Insights gained while exploring regulation and cybersecurity maturity

Niek J. van Rensburg
MIT Sloan School of Management
niekjvr@mit.edu

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

Jeffrey G. Proudfoot
Bentley University / MIT
jproudfoot@bentley.edu

Chris Rezek
Google
crezek@google.com

Abstract

Regulators are creating and deploying regulations to encourage organizations to improve their cybersecurity postures. For example, the Colonial Pipeline hack in the US resulted in new cybersecurity regulations being issued for the pipelines and natural gas industry, a change for an industry that was historically self-regulatory. While this is one specific example, there is a general trend of an expanding cybersecurity-regulation landscape. In this context, the following question is often raised: in what ways do regulations influence organizational cybersecurity maturity? To date, researchers have yet to answer this question. We conducted in-depth interviews with 22 cybersecurity and regulation experts as a preliminary effort to help answer this question. We used a qualitative inductive approach to analyze over 300 pages of transcripts which resulted in a rich description of 11 key insights ("gold nuggets") taken from these interviews.

Introduction

With the number of cybersecurity attacks increasing year-on-year, events like Log4j (Uberti et al., 2021), SolarWinds (Murphy et al., 2020), and Colonial Pipeline (McMillan et al., 2021) are gaining more attention from popular media while putting hundreds of millions of computers at serious risk. Policymakers around the world have realized that they must "do something" to intervene (e.g., (Rundle, 2021)). That "something" usually takes the form of new laws and regulations. However, do these new regulations actually help improve organizational cybersecurity or, ironically, might they actually impede their improvements in cybersecurity?

New Regulations are enacted as a means to encourage organizations to improve their cybersecurity postures (Khemani & Shapiro, 1993). The Colonial Pipeline hack resulted in the US government issuing cybersecurity regulations for the first time to the pipelines and natural gas industry (R. Smith, 2021), an industry that was historically reliant on self and voluntary reporting. Other critical infrastructure industries are also being targeted (e.g., see (Volz & Uberti, 2021) and (Uberti, 2021)) for additional regulatory oversight.

With an expanding regulatory landscape, the question is often raised, in what ways do regulations influence organizational cybersecurity maturity? However, minimal research has addressed this topic area specifically, and, organization-level security issues, generally (De Vaujany et al., 2018; Wall et al., 2015).

To answer this question, our team of MIT researchers, in partnership with an industry stakeholder, conducted in-depth interviews with 22 cybersecurity stakeholders operating on 6 continents. Our interviewees represented a variety of contexts, including academia, industry, and regulators. The interviews were held with CEOs, CISOs, CTOs, vice-presidents, product managers, consultants, researchers, and regulatory engineers. Our data collection yielded a corpus of transcripts in excess of 300 pages. We used a qualitative inductive approach for our analysis of the data; this approach yielded key insights about the interaction of cybersecurity and regulations.

In this paper, we report the key insights that emerged from our interviews and analysis. We refer to these insights as “gold nuggets”, i.e. important lessons that should be shared. We also propose strategies which organizations can pursue to capture the “shine” from these nuggets. Before presenting these findings, we first acknowledge the current state of research on this topic and provide an overview of our methodological approach.

Literature Review

Our review of cybersecurity and regulation literature primarily focused on the information systems (IS) domain. This is due to the relevant perspective of the IS discipline to our research question addressing the interaction of cybersecurity and regulations (i.e., focusing only on the more technical computer science perspective of security would miss key managerial aspects; focusing only on policy or law journals would miss the managerial and technical perspective that the information systems literature captures).

While some scholars have reported that regulations can facilitate organizations’ cybersecurity efforts (Chabinsky et al., 2017; Sterns, 2020), a majority of the research in this area identifies the complexities and challenges regulations introduce (Bayard, 2019; Mohammed, 2017; J. Smith, 1993; Sterns, 2020). For example, the actions of both managers and employees have been identified as critical influences on the success or failure of regulatory efforts. Specifically, managers need to be aligned with employees (Hsu, 2009) and managers need to set the proper tone by demonstrating that they prioritize compliance (Buchwald et al., 2014; Spears et al., 2013; Warkentin et al., 2011). At the employee level, employees need to be more aware of controls and requirements to effectively minimize risk (Spears & Barki, 2010), a lack of employee buy-in can threaten the positive effects of regulations (Warkentin et al., 2011), and, too many security interventions (in general) can lead to a sense of security fatigue (Cram et al., 2021).

