Research Plan to Analyze the Role of Compliance in Influencing Cybersecurity in Organizations

Stuart Madnick, Angelica Marotta, Nelson Novaes, Kevin Powers

Working Paper CISL# 2019-24

December 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Research Plan to Analyze the Role of Compliance in Influencing Cybersecurity in Organizations

Stuart Madnick, Angelica Marotta, Nelson Novaes, Kevin Powers

RESEARCH DESCRIPTION

Overview

Today, in order to be successful, every organization needs to be cyber secure. Cybersecurity is the practice of protecting the confidentiality, integrity, and availability of critical organizational assets. However, this practice can be complex and time-consuming, and typically is not the primary strategic goal for the majority of organizations. Conversely, compliance is one of the most powerful motivating forces behind most business investments due to the financial or reputational impact it may have. Compliance is generally defined as the act of conforming to rules or policies. In most industries, ensuring the application of these rules or policies often means meeting a third party's regulatory requirements, such as a government or a cybersecurity framework. Nevertheless, meeting compliance regulations doesn't necessarily enable an organization to cover all cybersecurity needs. This means that achieving the highest level in compliance doesn't often mean that is also possible to achieve an equally high level in cybersecurity. The research question for this study is: To what extent does compliance help or hinder security for the organization – and why/how. Therefore, when trying to understand the interplay between compliance and cybersecurity, generally, two scenarios may occur:

Compliance helps security. Although compliance doesn't always equal security, but in some cases, it can help increase security. For instance, in Germany, a hacker stole unencrypted data on hundreds of thousands of customers of a company because it had failed to implement adequate security measures under the GDPR[1]. As a result, the company received a € 20,000 fine for failing to follow fundamental security practices. Therefore, even though, compliance requirements often offer the bare minimum in terms of security protocols, for some companies the existence of regulations may cause them to at least achieve the overall goal of a basic cybersecurity posture. This has also been observed in a 2017 online survey[2] conducted by Texas-based company SolarWinds, which interviewed around 200 federal government IT decision makers and influencers. The purpose of this survey was to determine the challenges faced by IT professionals to prevent security threats. Results revealed that sixty-eight percent of respondents agreed that the implementation of relevant standards was critical to achieving their cybersecurity targets and sixty percent agreed that compliance has helped them improve their agency's cybersecurity capabilities. Therefore, in some cases, meeting compliance requires companies to reconsider their procedures and address critical gaps. If a company is motivated to worry about fulfilling compliance requirements, which also include cybersecurity, it is likely that the company is also more motivated to allocate additional resources and create favorable conditions for better cybersecurity than a company that is not focused on compliance.

[1] https://europrivacy.info/2018/12/15/first-gdpr-sanctions-are-underway-the-german-case/

[2] https://www.slideshare.net/SolarWinds/solarwinds-federal-cybersecurity-survey-2017-government-regulations-it-modernization-and-careless-insiders-undermine-federal-agencies-security-posture/1

Another positive aspect of being compliant is that regulations may help companies hold their teams accountable to actually implementing the necessary practices, making it difficult for attackers to breach their systems or cause irreparable damages. For example, a Report[3] of Cybersecurity Practices by the Financial Industry Regulatory Authority (FINRA) tells the story of how one of its reviewed firms interpreted FINRA obligations to respond to a cyber-attack through the concept of accountability. One of the firm's first steps, for instance, was establishing a leader for the incident response process and an internal leader for each type of incident as well. Additionally, they identified the role of every person involved in the process and the workflow of the response steps. This approach helped the company repair some of the reputational damage caused by the attack and keep its employees accountable for their actions.

