulations (e.g., the New York State Department of Financial Services established the '23 NYCRR 500' set of regulations for financial institutions) and organizations beholden to that regulator must comply with, or abide by, those regulations or face a punitive outcome (e.g., a bank that does not adhere to regulations imposed on the financial industry will pay a fee as a penalty for their noncompliance). On this topic, Warkentin et al. (2011) observed that organizational leaders are "responsible for ensuring that their organizations are in compliance with an ever-expanding alphabet soup of governmental regulations and requirements, industry standards, and international conventions…" (Warkentin et al. 2011, p. 280).

However, despite this expanding regulatory landscape, organizations are increasingly recognizing that security breaches are not merely a possibility but an eventuality (Bochman 2018). Ironically, some of the most resource-laden, technologically-adept, and/or heavily-regulated (e.g., finance) companies have been the most recent victims of cyberattacks (Horwitz and McMillan 2019; Sandler 2019; Winder 2020). Most notable, however, was the recent breach of a major cybersecurity firm (Volz and McMillan 2020), which caused one lawmaker to state that "Better cyber hygiene alone is not going to win the battle. We need international norms." (Rundle 2021). However, the linkage between new regulatory measures and positive organizational outcomes (e.g., a better security posture) remains tenuous. For example, within the context

[1] While cybersecurity maturity can be defined differently (for example, see (Dube and Mohanty 2021; Ozkan et al. 2021; Rabii et al. 2020)), Dube and Mohanty (2021) describe it concisely as the increasing internal efficiency, and external effectiveness, of cybersecurity activities.

of privacy, another domain experiencing a surge in regulatory activity, Miltgen and Smith (2015, p. 741) stated "One tacit assumption on the part of governmental regulators seems to be that regulations impact behavior. Ironically, in spite of the spike in international regulatory attention..., there has been very little research on that relationship...". The counterintuitive phenomenon of simultaneous growth in both cybersecurity regulations and breaches begs the following question: *in what ways do regulations influence cybersecurity maturity*?

We conducted interviews with 12 relevant industry experts to investigate the interaction of regulations and cybersecurity maturity. During these discussions, we asked interviewees questions about the interaction of their organization's regulatory compliance activities with cybersecurity maturity. In conjunction with our data collection, we analyzed the accruing data using a prominent inductive coding methodology (Glaser and Strauss 1967; Urquhart 2013; Wiesche et al. 2017). Our analysis yielded an initial conceptualization of regulatory factors that we categorize as either facilitating or impeding cybersecurity maturity. We classify this conceptualization as a rich description (Van Maanen 1989; Wiesche et al. 2017), an important initial contribution that serves as a catalyst for scholars to engage in future research on regulatory compliance and cybersecurity maturity. At a more general level, our research constitutes a response to information security researchers' calls for more organizational-level security scholarship (Wall et al. 2015), which remains an understudied topic in the literature. We now summarize relevant literature, report detailed accounts of our methodology, analysis, and results, and engage in a discussion of the contributions, limitations, and future research opportunities stemming from this work.

Literature Review

Our review of the outstanding organizational-level security scholarship indicates that the impact of regulatory compliance on cybersecurity maturity is a largely unexplored area, and that more generally, organizational-level cybersecurity research is minimal. To date, a majority of information systems security literature has focused on micro-level issues, including factors influencing security policy compliance (for examples, see (Cram et al. 2019, 2021)). Concerning the scarcity of information systems research on regulatory topics, De Vaujany et al. (2018, p. 755) stated "As information technology (IT)-based regulation has become critical and pervasive for contemporary organizing, information systems research turns mostly a deaf ear to the topic." Additionally, other security scholars have gone so far as to specifically comment on the lack of organization-level security research. For example, Wall et al. (2015, p. 40) stated "Despite the importance of organizational privacy and security, actual organization-level IS privacy and security research is in a nascent state, which has led to calls for more organization-level research (Belanger and Crossler 2011; Crossler et al. 2013; Pavlou 2011; Smith et al. 2011)." Finally, a guest editorial outlining pivotal artefacts for future security and privacy research identified the importance of the legal artefact, which focuses on the nexus between security/privacy and law, regulations, etc. (Lowry et al. 2017).

