Cybersecurity regulation development and dissemination deficiencies harming organizational cybersecurity outcomes

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

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

Abstract

The increasingly hostile and dangerous digital landscape is resulting in frequent and severe cyberattacks in virtually every industry and context. A byproduct of this trend is mounting pressure on policymakers to intervene and thereby reduce cyber risk, protect vast oceans of data, ensure consumer privacy, and at a more macro level, shore up national security. Policymakers' response to this pressure often takes the form of cybersecurity regulations – mandates imposed on organizations requiring their compliance with prescriptive cyber behaviors enforced through accompanying punitive measures levied for noncompliance. However, researchers have yet to conclusively understand the nuances and effects of cybersecurity regulation development, dissemination, and organizational response. In this research, we explore a subset of this problem space: the potential deficiencies of cybersecurity regulation development and dissemination. To do so, we chose a qualitative approach and conducted 22 semi-structured interviews with a heterogeneous sample of cybersecurity and regulatory experts. Using an inductive coding analysis, we identified three core deficiencies emerging from our data associated with the development and dissemination of cybersecurity regulations, which, counterintuitively, may harm the cybersecurity posture of compliant organizations. We discuss these deficiencies and provide illustrative quotes to solidify their salience. We conclude with the implications and limitations of our work and propose avenues for future research.

Background

Cyberattacks continue to plague virtually every facet of our digital word in alarming degrees of frequency, severity, and sophistication. For example, critical infrastructure continues to be a frequent target, especially by nation-state sponsored hackers, with a reported 50% increase in the number of ransomware attacks targeting industrial companies in 2023 (Rundle & Stupp, 2024). Hacktivism is also on the rise, as 2023 brought a 153% increase in denial-of-service attacks against financial institutions (Stupp, 2024b). Other recent attacks have spanned a variety of industries and geographic areas, including breaches at Global Affairs Canada, Sweden's government services, Microsoft's senior leadership, and Australia's largest private health insurance provider (Center for Strategic & International Studies, 2024). Even cybersecurity companies and researchers have been directly targeted by various attacks, including holding sensitive data ransom, swatting (reporting a crisis so local authorities send a SWAT team to the target's location), intimidation, and financial framing (Srivastava, 2023).

In light of such incidents, policymakers feel compelled to intervene and continue to operationalize their response in the form of new and updated cybersecurity regulations (Rundle, 2021) - mandates imposed on organizations requiring their compliance with prescriptive cyber behaviors enforced through accompanying punitive measures levied for noncompliance. A recent quarterly report demonstrated this continuing expansion of the cybersecurity regulation landscape, with a list of 7 pending cybersecurity regulations proposed by a variety of agencies (e.g., SEC, NYDFS, FDA, and ENISA) in a broad range of jurisdictions (e.g., U.S., EU and U.K.) (Acebo, 2023). One prominent example of a new cybersecurity regulation is the recently-finalized SEC rules requiring public companies to (1) rapidly disclose material cyber incidents and (2) ensure cyber expertise at the board level, thereby placing increasing scrutiny and oversight on corporate directors (Proudfoot et al., 2023; Rundle, 2023).

However, questions remain about the value of cybersecurity regulations and the extent to which they help organizations improve security (Marotta & Madnick, 2020; Proudfoot & Madnick, 2022; Wladawsky-Berger, 2021). Executives often perceive them to be dated, confusing, and even harmful, when compliance means reverting to less-effective policies, practices, and controls (Abraham et al., 2019; Fuster & Jasmontaite, 2020; Mohammed, 2017). Further, not only are there questions about whether cybersecurity regulations translate to positive security outcomes, but there can also be detrimental business impacts stemming from compliance.

For example, a pending cybersecurity regulation proposed by the United Nations (impacting 53 countries) is leading several car manufacturers (e.g., Porsche and Volkswagen) to discontinue older models, as retrofitting these vehicles to achieve compliance would not be cost effective (Stupp, 2024a). Finally, an increasingly complex regulatory landscape can be difficult and expensive for organizations to understand and harmonize (i.e., ensure compliance with what may be conflicting requirements from different regulations). The former director of the U.S. Cybersecurity and Infrastructure Agency (CISA) recently commented on this and stated that the “over-bureaucratisation” of cyber regulations has led to “jurisdictional turf battles and the absence of a unified constituency” for cyber oversight (Krebs, 2023).