Outside of manager and employee dynamics, a number of other factors have been explored. In terms of research on regulations, some scholarship has focused on regulation development (S. Smith et al., 2010), the social and political influences affecting regulation development (Backhouse et al., 2006), and the implications of regulations not accounting for industry or organizational differences (Siponen & Willison, 2009). Additionally, scholars have explored the effects of compliance requirements on smaller organizations (Wall et al., 2015), the effects of organizational resource allocation on compliance efforts (Kwon & Johnson, 2013), and the negative implications of organizations’ and courts’ need to interpret regulatory requirements (Gozman & Currie, 2014; Lechner, 2012) (i.e., how can an organization be punished for noncompliance if regulations can be interpreted differently and there is no clear understanding of what compliance actually means?). Finally, research has also addressed the broader question of how compliance relates to security outcomes (Marotta & Madnick, 2020; Wladawsky-Berger, 2021).

Despite the work that has been done to date, there have been numerous calls for additional scholarly attention to IT-based regulation topics (De Vaujany et al., 2018), and, more generally, a need for more scholarship on organization-level security issues (Belanger & Crossler, 2011; Crossler et al., 2013; Pavlou, 2011; J. H. Smith et al., 2011; Wall et al., 2015). Our research is a response to these calls as it takes a step to help illuminate the complex dynamics at the heart of regulatory response and organizational cybersecurity. In the next section, we discuss our methodological approach.

Methodology

Our dataset is comprised of over 300 pages of transcripts collected from 22 interviewees during semi-structured interviews; these interviewees represented 19 distinct companies. In aggregate, these interviews spanned over 20 hours of discussion about cybersecurity and regulation topic areas. Our interviewees represent a variety of industries (e.g., technology, finance, industrial control systems, regulators, etc.) and are employed in high-ranking organizational roles (e.g., CEOs, CISOs, CTOs, etc.). We also sought an international perspective as a third of our interviewees are affiliated with companies based outside of the United States and six of the companies based in the United States operate internationally (i.e., half of our sample accounts for an international perspective on regulations and cybersecurity). All interviews were recorded to capture audio and video data, which was then used to validate transcripts that were automatically generated by our videoconferencing platform.

As described in the previous section, minimal IS scholarship on cybersecurity and regulations has been conducted at the organizational level. Due to this lack of theoretical framing, we chose a qualitative inductive approach for data analysis inspired by a coding-based technique commonly used in the IS literature (Levina & Vaast, 2008; Urquhart et al., 2009). There has been extensive discourse about the proper use of this approach and scholars have applied it differently (Matavire & Brown, 2013). We used it to identify emerging themes in our qualitative data that were then used to develop a rich description (Wiesche et al., 2017). Our rich description is organized as a collection of insights to help organizations and regulators better understand the interplay of cybersecurity efforts and regulations (rich descriptions are a standalone contribution that can result from this type of methodological approach; see (Chang et al., 2011; Lederman & Johnston, 2011; Ribes & Finholt, 2009)). The following section presents these results.

Results

Our analysis of the data revealed the following eleven key takeaways, which we refer to as “nuggets”, that organizations and regulators should consider to help maximize the value of cybersecurity regulations.

Nugget #1: Compliance can be your friend

As a starting point, regulation was supported by ALL the interviewees to establish baseline cyber defenses in different industries because it provides:

A Baseline: Regulation establishes a baseline set of expectations with regards to cybersecurity that can be well understood;

Attention and support: Regulation assists in getting the required attention and support from the board to address cybersecurity;

Secure funding: Regulation helps secure funding for cybersecurity initiatives. Some companies may have no cyber capabilities if compliance did not force their hand;

Legal support since regulation is the law: so it is not challenged by employees and requires less effort to get their support and buy-in to implement controls;

Assurance: Regulation gives assurance to the board and employees that the organization is addressing cybersecurity defenses. The organization is also able to report on the type of defenses they implemented with the funding provided; and

Avoidance of key-man dependency: Regulation decreases key-man dependency risk. Regulations and standards ensure that an organization implements controls that are not dependent on a key individual within the organization, but rather on requirements created and used by a wider community.