The organization-level security work that has been done to date within a regulatory context has explored a variety of topic areas. For example, one stream of research in this domain looks at the added complications and friction that regulatory response triggers (Bayard 2019; Mohammed 2017). Other scholars have investigated the dynamics between managers and employees and how their involvement in regulatory efforts are critical to the success of regulatory initiatives (Buchwald et al. 2014; Hsu 2009; Warkentin et al. 2011). Regulation development has also been explored (Smith et al. 2010), including social and political influences (Backhouse et al. 2006) as well as how standardized regulations can have differing impacts on different industries (Siponen and Willison 2009) and organizations of different sizes (Wall et al. 2015). In terms of regulatory outcomes, researchers have also explored the relationship between compliance and cybersecurity practices (Marotta and Madnick 2020) and have found regulatory response to be an important factor in terms of organizations' cyber readiness (Hasan et al. 2021). However, organizational safeguards implemented to promote security and privacy often yield expected and unexpected outcomes, some of which can be adverse (Parks et al. 2017).

Overall, it is clear that (1) additional research at the intersection of regulatory compliance and cybersecurity maturity is warranted, and (2) general scholarship on organizational-level security topics is scarce. Next, we introduce the methodology used to investigate our research question in this novel problem space.

Research Methodology

Investigating a research area that has minimal extant work and a lack of theory is a key application of this type of inductive coding analysis (Fernandez 2004; Seidel and Urquhart 2013; Wiesche et al. 2017). The intent of this research is to make a contribution in the form of a rich description (Van Maanen 1989). Rich descriptions serve as valuable contributions to the literature due to their creation of new domain knowledge (Wiesche et al. 2017), especially in rapidly-evolving technology-driven disciplines (Taylor et al. 2010). This new domain knowledge, in turn, drives future research and the eventual cultivation of theory in previously understudied areas (Avison and Malaurent 2014; Davis and Marquis 2005). We conducted 12 semi-structured interviews with high-ranking experts in the areas of cybersecurity and regulations (e.g., managers and executives); interviewees were voluntary participants associated with a cybersecurity forum. We purposefully sampled (Patton 2002) interviewees at these higher organizational ranks due to their increased exposure to the interaction of regulatory compliance and cybersecurity issues/decisions (i.e., lower-ranking employees are focused on more granular and compartmentalized activities, including adoption and implementation of controls, etc.). Our interviewee pool represented a variety of industries, including: utilities, consulting, finance, manufacturing, technology, media, cybersecurity, and regulatory. We used this type of interview format to facilitate the emergence of novel insights as not to confirm existing views (Tschang 2007).

The interviews were guided with an emphasis on the following three topic areas (i.e., 'ideational constructs' or 'seed concepts' (Glaser and Strauss 1967; Urquhart et al. 2009)) and their potential relevance to the interaction of regulatory compliance and cybersecurity maturity. Our three ideational constructs include: (1) cybersecurity maturity level, (2) cultural differences, and (3) industry segmentation. This initial set of interview data was iteratively coded to permit concepts to inductively emerge and to develop an initial conceptualization of regulatory compliance impacts on cybersecurity maturity. We engaged in constant comparison throughout to ensure that we were "naming and comparing data incident to data incident, data incident to concept, and concept to concept" (Matavire and Brown 2013, p. 121; Urquhart et al. 2009).

Specifically, analysis was initiated with open coding to first apply a succinct label to each data slice to identify first-order concepts (Corbin and Strauss 2008; Strauss and Corbin 1990). The labeled data were then analyzed during axial coding to allow categories to emerge and coalesce thereby forming second-order themes (Strauss and Corbin 1990). For example, several statements made by our interviewees related to (1) the challenges and expertise needed to interpret a set of regulations and (2) the subsequent friction of operationalizing regulations. These first order concepts served as the basis for creating the second-order theme 'Interpretation & Implementation' (we used this same process for establishing all six of our second-order themes). Finally, selective coding was conducted to establish a relationship between our six second-order themes and cybersecurity maturity (this relationship being either impeding or facilitating). For example, the tone of our interviewee comments about the interpretation and implementation of regulations is that they impede positive cybersecurity outcomes; accordingly, the 'Interpretation and Implementation' second-order theme was established as an impediment to cybersecurity maturity.

Analysis and Results

Our analysis yielded two category groupings of regulatory factors that impact cybersecurity maturity: facilitators of cybersecurity maturity and impediments to cybersecurity maturity. It is important to note that each factor was assigned as either a facilitator, or an impediment, based on inter-respondent patterns found in the data (i.e., strong leadership was evidenced in our data as a facilitator, but it is possible that it could have been considered an impediment for organizations experiencing poor leadership, which would likely yield negative cybersecurity outcomes if that was the pattern in the data). This type of approach has been used in prior research leveraging this same methodology (see (Cram et al. 2021)). Refer to Figure 1 to see a visualization of these category and factor groupings. Explanations for each factor, along with examples of interviewee quotes anchoring the emergence of each factor, are provided in the following subsections.