Compliance hinders security. A company may have managed to implement the controls outlined in a specific regulation, which describes the necessary requirements to protect its data; however, that does not mean that its network and systems are still completely protected from cyber threats or that an employee will not send sensitive data via email by mistake. The process of achieving compliance is often costly and exhausting. Additionally, since organizations employ different structures for the management of compliance and cybersecurity there may be conflicts of interests between different entities or units. Therefore, it's not unusual for organizations to let compliance be a substitute for their cybersecurity strategy, considering the amount of time, money, and effort involved in implementing compliance activities. Regardless of whether a company demonstrates a low or a high level of compliance, the compliance processes are generally the same and often involve predefined protocols based on checklists and spreadsheet questions. However, the "checklist mindset", while good for gap analysis, may turn into one of the major risks to be addressed in a developed organizational environment. Consequently, even though companies meet regulation requirements, they may still experience major attacks. For example, despite being within the scope of PCI DSS compliance, Equifax suffered a data breach that impacted over 143 million customers[4]. In this case, compliance did not eliminate the probability of breaches. In recent years, many organizations that suffered major data breaches have claimed their systems were violated despite being fully PCI compliant. For example, Target, a U.S. company operating in the retail sector, suffered from a data breach[5] that exposed credit and debit card data on more than 100 million customers. Just like Equifax, the company was PCI compliant at the time of the attack. This is particularly relevant when considering that regulatory requirements become outdated quickly in the cybersecurity sector or may be misinterpreted. This may increase the risk of data breaches by forcing companies to adhere to obsolete or unclear cybersecurity requirements. Furthermore, being "in compliance" may produce a false sense of security – making the organization even more vulnerable. For example, MEDantex, a Kansas-based healthcare company, leaked sensitive patient medical records[6] despite, apparently, claiming to be HIPAA compliant, as they had announced on their website[7]:

> "MEDantex is serious about keeping your data secure. We are HIPAA-compliant, and our servers are protected with 128-bit encryption. Our security and HIPAA compliance team is made up of department managers and headed by a security officer that continually monitors your data."

---

[3] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
[4] https://www.sans.org/reading-room/whitepapers/breaches/pci-dss-security-breaches-preparing-security-breach-affects-cardholder-data-38340
[5] https://www.computerworld.com/article/2487587/update--breach-exposes-data-on-110-million-customers--target-now-says.html
[6] https://krebsonsecurity.com/2018/04/transcription-service-leaked-medical-records/
[7] https://medstack.co/blog/not-healthcare-security/

HIPAA defines a large set of rules and procedures, many of which require proper technology that provides the security features suggested by HIPAA guidelines. However, like other regulations, these regulation guidelines are open to interpretation, leaving it up to employees to determine the best way to fulfill the requirements. In the healthcare industry, there may be a number of risks associated with misinterpretation because most of the employees who work for a healthcare organization may be specialized in patient care but may not necessarily have the technical skills to correctly manage a compliant cybersecurity infrastructure. As a result, this may cause costly mistakes and show people that there is a lack of care when securing medical information.

This example also shows that the relationship between compliance and cybersecurity can also become more complicated when the privacy component is involved. The concept of privacy has evolved with the introduction of information technologies - from " the right to be let alone" as Samuel D. Warren and Louis D. Brandeis formulated, now privacy mainly refers to the right to access and control the use and circulation of personal data through digital channels[8]. Therefore, in today's digital environment, although the issue of privacy is crucial, it is data privacy that is of primary importance rather than privacy per se. Data privacy is generally focused on the proper governance of data. This generally involves implementing regulation requirements to ensure that individuals' personal data are being collected, used, shared, and transferred in appropriate ways. In this context, cybersecurity plays a key role in building privacy as it helps to protect data from unauthorized access and prevent data breaches. However, even though cybersecurity, privacy, and compliance are all connected, the three can sometimes be in conflict. Often, these issues arise when making decisions about how to manage data. Some regulations, for example, may require organizations to adopt solutions with which cybersecurity is aligned but privacy is not. The conflicting interplay may also work the other way around - compliance can complicate cybersecurity when certain laws or regulations impose privacy measures that interfere with or limit the access to information, which would be useful to guarantee security (e.g. if privacy requirements hinder the use of protection solutions aimed at countering data leaks). In most cases, these types of issues arise when the application of privacy requirements guarantees individuals' right to privacy while preventing authorities from collecting important information to conduct investigations. For example, tracking down a suspect of a crime may be useful to solve a criminal case, but, at the same time, this may violate the alleged criminal's privacy or some aspects of privacy.

The framework resulting from these scenarios is an overall organizational situation in which compliance can be either an excellent starting point to develop the appropriate cybersecurity culture within an organization or an obstacle that will only lead an organization to a false sense of security. However, often, whether compliance is a positive or negative factor in achieving cybersecurity is not black and white but rather a matter of a series of factors, which may either minimize or maximize the impact of compliance on cybersecurity. This research attempts to provide a better understanding of these factors by evaluating compliance as a critical factor in the organization's cybersecurity strategy.