One interviewee indicated that their own research showed 70% of companies argued for more regulation to enable better cyber outcomes. Evolving regulation can help raise the baseline cyber posture within organizations.

Implications for management: Regulation can be leveraged to establish and evolve baseline cybersecurity within any organization.

Nugget #2: Compliance does not mean secure, security needs maturity

Cyber risks extend beyond the scope of regulation, because being compliant does not mean that you are totally secure. An example was raised where a retailer was Payment Card Industry (PCI) compliant but was still attacked and ultimately hacked (Moldes, 2018). The maturity of the cybersecurity programs within organizations directly influences how well they are managing their cyber defenses.

It was also noted that certain regulations can be outdated, which directly impacts the cybersecurity of an organization. One institution had to build a different system architecture and downgrade their security on that system to be compliant with FEDRAMP (Federal Risk and Authorization Management Program), because that regulation was exceptionally stringent while also being outdated.

Organizations with mature cybersecurity programs may view regulation as a hindrance to further improve their defense. Resources committed to improve cybersecurity were in some cases re-prioritized to address laborious compliance requirements, which was not the best use of resources for the organization from a cyber risk management perspective at that point in time. In one instance, a bank decided that being non-compliant was the most appropriate risk management course of action. They stopped their compliance remediation program (and took the risk to possibly incur fines) and prioritized their cyber resources to enable employees to securely work-from-home during the COVID pandemic. It should be noted that compliance by itself is perceived to have "zero tolerance for risk", while risk management accepts, manages, avoids or transfers different risks. This highlights that taking a risk management approach to cybersecurity can assist companies to better achieve their business objectives.

Specialist cybersecurity technology companies are engaged when companies want to "raise the bar" with regards to cybersecurity, and not only manage compliance. It is worth noting that these technology providers are normally not exposed to the same regulatory requirements of their client companies.

Organizations with cyber programs that they deem to be mature or advanced, are constantly focusing to develop and deploy new cyber capabilities. They can pursue this, because their cyber "foundations" are strong, i.e. they have already established the baseline security required by the regulations.

Once an organization establishes a baseline cyber capability, they should focus on managing the risks to which the organization is exposed. If there are bigger risks to address, these should be prioritized as opposed to regulation driving prioritization.

Implications for management: After establishing baseline cyber capabilities, organizations should take a risk management approach to cybersecurity to further mature their posture as compliance does not mean secure.

Nugget #3: Small and Medium Enterprises (SMEs) are often forgotten

A shared view was that small businesses tend to follow little, if any, regulations at all. More often than not, they do not have the resources to be able to comply. An example was provided where a sewing shop was hacked and pornography was sent to all the shop's clients. The shop owner had no idea how to respond to this (or even where to report it), and just informed her clients when they called the shop. She did not even change her password post the event, as she felt the hacker would only "bypass" it again.

It was also indicated that software start-up companies view compliance across a "continuum" between business and engineering needs. Business orientated employees view compliance as something to address in the future. Their initial focus is to build and launch a product that people care about and are willing to pay money for, as quickly as possible. Once that is accomplished, they believe there should be more resources available to address compliance. Engineering oriented employees, on the other hand, want to design and build solutions with robust defenses in-place from the outset and want to avoid rework in the future (i.e. incorporate the compliance requirements during the initial build phase). This creates tension within the organization that must be managed constantly, tension between becoming commercially viable while protecting your organization and your clients. For start-ups, it appears that the commercial needs often initially trump compliance requirements, and organizations are willing to accept this risk.

One interviewee felt that "they (small businesses) are just being thrown to the wolves", as cybersecurity (and compliance) is simply not a priority in most cases.

Implications for management: Greater organizational scale and size facilitates compliance, while compliance can hinder SMEs ability to become financially sustainable.

Nugget #4: Cyber rating of software and hardware is needed

It was indicated that a market breakdown exists in the supply of cybersecurity solutions and technologies. Massive information asymmetry exists between the vendor and the buyer of the technology. Anyone can claim to offer cybersecurity solutions irrespective of such a claim being true, and this is having a negative impact on the customers and the industry.