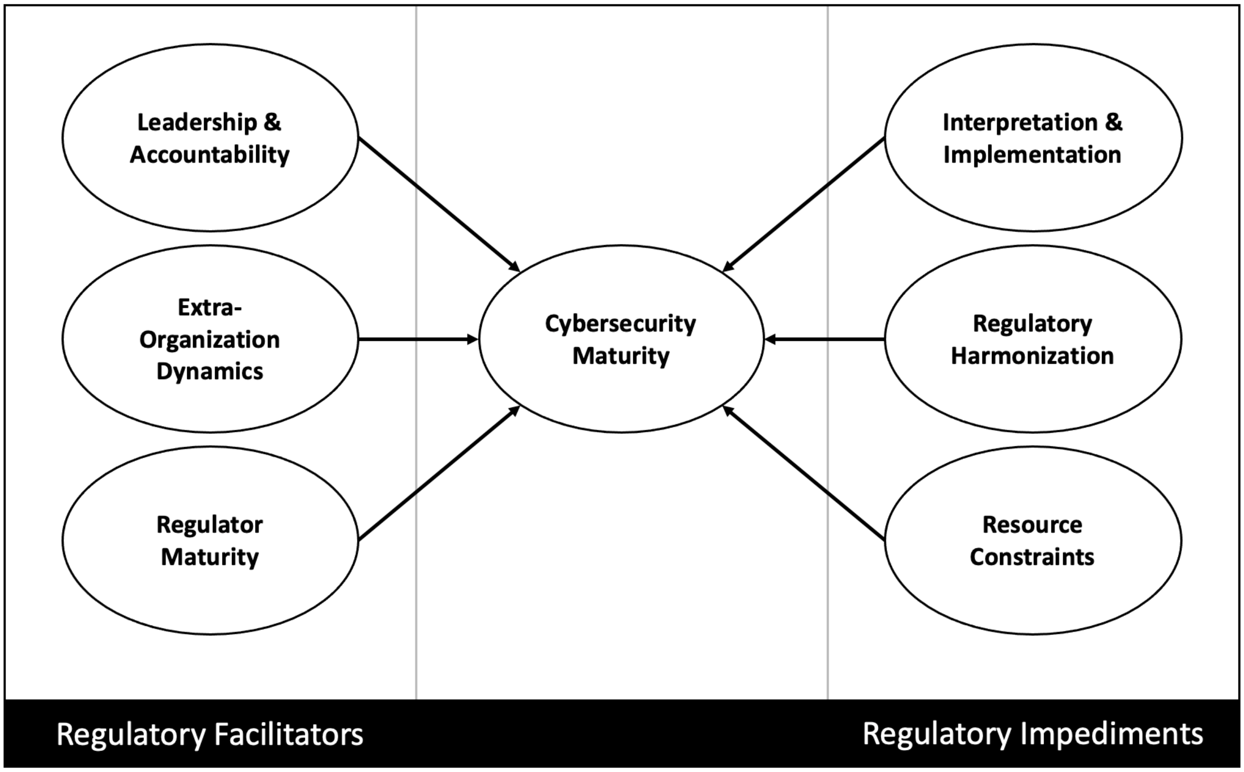

Figure 1. Regulatory Facilitators and Impediments Impacting Cybersecurity Maturity

Regulatory Factors that Facilitate Cybersecurity Maturity

The first regulatory facilitator of cybersecurity maturity we identified is 'leadership and accountability'. Core themes of this factor include the importance of organizational leaders demonstrating support of compliance efforts with regulations, ensuring that organization members are consistently held accountable for properly operationalizing regulations, and proactively advocating on behalf of the organization to external regulators. In short, leaders must set the tone from the top that complying with regulations is a priority. Sample interviewee quotes that we used to establish this factor are provided below:

> *"If organizations fail to allocate responsibility for overseeing compliance, they will never be secure." (*Int-1 – Critical Infrastructure*)*

> *"Sometimes, regulations force executives to understand the importance of cybersecurity and represent an important first step from which to build on." (*Int-2 – Consulting*)*

The second regulatory facilitator of cybersecurity maturity that we identified is 'extra-organization dynamics'. This factor speaks to the nature of the relationship between a regulator and an organization that is operating within that regulator's jurisdiction (e.g., a bank that is beholden to a regulator overseeing financial institutions). For example, does the organization take an adversarial position towards the regulator or does the organization seek a collaborative/receptive dynamic in which a symbiotic relationship can emerge (i.e., the regulator helps the organization mature its cybersecurity posture *and* the organization provides information to the regulator about emerging threats to ensure that regulations are current). Our interviewee comments indicate that a more open and collaborative dynamic helps to facilitate cybersecurity maturity. Sample interviewee quotes that we used to establish this factor are provided below:

> *"One of the biggest banks told us…'We thought…we have been doing security for a long time -- we didn't think regulators could actually teach us anything. However, going through this process, we found we have a few things that we had to brush up a little bit on'." (*Int- 11 – Regulator*)*

> *"We try to feed in proactively to these groups [regulators] so then it's guidance that we feel is healthy and will improve security." (*Int-12 – Finance*)*

The final regulatory facilitator of cybersecurity maturity that we identified is 'regulator maturity'. While it can be common to discuss maturity as it relates to individual organizations, our analysis revealed that regulator maturity can vary quite drastically between industries and across geographic regions. Some regulators are extremely mature and proactive in maintaining the relevance of their regulations while others lack expertise and, as a result, may maintain outdated, irrelevant, or even unintentionally harmful requirements. Accordingly, as regulators mature, there is a greater likelihood that the regulations they impose will facilitate the cybersecurity maturity of relevant organizations (and a majority of interviewees pointed to regulators being mature; thus, this factor was not classified as an impediment to cybersecurity maturity). Sample interviewee quotes used to establish this factor are provided below:

> *"… some regulators are super mature and they will be actively pushing their organizations to comply with not just their own but other regulations." (*Int-11 – Regulator*)*
>
> *"Our regulatory model is continually behind in terms of security… [they] are developed so slowly that, in many cases, by the time they are in place, what you were trying to mitigate has far since evolved into a new issue or is no longer an issue." (*Int-8 – Cybersecurity*]*

Regulatory Factors that Impede Cybersecurity Maturity

Our analysis also identified three novel regulatory factors that impede organizational cybersecurity maturity. The most prominent of these three factors is 'interpretation & implementation'. When new regulations are introduced, or existing regulations are updated, organizations are forced to respond by interpreting and implementing these new regulations. Our interviewees reported that this process can be extremely challenging due to the high percentage of regulations that are nebulous, overly prescriptive, or that introduce friction into organizational processes, which can disenfranchise employees to compliance efforts. Overall, the interview data suggest that this interpretation and implementation process ultimately impedes cybersecurity maturity. Sample interviewee quotes used to establish this factor are provided below:

> *"…failing to understand the scope and implications of what is required may lead to significant consequences in terms of liability and data exposure." (*Int-9 – Finance*)*
>
> *"…[regulations] inevitably add friction and slow down internal processes." (*Int-10 – Technology*)*

The second regulatory impediment to cybersecurity maturity that we identified is 'regulatory harmonization'. It is not uncommon for an organization to find itself beholden to more than one set of regulations, and in highly-controlled industries (e.g., finance and healthcare), an organization may find that it is forced to comply with many sets of regulations. The process of reconciling different sets of regulations is extremely complex as it requires reviewing sets of regulations, parsing through different regulatory lexicons, identifying and mapping overlapping regulations, flagging competing regulations, deciding which competing regulations to implement (or abandon), etc. This process is referred to as regulatory harmonization and is classified as an impediment due to the time, personnel, and other resources organizations must allocate to engage in this difficult process. Sample interviewee quotes used to establish this factor are provided below:

> *"We often find ourselves drowning in a sea of different techniques to measure security programs, so it is necessary to find a flexible scheme that provides a common language and a common understanding of what's essential from a security point of view." (*Int-7 – Media*)*
>
> *"We call it the high-water mark, and we pick the most onerous one and then satisfy the other ones by default. If we try to balkanize it, it becomes very dangerous and then you have to be selective." (*Int-12 – Finance*)*

The final regulatory impediment to cybersecurity maturity that we identified is 'resource constraints'. Organizations can largely self-determine how they are going to allocate cybersecurity budgets, yet regulations introduce a unique obligatory security investment that may not coincide with organizational strategy and/or may stress financial resources. Ultimately, an organization must carry out a "regulatory-cybersecurity calculus" to determine if it is willing to accept the risk, or punitive outcomes, stemming from noncompliance. The data constituting this factor suggest that organizational resource constraints reduce compliance with regulations and thus are an impediment to cybersecurity maturity. Sample interviewee quotes used to establish this factor are provided below:

> *“A lot of big organizations are focused on the bottom line. Unfortunately, a lot of compliance with cybersecurity and IT equals money – it is expensive.”* (Int-6 – Regulator)

> *“Eventually, after a review, it was decided that it would have cost more money to improve compliance with these security requirements than it would have if we had to leave it as it was. We then decided to accept that risk.”* (Int-9 – Finance)

Discussion, Limitations, and Future Research

Our analysis resulted in the emergence of six novel regulatory factors that impact organizational cybersecurity maturity. Based on the nature of these factors and their relationship to cybersecurity maturity, we were able to group these factors into two overarching categories that either facilitate or impede cybersecurity maturity. In addition to the inherent contribution of our novel rich description, the specification of these novel categories and factors yields a number of important contributions to both research and practice. Table 1 outlines these key contributions; a discussion of each contribution is provided below.