Proposed Research

This study is proposed with the purpose of providing an analysis of the role of compliance in affecting or facilitating the achievement of cybersecurity. The main hypothesis of this research project is that the extent

[8] https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1662104&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1

to which compliance is effective depends on three factors: an organization's cybersecurity maturity level the cultural differences between countries, and the industry segment organizations operate in.

H1. Maturity level.

a. **If an organization has achieved compliance, it might neglect important aspects of security that have not been addressed – putting itself at risk.**

   One of the main goals of regulations is ensuring that organizations reach and maintain a specified level of preparedness and capacity for meeting certain objectives about cybersecurity (i.e. cybersecurity maturity level). If an organization is, for example, mature enough to sustain the level required by regulations, it will probably only focus on complying with the required security standards and will not be motivated to implement additional cybersecurity policies and processes.

b. **If an organization is very weak in security, regulations might guide and force the organization to improve.**

   Organizations with lower levels of maturity may view compliance as a motivating factor in achieving better cybersecurity and staying vigilant in their cybersecurity operations[9]. For example, in the case study "A Culture of Cybersecurity at Banca Popolare di Sondrio"[10], Banca Popolare di Sondrio (BPS) built its success on its ability to leverage the power of technology to provide better and more secure services for its customers. When the Bank started its digital transformation, its practices and processes were not mature enough to sustain the continuous cybersecurity readiness of the whole system. However, being an organization operating in a highly regulated environment, the implementation of regulations positively impacted various aspects within the Bank and helped it move towards a more proactive maturity level. The introduction of GDPR particularly forced employees to change their cybersecurity habits. For example, employees started to follow established cybersecurity practices and implement new organizational measures to ensure an appropriate level of cybersecurity to prevent data breaches.

c. **An organization may think (or even "stretch things") so as to appear compliant (and secure) to save costs – without much actual regard to security**

   The cost of being compliant can sometimes be a burden for organizations that are not cyber mature. It requires a lot of paperwork to manage, and it needs to be handled correctly since an error or omission can lead to consequences, such as legal actions, penalties, and sometimes, loss of the requirements to operate or do business in a given industry. This could result in organizations being under pressure, therefore neglecting or completely ignoring security measures. For this reason, they often check the compliance "checkbox" and do the least about security just to pass audits. This is a common approach but unfortunately, it prevents organizations from having the means to reflect on the impact that regulations may have on

[9] http://130.18.86.27/faculty/warkentin/SecurityPapers/Newer/VanceSiponenPahnila2012_I&M49_HabitPMT.pdf
[10] https://cams.mit.edu/wp-content/uploads/BPS-Case-Study-03012019.pdf

security. For example, some standards have different levels of compliance; each of them has specific requirements necessary to validate its compliance. In these cases, one of the largest problems is that organizations tend to have minimalistic approaches to meeting requirements because of the graduality of the compliance process. The family of PCI DSS standards, for instance, falls under this category of standards as it comprehends four levels of PCI compliance. One of the first cybersecurity requirements is to protect cardholder data by installing and maintaining a firewall configuration[11]. Although meeting this requirement seems to be sufficient from an audit perspective, given the vagueness about the degree to which this firewall must protect cardholder data, from a cybersecurity point of view, it may be necessary to implement additional measures. Thus, some organizations don't consider supplementary cybersecurity protections when they are not technically required.

Additionally, if meeting compliance requires organizations to make extra financial efforts in terms of security, they may decide to dedicate more time to appearing compliant and avoiding fines rather than actually ensuring compliance applicability. According to Javvad Malik, an IT security professional[12],

> "Organizations with small and overstretched security teams and limited budgets for cybersecurity are likely to be extremely worried about the threat of GDPR fines. After all, the potential of having to pay up to 4% of global turnover could have a serious effect on a fledgling business potentially impacting earnings or funding opportunities. They could also lose customers through reputational damage and even have to consider making redundancies. Set against this backdrop, it's easy to see why some might consider trying to cover up a data breach, rather than deal with the consequences. But this could lead to far greater problems for them in the long term."

This means that many organizations may decide to give up on security to prevent any issue associated with compliance penalties and hide their maturity "insecurities." For example, Article 33 of the GDPR introduces a duty on all organizations to report a data breach within 72 hours. In order to avoid large fines, organizations might try to cover up data breaches rather than reporting them within 72 hours. One reason for this could be a lack of preparation or adequate tools in identifying or reporting data breaches in a timely manner.