Cybersecurity is a complicated and very specialized industry, and most organizations do not have the skills to do a proper evaluation of the software or hardware solutions they are buying. They may not know whether the solution will really work for them or not. Even where they have cybersecurity personnel, it is unlikely that they have the required expertise to do a proper technical evaluation of the solution, as it is exceptionally difficult and onerous. Significant reliance is placed on Gartner and Forrester reports when selecting solutions. Usually a product is only trusted after it has been used for a couple of years.

Only exceptional companies with significant resources may have the capability to technically evaluate these technologies. This is even more challenging because it not only depends on the organization who chooses to adopt the technology, but also on their suppliers whose products they incorporate.

A need remains to rate/rank cybersecurity tools & services. Certification that consists of a technical review and assessment performed by an independent, suitably-qualified third party can provide better insight and comfort to organizations, whether a specific tool or service can benefit their cyber defenses. This has a downside, as it can create a false sense of comfort, as cybersecurity requires more capabilities than only technical solutions (e.g. training and awareness of staff).

Implications for management: Cyber ratings of cybersecurity products and services would be a great aid to all companies, but especially SMEs.

Nugget #5: Cyber ratings of partner organizations in supply chains is increasingly important

A similar situation exists when deciding whether partnering with another organization is safe, especially a SME. For example, the Target hack occurred via an attack on its air conditioning maintenance company, an SME, which had access to Target's main systems (Manworren et al., 2016).

Some organizations' cybersecurity postures are assessed by cyber rating agencies such as BitSight and SecurityScorecard, which are increasingly used to manage third-party risk. For example, it was reported that the cybersecurity of SolarWinds, which was hacked and provided the path for the hackers to attack its clients, was below "average." It begs the following questions: did anyone check their rating? Was that rating high enough to feel safe?

Implications for management: Cyber ratings of a partner/supplier provides better insight into the risks inherent within the supply chain and assists to better manage third party risk.

Nugget #6: Integrate and standardize risks and controls

Various companies are struggling to manage multiple regulations that also vary when they operate in different countries. One stakeholder's organization had to comply with more than 300 regulations across the globe.

In certain instances, the regulations are very similar but with small nuances. Difficulty starts when the regulations are in conflict, for example the duration that client data must be protected in different jurisdictions. The main challenge with such an inconsistent, incoherent and increasing regulatory burden is that organizations lose sight of the "prize" (strong cyber defenses) and get stuck trying to sort the compliance "weeds". This can result in compliance being managed by taking a risk-based approach, i.e. prioritizing only the compliance issues that are deemed to be the greatest risk to the organization (and the important, basic cyber foundation not being established).

An emerging approach to address this is that companies create a single, standardized risk and controls framework with standardized compliance and risk language. This framework then maps the controls to the respective governance, risk and compliance requirements that the company must adhere to in different jurisdictions. It is a "build once and use many times" approach to manage complexity.

Organizations that have successfully adopted and implemented this approach deem it as a competitive differentiator, especially in an increasingly digital operating environment where controls are better automated and visualized.

Companies are also increasingly designing compliance into their processes and client journeys. This enables better compliance and can improve the client experience, while being more cost effective (and less painful) compared to if it were to be retrofitted. Having a standardized risk and controls framework available to be leveraged supports this approach ("build once and use many times").

Implications for management: Create a centralized, standardized risk and compliance framework that is mapped to different regulations to better manage complexity, compliance and risk.

Nugget #7: Quantify your cyber risk appetite

Throughout the interviews, organizations constantly referred to a risk appetite that supports their digital ambitions. It was also highlighted that many struggle to quantify this "appetite".

The financial services industry has strong expertise to identify, measure, monitor and price risk. Some of the companies interviewed in this sector are now focusing on maturing their management of cyber risk by developing a quantitative, measurable "cyber risk appetite". One interviewee highlighted an example where the company chairman described their cyber risk appetite as being prepared to accept any attack which cost them not more than half the year's profit.