1.	General insights into why an expanding regulatory landscape may not be reducing organizational security risk.
2.	Organizational leadership and accountability are key facilitators of cybersecurity maturity in a regulatory-compliance context.
3.	Forcing organizations to interpret ambiguous regulations can have adverse outcomes; managers need to identify and mitigate the disenfranchisement / security fatigue experienced by employees due to the operational friction introduced by regulations.
4.	The value of a set of regulations is linked to the maturity of the regulator that developed those regulations.
5.	Regulatory harmonization can be an impediment to cybersecurity maturity (this is a finding that contradicts prior work).
6.	Resource constraints are an impediment to cybersecurity maturity; however, this factor was not as prominently discussed as any of the other factors that we identified.

Table 1. Key Research Contributions

First, our rich description of regulatory factors that facilitate or impede cybersecurity maturity helps to illuminate why an expanding regulatory landscape may not be reducing organizational security risk. Clearly, organizations are grappling with the challenges associated with interpreting often complex/convoluted regulations, reconciling multiple sets of often contradictory regulations, and making resource-allocation decisions about their regulatory response. These impediments demonstrate that regulations do not yield a 1:1 ratio of regulatory compliance measures leading to equal advances in cybersecurity maturity. As noted several decades ago, “if corporations are forced to deal with a complex regulatory environment, it can have an adverse effect on their performance” (Smith 1993, p. 119).

Second, our identification of organizational leadership and accountability as being a facilitator of cybersecurity maturity builds on a number of prior studies that have found linkages between leadership and compliance success. For example, Hsu (2009) found that the expectations of managers in regulation implementation can have a strong influence on implementation success and that misalignment between managers and employees can yield poor implementation outcomes. Similarly, Spears et al. (2013) found that managers are critical for setting the proper tone and involving end users in security initiatives that are often instigated by extra-organizational forces (e.g., regulations). Warkentin et al. (2011) stated that managers need to demonstrate that they prioritize compliance, and, in an IT governance context, Buchwald et al. (2014) reported that top management commitment is a critical element leading to governance success. Finally, this finding parallels a result reported in a micro-compliance meta-analysis that found organizational support to be a key driver of employee security policy compliance (Cram et al. 2019).

Third, our research further solidifies prior findings that interpreting ambiguous regulations can have adverse outcomes. For example, Gozman and Currie (2014) evaluated regulatory change from an institutional change perspective and discussed 'conversion' as a phenomenon in which rules remain constant but are interpreted differently for the exploitation of organizational ambiguities. From a punitive standpoint, penalties leveed for regulatory noncompliance have been abandoned in some cases due to issues of interpretation (Wall et al. 2015), and courts are having increasing difficulty interpreting some regulations (e.g., Sarbanes-Oxley; see Lechner 2012). To help overcome challenges linked with interpreting regulations, organizations should emphasize two of the facilitators we identified (i.e., leadership and accountability and extra-organization dynamics) to help cultivate collaborative relationships with regulators and thereby (1) clarify nebulous regulations, (2) push back on overly-prescriptive or harmful regulations, and (3) demonstrate that the organization is meeting the 'spirit of the law' rather than simply using a 'checking-the-boxes' approach (i.e., implementing regulations because it is required and only doing the minimum that is required and thus not actually trying to improve security).

In terms of implementation, this is the only regulatory impediment we define that directly impacts the daily operations of rank-and-file employees. Prior regulatory compliance research has recognized the important contributions that individual users must engage in to ensure compliance. For example, Spears and Barki (2010) found that employees should be more aware of risks and controls and that they should proactively participate in risk management within their business processes. Similarly, Warkentin et al. (2011) identified that employees can present a threat to regulatory compliance. Managers need to acknowledge the disruption that may occur due to newly-implemented regulations at the business process / employee level. More importantly, managers should proactively work to mitigate disenfranchisement or fatigue that may occur as employees grapple with newfound operational friction (Cram et al. 2021).

Fourth, our findings identify that the value of a set of regulations is linked to the maturity of the regulator that develops those regulations. A number of prior studies have investigated the development and implementation of regulations (e.g., Smith et al. 2010), and these studies acknowledge a variety of issues in regulation development. For example, these issues can include the generality of regulations that do not account for organizational/industry differences (Siponen and Willison 2009) and the social or political influences that can impact regulation development (Backhouse et al. 2006). Our findings support but add to these prior findings by further specifying that regulator maturity varies, and as a result, some regulators may be more susceptible to these external forces (e.g., political) as they develop regulations. In light of these findings, organizations need to acknowledge regulator maturity when determining how to respond to regulatory measures, and if organizations find themselves at a higher level of security proficiency than a regulator, they may seek to facilitate the maturation process of that regulator. In this way, a symbiotic dynamic can be created between organizations and regulators that can advance the overall cybersecurity posture of organizations operating in a given industry or geographic area.