But what can be done to maximize the positive effects of new and/or updated cybersecurity regulations? Prior information systems research has explored the regulatory problem space in a variety of contexts, including organizational management support of regulations (Buchwald et al., 2014; Hsu, 2009; Spears et al., 2013), use of controls and requirements for risk reduction (Spears & Barki, 2010), factors governing regulation development (Backhouse et al., 2006; Siponen & Willison, 2009), and organization size (Wall et al., 2015). However, minimal work has been conducted to explore the nuances of how the development and dissemination of regulations set up organizations for improved cybersecurity. It is our contention that current deficiencies in the regulation-generation process often result in harmful cybersecurity outcomes in compliant organizations. To guide our investigation of this supposition, we propose the following research question:

> **RQ:** What deficiencies in cybersecurity regulation development and dissemination harm organizational cybersecurity outcomes?

In the following section, we outline the qualitative methodological approach we used to explore this research question. We then describe the three main regulation development and dissemination deficiencies we identified based on an inductive coding analysis of over 300+ pages of transcripts generated from our 22 interviews with cybersecurity and regulatory experts. Finally, we discuss these results and acknowledge the (1) limitations and (2) future pathways for research associated with this work.

Research Methodology

Our data was collected over the course of 22 semi-structured interviews designed to facilitate the emergence of novel insights and push back against extant assumptions on the topic of cybersecurity regulation development, dissemination and organizational outcomes (Monteiro et al., 2022; Tschang, 2007). The interview format was guided by having respondents address the following 3 topic areas: background/context of the interviewee, (2) cybersecurity and regulatory operations of the respondent’s organization, and (3) moderating effects from organizational leadership, regulator expertise, motivations, resources, and compliance. A fourth open-ended segment of the interview was also afforded for interviewees to comment at will on any related topics not addressed during their responses to the first three topic areas. Interviews were conducted and recorded using a computer-mediated teleconferencing platform; the length of each meeting averaged just under one hour and ranged from 35 to 65 minutes.

Each recording was transcribed and checked for accuracy, ultimately yielding over 300 total pages of interview data, with an average of 15 pages of transcribed data per recording.

Interviewees were intentionally sampled (Patton, 2002) based on (1) their exposure to regulatory operationalization efforts within their respective organizations, and (2) their interactions with regulators. All participants held high-level positions in their organizations which provided a critical perspective for our data concerning strategic-level decision-making on cybersecurity and regulatory response (e.g., CEO, CTO, CISO, SVP, etc.). Interviewees were affiliated with 19 different organizations representing a diverse range of industries to improve the generalizability of our findings (the industries represented included financial services, technology, healthcare, industrial control systems, consulting, insurance, education, government, energy, etc.). We also sought to maximize the generalizability of our findings by speaking with interviewees affiliated with international organizations; ~30% of our participants represented organizations based outside of the United States and 40% of participants operating within the United States worked for international firms, thereby providing a more global perspective.

We utilized an inductive coding analysis technique to analyze the qualitative data collected for this study (Urquhart et al., 2009). The use of this approach is often modified by researchers based on the context and nature of the study and data (Matavire & Brown, 2013) and is commonly used in rapidly-evolving (Taylor et al., 2010), understudied domains with a lack of prior theory development (Fernandez, 2004; Seidel & Urquhart, 2013; Wiesche et al., 2017) (as is the case within the context of cybersecurity regulations). Our goal was to generate a rich description (Van Maanen, 1989) identifying key factors shaping the effects of cybersecurity regulation development and dissemination on organizational cybersecurity outcomes. The broader objective of this type of research contribution is to lay the groundwork for future theoretical development (Avison & Malaurent, 2014; Davis & Marquis, 2005).

Our coding process entailed a granular review of each transcript with the purpose of assigning a concise term to each slice of data, referred to as a first-order concept (Corbin & Strauss, 2008; Strauss & Corbin, 1990). As coding progressed through the transcripts, terms were continuously reviewed and refined until second-order themes began to develop based on constant comparison of the first-order concepts (Boldosova, 2019; Corley & Gioia, 2004; Glaser & Holton, 2004; Locke, 2001; Wessel et al., 2019). In the final step, the relationships between our themes and organizational cybersecurity outcomes were identified and solidified.