Such dollar-based cyber costs involved in cybersecurity events include:

- Loss of business, clients, money (direct revenue impact);
- Operational downtime (wasted resources, required overtime, cash flow impact, etc.);
- Data breaches (detection and escalation, notification to clients, required remediation of data). IBM Security estimates that data breaches now cost companies $4.24 million per incident on average (IBM, 2021); and
- Reputational damage (possible share price impact and longer-term impact on client base).

A quantified and measurable cyber risk appetite makes the risk more tangible to executives, management and board members. It serves as an indicator of the financial impact that cybersecurity events can have on their business, while at the same time providing guidance on the level of risk taking that is deemed appropriate. Banks are regulated to hold capital for their operational risk exposure (of which cybersecurity is a part) and this approach helps to understand the respective cyber risks within their operational risk profile.

Implications for management: A quantifiable, monetized cyber risk appetite provides improved guidance to personnel and the board on the extent of cyber risk and further matures its capability to manage it.

Nugget #8: Unregulated firms are building a "regulatory moat"

Regulated firms view regulation as a non-differentiating component: it is a requirement that everyone in the industry must meet to operate. On the other hand, firms that are effectively unregulated (e.g. cloud providers such as Amazon Web Services, Microsoft Azure, Google Cloud, etc.), view regulation as a competitive differentiator. They are increasingly focused to deliver regulation-compliant solutions on behalf of their clients.

Certain unregulated companies also expressed that compliance can be a barrier to better cybersecurity. Where cybersecurity technology provider companies cannot adhere to a possible client's compliance requirements, their technologies are not utilized by regulated companies, irrespective of their ability to improve the client's cyber defenses. This may be to the detriment of the client organization's cybersecurity efforts, as the compliance consideration overrides the actual cybersecurity benefit to be realized.

But this barrier is also the opportunity for the unregulated cybersecurity companies that can meet the compliance requirements. Helping client companies in managing their compliance while improving their cybersecurity is viewed as a key competitive advantage by technology companies. One interviewee (from a company in an unregulated industry) indicated that it is their goal to build a "regulatory moat" by improving the experience of their clients, which can include helping them be compliant.

As non-regulated companies are providing more regulatory compliant services to their clients, the clients are increasingly becoming dependent on them and increasing their third-party risk exposure. By providing more services, these unregulated (technology) companies are slowly "eating the world of traditional businesses", which can impact the long-term prospects of these companies.

As highlighted in *Nugget #6: "Build standardized controls once and use many times",* organizations should design compliance into their processes and controls from the outset. Companies adopting this approach can create better client experiences with less friction (e.g. through automation of verification checks or re-use of available information). Companies need to continuously develop their own intellectual property and benefit their clients to remain competitive. Better client experiences with better compliance increases trust between the client and the organization, which can translate into a competitive and differentiating advantage within the industry.

Implications for management: Companies need to leverage compliance into a competitive advantage through better client experiences and trust to remain competitive.

Nugget #9: Regulators should be a partner and not the police

It was requested that the vast sea of regulations should simultaneously be reduced and better integrated. A regulating authority confirmed that they do rely on available standards instead of starting something new, but no mechanism exists that drives harmonization across different regulations. There is significant responsibility placed on industry participants to review and comment on proposed regulations to drive this harmonization.

A possible way to address this is to create an authority whose task it is to drive harmonization between different regulating and standard setting bodies that affect cybersecurity. Such an authority must have veto rights on proposed changes to different regulations and standards.

Companies also want regulating auditors to approach their role in a constructive manner, to focus on the big issues and make suggestions to improve overall cyber posture and possibly even overlook minor violations. The auditor should be viewed as an ally, as opposed to being an adversary. The purpose of an auditor and a regulator is to be overseeing and challenging, and support organizations to make the right decisions in terms of how they manage the risk of the organization. They should not be viewed as a policeman coming to look and find as many violations as possible.

This creates a carrot whereby cyber posture can be improved. The stick, the issuing of regulatory fines, should still be available to ensure minimum compliance is adhered to. The stick should have enough firepower to promote correct behavior but is only to be used as a last resort.

Implications for management: Regulating and standard setting bodies should work together and become partners of their constituents, and not be the cyber police.

Nugget #10: Together we are stronger

Companies expressed a need for better information and insight generation amongst peers, as attackers are seen to be "out-inventing" the defenders. Frustration was expressed by companies, because regulatory authorities only "take" information submitted and give very little in return (for example industry insights). Where regulatory authorities share information, it is viewed to be outdated or not helpful.