Fifth, our finding that regulatory harmonization can be an impediment to cybersecurity maturity is an important perspective in light of prior work. The underpinnings of this finding are based on the premise that as organizations are subjected to multiple sets of regulations, it will become increasingly difficult for organizations to interpret them, respond to them, allocate resources for them, and prioritize conflicting requirements from different sets of regulations. However, in one study investigating how organizations choose to violate externally-governed privacy and security rules (Wall et al. 2015), the authors hypothetically state that a company in the healthcare space might not violate privacy laws if regulations other than HIPAA were in place (i.e., sets of overlapping regulations will make it less likely that an organization will violate those regulations). Our findings suggest that a layered approach to regulations can actually be harmful and burdensome and that, in general, adding multiple layers of regulations will not necessarily equate to improved organizational cybersecurity maturity.

Sixth, while the costs of cybersecurity investments can be a deterrent for executive approval, organizations are compelled to allocate resources to comply with regulations (or decide to deal with punitive outcomes for noncompliance). However, the actual benefit of investing in regulatory responses remains unclear. Wall et al. (2015) point out that regulatory compliance investments can be too burdensome for smaller and medium organizations and that lawmakers do not weigh the potential costs of the regulatory measures that they establish. Further, Kwon and Johnson (2013) submit that responding to compliance drivers may waste resources and cultivate a mindset of compliance rather than a mindset of security. Our analysis identified resource constraints as an impediment to cybersecurity maturity, however, it was not as prominently discussed as any of the other factors that we identified (either facilitators or impediments). It is possible that as cybersecurity has become a growing priority of organizations of all sizes over time, security budgets have been increased and resource constraints, while still present, are not as constricting as they once were, especially for larger organizations.

Finally, at a higher level, our results provide new insights into the dynamics of regulatory compliance and cybersecurity maturity interactions. One prior study investigated this phenomenon in a healthcare context and found that the organizations that are more mature operationally tend to focus on actual security outcomes while less mature organizations have a propensity to fixate on compliance (Kwon and Johnson 2013). The authors contend that this is because "many organizations start with compliance and work backward to security. Such an approach is the easy short-term path, since coping with uncertain risks is less straightforward than working to meet specific, measurable compliance goals" (Kwon and Johnson 2013, p. 45). Our results resonate with this finding as organizational leadership and accountability are critical to ensure that an organization views compliance as a means to the end goal of advancing cybersecurity maturity rather than compliance being an end goal in and of itself. In other words, managers and executives should guide the organizational narrative to create a culture that avoids a "checking-the-boxes" attitude towards compliance and, instead, fosters one that focuses on striving for meaningful security outcomes.

In addition to articulating the important contributions of this work, we must also acknowledge its limitations. First, our conceptualization is based on a set of only 12 interviews and our interviewees represent a limited set of industries (utilities, consulting, finance, etc.). Despite seeking a heterogeneous set of interviewees, the generalizability of our findings may be limited to the industries our interviewees represent. A second limitation of our work is the size of the organizations represented by our interviewees. Our pool of participants represents large organizations, which may have different sets of perspectives, priorities, expertise, and constraints in terms of how regulatory requirements impact their process, resources, etc. Accordingly, our findings should be applied with caution to smaller- and medium-sized businesses. Future research should seek to (1) explore how our rich description (a) applies in a variety of industry contexts and (b) scales in response to organizational size, and thereby (2) establish a broader set of impediments and facilitators of cybersecurity maturity that can be optimized to improve overall organizational cybersecurity performance.

Conclusion

Organizations are increasingly forced to comply with an ever-expanding landscape of cybersecurity regulations, yet, counterintuitively, the frequency and severity of security breaches persist. This research represents an effort to better understand the interaction of regulatory compliance and cybersecurity maturity. Based on an inductive coding analysis of qualitative data collected during 12 interviews with relevant industry experts, we conceptualized 'leadership & accountability', 'extra-organization dynamics', and 'regulator maturity' as regulatory facilitators of cybersecurity maturity and 'interpretation & implementation', 'regulatory harmonization', and 'resource constraints' as regulatory impediments to cybersecurity maturity. Our rich description serves as a valuable standalone contribution answering the call for more organization-level cybersecurity research. Overall, these findings can be leveraged as new and compelling knowledge in the rapidly evolving, critically important, yet understudied domain of organizational-level cybersecurity regulations and serve as a catalyst for future research in this area.