H2. Cultural differences between countries.

a. Compliance may have a negative or positive impact on the cybersecurity posture of an organization, depending on the cultural context in which it operates.

Regulations, especially those related to privacy, might vary greatly from one country to another. Consequently, some cybersecurity practices, for instance, may represent a problem in one country while, in other countries, the same practices would be considered correct. For example, the philosophy behind GDPR is that privacy is a fundamental right under the Charter of

[11] https://www.pci-guide.co.uk/section-1.html
[12] https://eugdpr.com/news/new-cybersecurity-industry-survey-exposes-widespread-concern-upcoming-gdpr/

Fundamental Rights of the European Union[13]. Therefore, the new regulation is shaped around this principle and is intended to harmonize the way that personal data are processed throughout the EU. In the United States, data protection is based on concepts of autonomy and liberty articulated in the US Constitution and the Bill of Rights[14] and follows a more sectoral approach, according to which data protection is regulated depending on the category into which individuals' information falls. Examples of this approach include the Gramm-Leach-Bliley Act (GLBA), which regulates financial services and the Health Insurance Portability and Accountability Act (HIPAA) which covers health data. This aspect can be especially important for multinational companies; considering the cultural differences of every country, it may be hard for them to achieve compliance through a unique strategy for every branch, and this may leave their organization exposed to potential vulnerabilities.

b. Compliance rules in different countries might be directly or indirectly in conflict.

Because of the global nature of cybersecurity, there may be a potential for conflicts when regulations differ across countries or cannot be applied beyond the boundaries of a specific country. This may create privacy and security concerns and may affect the sense of security. For example, it is worth mentioning the battle between Brazilian investigation authorities and U.S. companies[15]. One of the main issues behind this conflict lies in the fact that companies with headquarters in the U.S. that provide internet application services in Brazil face issues regarding the application of the Brazilian laws, especially when it comes to disclosing contents of users' communications stored in their servers to local law enforcement. In a case involving Microsoft[16], the Brazilian government requested the company to disclose email communications of an individual involved in a criminal investigation. However, according to U.S. privacy laws, it is illegal to hand over the data stored in the U.S. even if they belong to a Brazilian citizen. Thus, Microsoft refused to fulfill the request and, as a result, a Brazilian Microsoft executive was arrested.

In Europe, one of the recent concerns involving cross-national compliance issues is the possible impact that Brexit may have on the rules around data security. According to a survey[17] of over 900 participants, over a quarter of survey respondents believed that the corporate and customer data their organization holds would be less secure if Brexit happened. If the UK were to leave the EU, the integration of GDPR into UK law could no longer be adequate to ensure that UK data security and privacy standards are accepted by the EU[18]. Therefore, without a new agreement, data flows between the UK and the EU would probably be affected, causing organizations to be more exposed to data breaches.

[13] http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[14] https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf
[15] https://www.migalhas.com/HotTopics/63,MI273592,61044-Brazil+and+the+United+States+of+America+Jurisdiction+and+the
[16] http://www.internetlab.org.br/en/privacy-and-surveillance/internetlab-files-amicus-brief-to-microsoft-warrant-case-in-the-us-supreme-court/
[17] https://www.alienvault.com/who-we-are/press-releases/infosecurity-europe-2017-survey-report-gdpr
[18] https://www.simplisys.co.uk/news/gdpr-brexit-sure-compliant/

H3. Industry segmentation and different regulators

- **Industry segmentation may affect a company's ability to build consistent cybersecurity strategies as they relate to regulations.**

  In addition to the geographical factor, regulations often vary according to the industry segment in which companies operate. For example, managing the financial sector represent a significant challenge for many companies because regulations within this type of industry vary significantly based on the type of financial service. Each of these regulations is aimed at establishing a set of robust cybersecurity practices, protecting costumers, and supporting the stability of the global economy[19]. However, due to the numerous requirements and the effort required to meet them, companies struggle to build consistent cybersecurity strategies. For example, in a survey of chief information security officers from financial institutions, participants indicated that 40% of their team's time and resources were devoted to reconciling various regulatory requirements[20]. In most cases, regulations use differing vocabularies and lexicons to define the same cybersecurity concepts and practices, causing a significant burden for companies. In the financial field, this is particularly important as companies must demonstrate their compliance with the words mentioned in every single regulation. Additionally, there are different regulatory agencies and entities involved, such as the U.S. Treasury, the Financial Industry Regulatory Authority (FINRA), etc. Typically, the number of regulators that companies need to communicate with may vary from 2 (small financial services) to 20 or more (large organizations). Regulators play a key role in the compliance process as they normally require companies to conduct assessments according to the framework they establish, and the results derived from these assessments need to be supported by documentary evidence. Therefore, this complicated regulatory environment may result in substantial financial impacts for organizations in terms of time, inefficiencies, and budget.