Analysis and Results

Three second-order themes were identified over the course of our inductive coding analysis: (1) regulator expertise, (2) regulation relevance, and (3) regulation granularity. All three of these themes were found to have a negative effect on organizational cybersecurity outcomes. We describe each theme and provide illustrative quotes to solidify the salience of each theme in the following subsections.

Regulator Expertise

In total, 15 experts yielded 38 coded statements that collectively formed this theme. Almost all of our experts who spoke on this issue acknowledged that the expertise of regulators varies, which directly impacts the quality of the regulations they develop. Several of our experts identified the positive relationship between a more experienced regulator and the quality of their regulations. Further, some regulators were identified as developing innovative regulations and reasonable regulations that ultimately help the regulation gain traction in relevant organizations. For example, one expert made the following statement about their observations of variability in regulator expertise:

> *The maturity level we see across customers, we see the same degree of variation across [regulators]. Some [regulators] are really mature and dialed in and want to reduce risk for [organizations within their jurisdiction]—others haven't got a clue.* (CISO, Financial Services, #1)

However, a majority of our experts spoke about frustrations that they have experienced as a result of (1) variations in regulator expertise, and (2) regulators perceived to be operating at a low level of expertise. These frustrations are specifically based on a variety of issues, including the development of misguided regulations, the inexperience/low technical or security aptitude of personnel working for regulators, regulators' poor understanding of how cyber risk integrates with other risk categories, and the reality that poorly developed regulations can ultimately result in a less-secure organization. Many experts posited that the lack of experienced personnel working as regulators is due to the financial constraints of public and government institutions, and subsequently, regulators cannot compete with companies in terms of attracting top technical talent. Overall, a portion of regulators are perceived to have a higher level of expertise in that they have the resources and personnel to generate effective cybersecurity regulations, but the broader perception is that many regulators are unable to do so. One of our experts commented directly about the technical proficiency of regulator personnel using an example of data storage requirements:

> *Regulators often don't work with the people who know what they're doing and they don't understand the technologies. Case in point—when you start talking about data localization, you have governments who say you must put all your data and anything you're using to do any of this stuff on the internet. You got to put it in this one location and that's where it can go...[But that means] you're not really using the Internet at that point. You're building a local area network or a regional area network and that's it. So, if you want true data localization, you will have no access to the Internet. Is that really what you [the regulator] intended?* (Manager of International Standards, Technology)

Additionally, another expert we spoke with acknowledged the financial constraints of regulators, which can impede regulators' ability to attract the most qualified technical experts:

> *I think there are some [regulators] that are very backwards in their thinking, I don't think they necessarily hire the most skilled individuals. And I think that's sort of reflected in the fact that these are government entities versus private institutions where for a private institution, I can afford to pay experts more money than maybe a government. Okay? So, I think you find a lesser quality of individual. I've met some very pragmatic and knowledgeable individuals in some of those regulatory bodies. But I would say they're in the minority.* (CTO/CISO, Cloud Computing)

Overall, our findings suggest that the proficiency of personnel working for regulators directly impacts the content of the regulation that is developed. Personnel lacking technical or security proficiency can yield problematic and incomplete regulatory guidance that can result in a false sense of security for an organization or leave blind spots in an organization's security posture.

Regulation Relevance

In total, 12 experts yielded 23 coded statements that collectively formed this theme. A prominent discussion point on the topic of regulation relevance is latency. Many cybersecurity regulations are perceived to be outdated due to the time it takes a regulator to develop the regulation and disseminate it to relevant organizations; this means that regulations are almost never on the "cutting edge." This latency factor can be exacerbated by regulators who rely on already dated materials to develop a regulation. In short, statements from our experts demonstrate consensus that cybersecurity regulations often fail to reflect the current technological landscape, do not address current cybersecurity threats, and do not incorporate effective cybersecurity solutions that correspond to those threats, all because of the inherent latency in the creation and dissemination of cybersecurity standards. For example, one expert we interviewed provided a specific example of an antiquated technology found in a regulation:

> *I think there's lots of outdated regulations out there. I was reading through some financial regulations recently, which still had...reference to diskettes...technology that's not even in use anymore or very rarely in use...it's not hard to dig and discover regulation that's just no longer applicable for the way we do things now.* (Client Director, Technology)

Additionally, we heard the following example from a security expert about latency in the dissemination of regulations negatively impacting organizations' decision-making:

> *So, looking at cloud. Right now, it's part of our group strategy and we're going to move 80% of work out to the cloud soon, but that's also because we waited...[to see] what the regulator is going to do, what do we have to fulfill to do it? There are other financial institutions that are way faster in this and more willing to take risk. But, if the regulator doesn't manage to regulate that quickly enough, or at least provide some guidance about what's acceptable and what's not, that hinders innovation and therefore also information security.* (CISO, Financial Services, #8)

Our experts also identified some additional negative effects stemming from dated/irrelevant cybersecurity regulations. For example, some dated regulations may actually require the organization to modify a current piece of their cybersecurity posture, putting the organization in a more vulnerable state. Additionally, companies operating in a specific industry may be anticipating the release of new or modified regulations, and while waiting, are unable to innovate new products or engage in strategic planning in anticipation that future regulations may conflict with these efforts. Overall, our experts consistently reported that regulations are dated and difficult to map over to existing technologies and cyber threats, but the downsides expand beyond security outcomes and bleed into product development and business strategy. Specifically, one of our experts spoke about government security requirements and identified how outdated requirements can result in a weakened cybersecurity posture for the organization:

> *FedRAMP has some requirements around cybersecurity; it was written for government. It was written a long time ago. It is required if you're going to do security with the government. But it's so outdated that, for example, in order to comply with FedRAMP, we had to downgrade our security in certain areas…So, the encryption algorithms that they wanted to use were outdated. They weren't as good, but ours were better. But guess what, we couldn't comply if we didn't use the exact one that they specified.* (Manager of International Standards, Technology)

In general, our findings highlight the direct impact that latency can have on the relevance of a regulation to an organization's operations. The longer it takes for a regulator to develop and/or release a regulation, the greater the likelihood that the regulation is outdated and fails to reflect current cybersecurity best practices or threats.

Regulation Granularity

Overall, 13 experts spoke on this topic resulting in 30 coded statements. We found that cybersecurity experts associate a number of challenges and limiting factors with granular regulations. Inherently, extremely granular regulations require extensive organizational modifications and interventions that require financial investment and the time and attention of relevant personnel. Further, regulations that are too specific are more likely to have varying degrees of value and impact depending on the size of the organization (i.e., a regulation requiring a very expensive type of control will impact organizations of varying sizes differently). Compounding the ill effects of resource consumption is that these types of mandated modifications and controls may not actually improve cybersecurity efforts. Our experts reported that misalignment between granular regulatory requirements and organizational risk is common and that regulators should prioritize risk mitigation over simply defining extensive regulatory requirements. On the topic of risk misalignment, one of our experts commented:

> *If you have one regulator who says everything you have needs to be encrypted…even in transit needs to be encrypted and encrypted at rest, well, that's a huge impact in terms of cost and performance. What is the risk that you're trying to address? They can't tell you the risk, they just tell you that you need to do it. So, it gets into people's opinions too much and it's not about the risk. I think the secret sauce here is our ability to think about risk and threats, and making informed decisions…and so that's where I think regulations get a bad name because they pursue the minutiae. And it's not even bound by risk. You spend a lot of time churning on things as opposed to really addressing things that matter.* (Executive VP, Consulting)

Additionally, our experts expressed concerns about operational guardrails that are too restrictive. For example, highly granular regulations will inherently become outdated faster as technologies change (a clear interaction with the previous theme). Also, when highly specific regulations constrain how organizations think about and enact cybersecurity, it can stifle what could otherwise be innovative or cutting-edge problem-solving (and as a result, novel security solutions). One of our security experts from the financial industry made the following statement about this hindrance:

> *The frustrating part is…the level which they're written at. So, the FFIEC has always written regulation like "up here," and now you're increasingly seeing…it's very prescriptive. And prescriptive stuff starts to be painful from a practitioner's perspective, because one, if they're telling you exactly how to do it, it limits your ability to solve the problem another way, or to put in an alternate or compensating control, that makes more sense.* (CISO, Financial Services, #10)