Acknowledgements

This research was supported by the Cybersecurity at MIT Sloan (CAMS) initiative (https://cams.mit.edu/). We also specifically acknowledge our partnership with Google and their support of this project.

REFERENCES

Avison, D., and Malaurent, J. 2014. "Is Theory King? Questioning the Theory Fetish in Information Systems," *Journal of Information Technology* (29:4), pp. 327–336.

Backhouse, J., Hsu, C. W., and Silva, L. 2006. "Circuits of Power in Creating de Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly* (30), pp. 413–438.

Bayard, E. E. 2019. "The Rise of Cybercrime and the Need for State Cybersecurity Regulations," *Rutgers Computer and Technology Law Journal* (45:2), pp. 69–96.

Belanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (36:4), pp. 1017–1042.

Bochman, A. 2018. "Internet Insecurity," *Harvard Business Review: The Big Idea* (The End of Cybersecurity), pp. 3–10.

Buchwald, A., Urbach, N., and Ahlemann, F. 2014. "Business Value through Controlled IT: Toward an Integrated Model of IT Governance Success and Its Impact," *Journal of Information Technology* (29), pp. 128–147.

Corbin, J., and Strauss, A. 2008. *Basics of Qualitative Research, 3rd Edition*, Thousand Oaks, CA: Sage.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525–554.

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2021. "When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue," *Information Systems Journal* (31:4), pp. 521–549.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:1), pp. 90–101.

Davis, G. F., and Marquis, C. 2005. "Prospects for Organization Theory in the Early Twenty-First Century: Institutional Fields and Mechanisms," *Organization Science* (16:4), pp. 332–343.

De Vaujany, F.-X., Fomin, V. V., Haefliger, S., and Lyytinen, K. 2018. "Rules, Practices, and Information Technology: A Trifecta of Organizational Regulation," *Information Systems Research* (29:3), pp. 755–773.

Dube, D. P., and Mohanty, R. P. 2021. "The Application of Cyber Security Capability Maturity Model to Identify the Impact of Internal Efficiency Factors on the External Effectiveness of Cyber Security," *International Journal of Business Information Systems* (38:3), pp. 367–392.

Fernandez, W. 2004. "The Grounded Theory Method and Case Study Data in IS Research: Issues and Design," in *Information Systems Foundations: Constructing and Criticising*, D. Hart and S. Gregor (eds.), Canberra, Australia: ANU Press, pp. 43–59.

Glaser, B. G., and Strauss, A. L. 1967. *Discovery of Grounded Theory. Strategies for Qualitative Research*, New York: Aldine Publishing Company.

Gozman, D., and Currie, W. 2014. "The Role of Rules-Based Compliance Systems in the New EU Regulatory Landscape," *Journal of Enterprise Information Management* (27:6), pp. 817–830.

Hasan, S., Ali, M., Kurnia, S., and Thurasamy, R. 2021. "Evaluating the Cyber Security Readiness of Organizations and Its Influence on Performance," *Journal of Information Security and Applications* (58).

Horwitz, J., and McMillan, R. 2019. "Hundreds of Millions of User Passwords Exposed to Facebook Employees," *The Wall Street Journal*. (https://www.wsj.com/articles/facebook-says-millions-of-users-passwords-were-improperly-stored-in-internal-systems-11553186974).

Hsu, C. W. 2009. "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems* (18), pp. 140–150.

Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems* (30:2), pp. 41–65.

Lechner, J. P. 2012. "DOL, Courts' Interpretations of SOX Grow More Divergent," *National Law Review*. (http://www.natlawreview.com/article/dol-courts-interpretations-sox-grow-more-divergent).

Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26), pp. 546–563.

Marotta, A., and Madnick, S. 2020. "Perspectives on the Relationship between Compliance and Cybersecurity," *Journal of Information Systems Security* (16:3), pp. 151–177.

Matavire, R., and Brown, I. 2013. "Profiling Grounded Theory Approaches in Information Systems Research," *European Journal of Information Systems* (22), pp. 119–129.

Miltgen, C. L., and Smith, H. J. 2015. "Exploring Information Privacy Regulation, Risks, Trust, and Behavior," *Information & Management* (52), pp. 741–759.

Mohammed, D. 2017. "U.S. Healthcare Industry: Cybersecurity Regulatory and Compliance Issues," *Journal of Research in Business, Economics and Management* (9:5), pp. 1771–1776.

Ozkan, B. Y., Lingen, S., and Spruit, M. 2021. "The Cybersecurity Focus Area Maturity (CYSFAM) Model," *Journal of Cybersecurity and Privacy* (1:1), pp. 119–139.