Methodology

We propose to conduct this research in five stages.

Stage 1: Literature Review: Learning from experiences with safety and safety regulations, as well as early experiences with interactions between compliance and cybersecurity.
We want to build on previous research that has relevance to this project. Generally, regulations and laws are created when it is necessary to regulate, control, or stop situations or issues affecting individuals. For example, the introduction of rules to encourage improvements in the health and worker safety area has strongly redefined and influenced the concept of safety over the years, from reducing stress and risks of incidents/occupational injuries in the workplace to the development of more comprehensive insurance plans. Regulations on safety represented a departure from which regulators defined rules on cybersecurity and cyber risk. When it came to dealing with the first major cybersecurity issues, there has been a strong legislative and regulatory reaction in some countries, which led to results thanks to the existing studies on safety. Thus, although the efforts to improve the safety and security of individuals through laws and regulations have taken different approaches, they seem to have similar principles and origins. For this reason, this study will first review the literature related to the various aspects of the compliance versus

[19] https://www.bcg.com/en-ch/capabilities/technology-digital/simplifying-compliance-in-cybersecurity.aspx
[20] https://www.fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf

safety debate in different sectors, such as health, worker safety, and construction industries. Subsequently, the literature related to the compliance versus security issue will be examined.

Stage 2: Learning from actual experiences of interactions between compliance and security.
Existing compliance/security-related management practices will be identified based on a comprehensive understanding of the most common industry practices and academic researches. This will be performed by reviewing case study papers and statistical reports. Additionally, existing regulations will be analyzed along with potential costs and risks involved in implementing the requirements associated with specific regulations. This will involve identifying the related controls and whether or not there are relevant differences between the presence or absence of these controls in terms of cyber risks. The results will be compared with recent attacks.

Stage 3: Collect and analyze data from companies.
The third stage of this research involves collecting and analyzing data from companies to investigate the role compliance in function of cybersecurity within their organizational systems. The primary research method for gathering data for this study will be research survey, where data for different organizations are collected through methods, such as questionnaires, interviews, and published information. Companies will have the opportunity to use the questions of the survey as a self-assessment method and compare their results with the framework developed in the final stage of this research. In particular, data will be acquired from organizations belonging to two major categories: large enterprises and small-to-medium-sized organizations. The survey will be useful to understand whether compliance has a positive or negative influence on the organizations' cybersecurity posture and hence to provide generalizable results about the object of this study

Stage 4: Framework
In this stage, a framework will be created to organize and present the data and insights gained. In fact, early versions of possible frameworks will be used to help focus and organize the data gathering process.

Stage 5: Recommendations.
The culmination of this research will be a set of recommendations for organizations. This will help managers and executives make more informed decisions and get a sense of whether their organization has an accurate understanding of their compliance impact on their cybersecurity environment. Comparison between these categories may be performed through the analysis of a number of organizational level factors that have an impact on the interplay between compliance and cybersecurity. Criteria may include organizational structure, business model, geopolitical diversity, reporting structure, market/industry type, etc.

Impact

Most executives assume that just because their organizations are compliant, they are automatically secure. While this may be true in some cases, managing security with a "checkbox mentality" may often result in inadequate protection. This paper has the purpose to address this issue and provide executives with the right tools to change this assumption. This research intends to achieve this by investigating the best way to develop the maximum benefit of synergy between cybersecurity and compliance. Particularly, the study has the following sub-objectives:

1. To provide a comprehensive overview of the main challenges facing organizations in balancing compliance and security;
2. To review current industry researches and practices regarding the role of compliance in security management;
3. To outline a conceptual framework for management to attain best compliance and security.

The result of this study will be valuable to executives as well as consulting organizations in developing better practices and tools for helping organizations avoid unrealistic expectations about their resilience capabilities and reduce the challenges connected to compliance and cybersecurity. Additionally, this research could be the foundation to build a network of organizations that could be interested in sharing their issues on compliance/security and finding solutions. This aspect could also be an incentive for companies to participate in this study.