Despite these downsides, there are benefits to more detailed regulations. For example, specific regulations require less interpretation and can create an environment in which attestation of compliance is easier to prove. Also, small- or medium-sized organizations with restricted budgets and personnel can benefit from greater direction on security controls and compliance measures as vague requirements can lead to increased planning, testing, training, and investment. A different CISO in the financial industry spoke concerning a positive aspect of granular regulations:

> *Some regulations are open to interpretation, right? Whereas others are very much prescriptive and…we found it to be a welcome thing when a regulator had specific regulations in mind…But we found that things that are prescriptive leave less open to interpretation, which is usually good because then it becomes a binary thing.* (CISO, Financial Services, #1)

In summary, the granularity of a regulation has important implications. Regulations that are too detailed are quickly outdated, stifle creative solutions, may not address important areas of risk, and will impact organizations of varying sizes in different ways. However, increased granularity can reduce interpretation across organizations, help point smaller organizations to better tools and security practices and promote better attestation of compliance.

Discussion, Limitations, and Future Research

Our results provide a novel, empirically-based perspective into the widespread challenges of regulation development and dissemination. Three key deficiencies emerged as a result of our analysis: regulator expertise, regulation relevance, and regulation granularity. Our findings first identify regulator expertise as a fundamentally problematic factor resulting in poor regulations. Most of our interviewees reported poor regulator quality as a precursor to poor regulation development and detrimental outcomes. Regulators with more technical and business expertise consider risk from a holistic view, and thereby anticipate how cyber regulations may (or may not) integrate with other risk areas and/or affect business strategy. However, regulators with this type of background are scarce, and as a result, regulations are often misguided, do not consider other risk areas, and harm business operations. This deficiency is most prominent in some geographic areas more than others (i.e., emerging economies).

A compounding problem in this space is the common (but naïve) view that compliance with regulations equals security, especially when regulations were developed by inexperienced regulators. The cybersecurity skills gap in regulators is likely being exacerbated by the estimated vacancy of 4 million cybersecurity positions globally (Rundle & Stupp, 2024); positions which can often attract top talent with more enticing compensation. Examples of possible ways to address this issue include: (1) inexperienced regulators should consider partnering with more experienced regulators to ensure quality regulations, (2) government regulators should increase wages for personnel to attract better talent, (3) regulators should rely more heavily on relevant standards and frameworks for best practices (this should be done with caution as doing so may introduce a different challenge as discussed in the next paragraph).

We also found the relevance of regulations to be a problematic factor for organizational cybersecurity outcomes. The most important factor impacting the relevance of regulations is latency, or the time it takes regulations to be developed and disseminated to organizations so that they can respond and achieve compliance. Our experts reported that this latency inevitably results in regulations that are outdated and do not reflect the current cyber landscape, including the most cutting-edge threats. Heightening the latency issue is that many regulators rely on existing materials to develop their own requirements. While ill-equipped regulators should draw from higher quality resources to help ensure the quality of regulations, this process inherently multiplies the latency factor (as the entities releasing these reference materials went through their own development process, thereby introducing additional latency). Finally, organizations waiting for anticipated regulation details can be held in a holding pattern of product development and stagnating business strategy (as not to pursue a direction that would later conflict with their ability to be compliant in the future).

The quotes included in our analysis section highlight the existence of outdated regulations, with some referring to diskettes or requiring specific encryption standards that weakened the security of organizations already using more secure encryption. Regulators should stive to maximize the relevance of their regulations by (1) referencing the most current third-party materials during regulation development, (2) providing transparency during the development cycle so organizations can anticipate the nature of future requirements, and (3) providing rapid updates to reduce the ill effects of grossly-outdated requirements (e.g., lingering requirements about diskettes).