Industry bodies have been created to address this need, such as Information Sharing and Analysis Centers (ISACs) in the US. They help organizations in not only being aware of what they themselves are seeing, but also what other organizations are seeing. It also creates camaraderie within the industry. But more can be done.

It is important that security working groups are created for all relevant industries. For example, the North American electrical grid is creating a new security working group that will consist of the top cyber experts (public and private) within the industry. This group will look at true cybersecurity threats coming from nation states (NERC, 2021). Deep and systematic vulnerabilities are to be identified and unpacked, to understand their respective risks and consequences, and how they can be mitigated.

This is a step continuing in the right direction, but the industry is asking for more immediate action and assistance.

Implications for management: Each industry must have an industry body established that is able to collect information from stakeholders and share relevant, valued, and timely insights and events in a trusted environment.

Nugget #11: Cyber investment should be encouraged and promoted

Cyber investments are in some instances viewed as "grudge" purchases because they are made to mitigate against risks that hopefully never materialize, while these risks are at the same time continuously evolving. Many companies only start investing in cybersecurity after a cyber event materializes.

A significant advantage can be realized if cyber related investments can be recovered in some form. This can be achieved, for example by creating more favorable taxation structures that promote cyber investments, or by allowing cyber related costs to be recovered in the base rate granted to energy companies. For example, Maryland launched the Buy Maryland Cybersecurity (BMC) tax credit scheme, that allows companies to claim a tax credit for 50% of the net purchase price of cybersecurity technologies and services purchased from a Qualified Maryland Cybersecurity Seller (*Buy Maryland Cybersecurity (BMC) Tax Credit*, 2018). Maryland also created a funding mechanism to encourage investment into the Maryland cybersecurity industry (Collins, 2022; Irani et al., 2015).

Implications for management: Cyber practitioners and industry groups should lobby that cyber investments can be better recovered through more favorable taxation structures or other funding mechanisms. Precedent for this has been established.

Conclusion

Cybersecurity breaches continue to have a profound impact on all types of organizations and critical infrastructure. Policymakers are increasingly enacting regulations to promote better cybersecurity, but the net effect of regulations on cybersecurity remains unknown. Our research was conducted to establish a better understanding of the dynamics at play in this problem space. We used a qualitative inductive approach to analyze over 300 pages of transcripts collected during 22 interviews with cybersecurity and regulatory experts. Our analysis resulted in a rich description of key takeaways, which we refer to as "nuggets", that organizations and regulators can reference to help maximize the value of cybersecurity regulations. Some of these insights include our assessment that (1) organizations generally appreciate the assistance that regulation gives them to improve their defenses, (2) a balance needs to be maintained that allows industry to use more imagination solving cybersecurity problems, and (3) managing cyber risk is critical to improve the overall resiliency of any organization in an increasingly digital environment. Collectively, our findings serve as a launching point for future scholarship in this area to (1) develop theory and (2) articulate more detailed practical recommendations for industry.

Acknowledgements

The research reported herein was supported, in part, by the Cybersecurity at MIT Sloan (CAMS) initiative, which is funded by a consortium of organizations, and assistance from Google.

References

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.

Bayard, E. E. (2019). The rise of cybercrime and the need for state cybersecurity regulations. *Rutgers Computer and Technology Law Journal*, *45*(2), 69–96.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *36*(4), 1017–1042.

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.

Buy Maryland Cybersecurity (BMC) Tax Credit. (2018). Maryland Department of Commerce. https://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit

Chabinsky, S. R., Petrasic, K. L., & Lee, H. Y. (2017). NYDFS cybersecurity regulations compliance guide: Applicability, exemptions, and penalties. *Banking Law Journal*, *134*(5), 263–272.

Chang, C. L., Chen, V., Klein, G., & Jiang, J. J. (2011). Information system personnel career anchor changes leading to career changes. *European Journal of Information Systems*, *20*, 103–117.

Collins, D. (2022, March 2). *Bills in Maryland aimed at strengthening cybersecurity defenses*. WBALTV. https://www.wbaltv.com/article/maryland-cybersecurity-protection-bills/39300280

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*, 521–549.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90–101.