Parks, R., Xu, H., Chu, C.-H., and Lowry, P. B. 2017. “Examining the Intended and Unintended Consequences of Organisational Privacy Safeguards,” *European Journal of Information Systems* (26), pp. 37–65.

Patton, M. Q. 2002. *Qualitative Research & Evaluation Methods*, Thousand Oaks, CA: Sage Publications.

Pavlou, P. A. 2011. “State of the Information Privacy Literature: Where Are We Now and Where Should We Go,” *MIS Quarterly* (35:4), pp. 977–988.

Rabii, A., Assoul, S., Ouzzani Touhami, K., and Roudies, O. 2020. “Information and Cyber Security Maturity Models: A Systematic Literature Review,” *Information & Computer Security* (28:4), pp. 627–644.

Rundle, J. 2021. “High-Profile Hacks Spark Calls for Global Cyber Response,” *The Wall Street Journal*. (https://www.wsj.com/articles/high-profile-hacks-spark-calls-for-global-cyber-response-11611570601).

Sandler, R. 2019. “Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested,” *Forbes*. (https://www.forbes.com/sites/rachelsandler/2019/07/29/capital-one-says-hacker-breached-accounts-of-100-million-people-ex-amazon-employee-arrested/?sh=7094b8ab41d2).

Seidel, S., and Urquhart, C. 2013. “On Emergence and Forcing in Information Systems Grounded Theory Studies: The Case of Strauss and Corbin,” *Journal of Information Technology* (28), pp. 237–260.

Siponen, M., and Willison, R. 2009. “Information Security Management Standards: Problems and Solutions,” *Information & Management* (46), pp. 267–270.

Smith, J. 1993. “Privacy Policies and Practices: Insider the Organizational Maze,” *Communications of the ACM* (36:12), pp. 105–122.

Smith, J. H., Dinev, T., and Xu, H. 2011. “Information Privacy Research: An Interdisciplinary Review,” *MIS Quarterly* (35:4), pp. 989–1015.

Smith, S., Winchester, D., Bunker, D., and Jamieson, R. 2010. “Circuits of Power: A Study of Mandated Compliance to an Information Systems Security de Jure Standard in a Government Organization,” *MIS Quarterly* (34:3), p. 463486.

Spears, J. L., and Barki, H. 2010. “User Participation in Information Systems Security Risk Management,” *MIS Quarterly* (34:3), pp. 503–522.

Spears, J. L., Barki, H., and Barton, R. R. 2013. “Theorizing the Concept and Role of Assurance in Information Systems Security,” *Information & Management* (50), pp. 598–605.

Strauss, A., and Corbin, J. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques (2nd Edition)*, Newbury Park, CA: Sage.

Taylor, H., Dillon, S., and Van Wingen, M. 2010. “Focus and Diversity in Information Systems Research: Meeting the Dual Demands of a Healthy Applied Discipline,” *MIS Quarterly* (34:4), pp. 647–667.

Tschang, F. T. 2007. “Balancing the Tensions Between Rationalization and Creativity in the Video Games Industry,” *Organization Science* (18:6), pp. 989–1005.

Urquhart, C. 2013. *Grounded Theory for Qualitative Research*, Los Angeles, CA: Sage.

Urquhart, C., Lehmann, H., and Myers, M. D. 2009. “Putting the ‘theory’ Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems,” *Information Systems Journal* (20:4), pp. 357–381.

Van Maanen, J. 1989. “Some Notes on the Importance of Writing in Organization Studies,” in *The Information System Research Challenge: Qualitative Research Methods*, J. I. Cash and P. R. Lawrence (eds.), Boston, MA: Harvard Business School Press, pp. 27–35.

Volz, D., and McMillan, R. 2020. “U.S. Cyber Firm FireEye Says It Was Breached by Nation-State Hackers,” *The Wall Street Journal*. (https://www.wsj.com/articles/u-s-cyber-firm-fireeye-says-it-was-breached-by-nation-state-hackers-11607461408).

Wall, J., Lowry, P. B., and Barlow, J. B. 2015. “Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess,” *Journal of the Association for Information Systems* (17:1), pp. 39–76.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention,” *European Journal of Information Systems* (20:3), pp. 267–284.

Wiesche, M., Jurisch, M. C., Yetton, P. W., and Krcmar, H. 2017. “Grounded Theory Methodology in Information Systems Research,” *MIS Quarterly* (41:3), pp. 685–701.

Winder, D. 2020. “Microsoft Security Shocker As 250 Million Customer Records Exposed Online,” *Forbes*. (https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=67a349194d1b).