Finally, regulation granularity emerged as the third factor harming the cybersecurity of organizations. Overly-granular regulations were reported to cause a number of problems, including the extensive interventions organizations needed in business operations to become compliant. Overly prescriptive regulations mean that organizations are forced to allocate personnel and resources to implement the necessary controls and reporting mechanisms for attestation of compliance, which takes away from other important business objectives. Further, requirements that are too specific often result in varying levels of cybersecurity impact and value. It also reduces the ability of the organization to innovate what may be optimal controls for their own unique industry or processes. The resource-consumption piece is especially harmful for smaller organizations often operating without the slack resources and expertise to use for compliance efforts. Most problematic is that our experts reported the common misalignment between overly granular regulatory requirements and actual risk, resulting in compliance and attestation efforts that do not bring the organization any real benefits in terms of actually improving their cyber posture. Finally, overly granular regulations exacerbate the relevance issue discussed in the previous two paragraphs as detailed requirements need to be reviewed and revised much more aggressively.

However, our experts also noted some degree of value added by detailed regulations. Granular regulations require less interpretation (i.e., reduced cost), which is a benefit, as vague requirements can be problematic in terms of implementing a response and knowing whether compliance has been achieved (and providing attestation of compliance to regulators). This is especially beneficial or smaller organizations operating without the expertise or resources needed to effectively “bridge the gap” between vague regulations and identifying how operationalization of those regulations can be achieved. Regulators should seek to find a middle ground that would provide larger organizations the flexibility to innovate and implement customized solutions while still offering sufficiently detailed information smaller organizations can benefit from in terms of facilitating their regulatory response.

Despite the strengths of this research, it is also important to acknowledge its limitations. Specifically, our description of the research methodology highlighted that our sample was comprised of 22 high-ranking and geographically-diverse executives with expertise in cybersecurity and regulations. It is important to note that two of these participants represented regulating bodies and were thus able to add a counter perspective (i.e., that of the *regulator*) in contrast to the more broadly represented organizational perspective in our data (i.e., that of the *regulated*). However, the distribution of data associated with those in the regulated versus regulator role may have impacted our findings. Future research could focus on the regulator side of these deficiencies so that a more comprehensive view of these phenomena can be articulated and suggestions for recourse can be identified. Additionally, while our sample focused on larger organizations, future research should seek to understand the effects of regulation development and dissemination on smaller- and medium-sized organizations. It is possible that organizations of different sizes may perceive unique challenges and weaknesses introduced by regulators, and any recommendations made as to how regulators can improve should consider the implications of these possible solutions for organizations of all sizes.

Conclusion

Our digital world continues to be rife with cyber risk. While organizations are increasingly willing to invest proactively in cyber risk mitigation efforts, these efforts vary in their nature and effectiveness and often fall short of cybersecurity best practices. Cyber regulations are a prominent tool used by policymakers to ensure a minimum threshold of security is achieved across an industry or within a geographic jurisdiction. However, the extent to which regulations *actually* improve organizational cybersecurity outcomes remains unclear. The purpose of this research was to investigate this phenomenon with a focus on cybersecurity regulation development and dissemination as inherently problematic for the effectiveness of cybersecurity regulations. Our analysis of over 300 pages of transcript data collected during interviews with 22 high-ranking, internationally-focused, executives resulted in the identification of three critical aspects of cybersecurity regulation development and dissemination, namely: (1) regulator expertise, (2) regulation relevance, and (3) regulation granularity. Our findings indicate that these factors often result in poor cybersecurity regulations that not only hamper regulation effectiveness, but may also be detrimental to the cybersecurity efforts of compliant organizations. Future research can further explore these factors, and identify others, to better understand what can be done to maximize the positive effects stemming from compliance with cybersecurity regulations.

Acknowledgements

This research was supported by the Cybersecurity at MIT Sloan (CAMS) initiative (https://cams.mit.edu/).

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*, 539–548.

Acebo, L. (2023, June 15). The Wall Street Journal Quarterly Cyber Regulations Update: June 2023. *The Wall Street Journal*. https://www.wsj.com/articles/quarterly-cyber-regulations-update-june-2023-c8f83dd1

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

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, *30*, 413–438.

Boldosova, V. (2019). Deliberate storytelling in big data analytics adoption. *Information Systems Journal*, *29*(6), 1126–1152.

Buchwald, A., Urbach, N., & Ahlemann, F. (2014). Business value through controlled IT: toward an integrated model of IT governance success and its impact. *Journal of Information Technology*, *29*, 128–147.

Center for Strategic & International Studies. (2024, March). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research (3rd ed.)*. SAGE Publications.