De Vaujany, F.-X., Fomin, V. V., Haefliger, S., & Lyytinen, K. (2018). Rules, practices, and information technology: A trifecta of organizational regulation. *Information Systems Research*, *29*(3), 755–773.

Gozman, D., & Currie, W. (2014). The role of Investment Management Systems in regulatory compliance: A post-Financial Crisis study of displacement mechanisms. *Journal of Information Technology*, *29*, 44–58.

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.

IBM. (2021). *IBM Report: Cost of a Data Breach Hits Record High During Pandemic*. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

Irani, D., Knight, J., Grimm, J., & Steward, S. (2015). *Information Assurance / Cyber Security*. Regional Economic Studies Institute - Towson University. https://www.stmarysmd.com/docs/Information%20Assurance%20Cyper%20Security%20Comparative%20Analysis.pdf

Khemani, R. S., & Shapiro, D. M. (1993). *Glossary of Industrial Organisation Economics and Competition Law*. Directorate for Financial, Fiscal and Enterprise Affairs, OECD.

Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*(2), 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

Lederman, R., & Johnston, R. B. (2011). Decision support or support for situated choice: Lessons for system design from effective manual systems. *European Journal of Information Systems*, *20*, 510–528.

Levina, N., & Vaast, E. (2008). Innovating or doing as told? Status differences and overlapping boundaries in offshore collaboration. *MIS Quarterly*, *32*(2), 307–332.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*, 257–266.

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.

McMillan, R., Volz, D., & Hobbs, T. D. (2021, May 11). Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat. *The Wall Street Journal*. https://www.wsj.com/articles/colonial-pipeline-hack-shows-ransomware-emergence-as-industrial-scale-threat-11620749675

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

Moldes, C. (2018). Compliant But Not Secure: Why PCI-Certified Companies are Being Breached. *CSIAC Journal*, *6*(1), 18–24.

Murphy, H., Warrell, H., & Sevastopulo, D. (2020, December 18). The great hack attack: SolarWinds breach exposes big gaps in cyber security. *Financial Times*. https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2

NERC. (2021). *Agenda and Minutes of Reliability and Security Technical Committee*. North American Electrical Reliability Corporation. https://www.nerc.com/comm/RSTC/AgendaHighlightsandMinutes/RSTC_Day_1_June_8_2021_Agenda_Package_ATTENDEE_ONLY.pdf

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go. *MIS Quarterly*, *35*(4), 977–988.

Ribes, D., & Finholt, T. A. (2009). The Long Now of Technology Infrastructure: Articulating Tensions in Development. *Journal of the Association for Information Systems*, *10*, 375–398.

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

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

Smith, J. (1993). Privacy policies and practices: Insider the organizational maze. *Communications of the ACM*, *36*(12), 105–122.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Smith, R. (2021, May 25). After Colonial Pipeline Hack, U.S. to Require Operators to Report Cyberattacks. *The Wall Street Journal*. https://www.wsj.com/articles/tsa-to-require-pipeline-operators-to-notify-it-of-cyberattacks-11621960244

Smith, S., Winchester, D., Bunker, D., & 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), 463486.

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.

Sterns, R. Q. (2020). Complementary approaches or conflicting strategies? Examining CISA and New York's DFS cybersecurity regulations as harmonizing framework for bilateral approach to cybersecurity. *Richmond Journal of Law and Technology*, *26*(1), 1–35.

Uberti, D. (2021, December 3). White House Readies Plan to Boost Cybersecurity of Water Supply. *The Wall Street Journal*. https://www.wsj.com/articles/white-house-readies-plan-to-boost-cybersecurity-of-water-supply-11638565221

Uberti, D., Rundle, J., & Stupp, C. (2021, December 21). The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw. *The Wall Street Journal*. https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180

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.

Volz, D., & Uberti, D. (2021, December 2). Biden Administration Issues Cybersecurity Directives for Freight and Passenger Rail. *The Wall Street Journal*. https://www.wsj.com/articles/biden-administration-issues-cybersecurity-directives-for-freight-and-passenger-rail-11638471602

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.

Warkentin, M., Johnston, A. C., & 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), 267–284.

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