Corley, K. G., & Gioia, D. A. (2004). Identity ambiguity and change in the wake of a corporate spin-off. *Administrative Science Quarterly*, *49*(2), 173–208.

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

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

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European union: The digital, the critical and fundamental rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 97–115). Springer.

Glaser, B. G., & Holton, J. (2004). Remodeling grounded theory. *Forum: Qualitative Social Research*, *5*(2), Article 4.

Hsu, C. W. (2009). Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*, 140–150.

Krebs, C. (2023, August 7). America's messy cyber regulations are no match for its adversaries. *Financial Times*. https://www.ft.com/content/5f143e48-3dda-46a3-82b6-a765782914d8

Locke, K. (2001). *Grounded theory in management research*. SAGE Publications.

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

Matavire, R., & Brown, I. (2013). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems*, *22*, 119–129.

Mohammed, D. (2017). U.S. healthcare industry: Cybersecurity regulatory and compliance issues. *Journal of Research in Business, Economics and Management*, *9*(5), 1771–1776.

Monteiro, E., Constantinides, P., Scott, S., Shaikh, M., & Burton-Jones, A. (2022). Editor's Comments: Qualitative methods in IS research: A call for phenomenon-focused problematization. *MIS Quarterly*, *46*(4), ii–xix.

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods*. Sage Publications.

Proudfoot, J. G., Cram, W. A., Madnick, S., & Coden, M. (2023). The Importance of Board Member Actions for Cybersecurity Governance and Risk Management. *MIS Quarterly Executive*, *22*(4), Article 6.

Proudfoot, J. G., & Madnick, S. (2022). Regulatory Facilitators and Impediments Impacting Cybersecurity Maturity. *Americas Conference on Information Systems (AMCIS)*.

Rundle, J. (2021, January 25). 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

Rundle, J. (2023, July 27). Cyber Experience on Boards Still Seen as Critical in New SEC Rules. *The Wall Street Journal*. https://www.wsj.com/articles/cyber-experience-on-boards-still-seen-as-critical-in-new-sec-rules-937702bd

Rundle, J., & Stupp, C. (2024, February 21). Cyber Threats Against Heavy Industry Intensify. *The Wall Street Journal*. https://www.wsj.com/articles/cyber-threats-against-heavy-industry-intensify-c27a157a?page=1

Seidel, S., & Urquhart, C. (2013). On emergence and forcing in information systems grounded theory studies: The case of Strauss and Corbin. *Journal of Information Technology*, *28*, 237–260.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*, 267–270.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503–522.

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. *Information & Management*, *50*, 598–605.

Srivastava, M. (2023, August 17). Cyber security researchers become targets of criminal hackers. *Financial Times*. https://www.ft.com/content/88560ffa-bb5f-428a-894e-d791a0ee342c

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques (2nd ed.)*. SAGE Publications.

Stupp, C. (2024a, February 20). Carmakers Park Aging Models as U.N. Cyber Rule Comes Into Effect. *The Wall Street Journal*. https://www.wsj.com/articles/carmakers-park-aging-models-as-u-n-cyber-rule-comes-into-effect-546396da?page=1

Stupp, C. (2024b, March 6). Banks Face "Hacktivist" Cyberattacks. *The Wall Street Journal*. https://www.wsj.com/articles/banks-face-hacktivist-cyberattacks-f23d3ec8

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

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

Urquhart, C., Lehmann, H., & Myers, M. D. (2009). Putting the "theory" back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal*, *20*(4), 357–381.

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

Wall, J., Lowry, P. B., & 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), 39–76.

Wessel, L., Davidson, E., Barquet, A. P., Rothe, H., Peters, O., & Megges, H. (2019). Configuration in smart service systems: A practice-based inquiry. *Information Systems Journal*, *29*(6), 1256–1292.

Wiesche, M., Jurisch, M. C., Yetton, P. W., & Krcmar, H. (2017). Grounded theory methodology in information systems research. *MIS Quarterly*, *41*(3), 685–701.

Wladawsky-Berger, I. (2021, October 26). *Compliance Doesn't Ensure Cybersecurity*. MIT Initiative on the Digital Economy. https://medium.com/mit-initiative-on-the-digital-economy/why-compliance-doesnt-ensure-cybersecurity-40bc8af8485c