Convergence and Divergence of Regulatory Compliance and Cybersecurity

Angelica Marotta, Stuart Madnick

Working Paper CISL# 2020-31

November 2020

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

Convergence and Divergence of Regulatory Compliance and Cybersecurity

Angelica Marotta, Stuart Madnick

Abstract

The introduction of technology in today's society and the risks associated with its use demonstrate the need to secure information and other digital assets at various levels and in various sectors. Not only is this aspect important for industries, companies, and individuals, but also for countries. Regulations in several organizational and cultural contexts are requiring increased and improved cybersecurity strategies. To better understand the commonalities and variations of the different compliance environments, we performed a comparative analysis drawing on eight interview-based case studies. This study examines the conditions under which compliance presents issues impacting cybersecurity and which areas are affected, in both positive and negative ways. The comparison features the cultural, regulatory, financial, and technical factors contributing to compliance problems. Finally, we draw out lessons about compliance strategy from both a regulatory and organizational point of view.

1. Introduction

Compliance regarding cybersecurity is a relatively young discipline that focuses on the processes and behaviors of the people aimed at preventing and reducing risks in different areas and industries. The need for cybersecurity regulations mainly stems from the desire for certainty in what is perceived as an unpredictable field (Hardy, 1993). Another factor that is often entrusted to precise general regulations is the necessity to avoid the cumbersomeness of having a multiplicity of different rules for different circumstances (Hardy, 1993). However, the regulatory aspect alone might not be enough to cover all these aspects and ensure that a company is protected from all risks and situations (Duncan & Whittington, 2014), especially as industry expectations are increasing. It is not acceptable that some companies consider compliance as a mere formal obligation. Organizations are required to consider all the actors that have a role in the regulatory machine: customers, employees, regulatory authorities, shareholders, and even the geographical area in which they operate. Such a comprehensive compliance perspective, however, presents challenges. For example, according to Dawson et al. (2016), "regulations create a diverse set of compliance environments that display some similarities, yet contain differences in focus and intent." Despite the benefits that regulations may bring to cybersecurity, the reality is that there are conflicts, tensions, variances, which makes compliance a difficult task, depending on the context.

This paper builds on this concept and offers an overview for understanding different compliance environments and their impact on cybersecurity using a comparative analysis of eight interview-based case studies. We identify the conditions under which compliance presents issues and which areas are affected. The comparison highlights relevant cultural, regulatory, financial, and technical factors contributing to different compliance impacts. From this study, we draw lessons about improvements to compliance strategy from both a regulatory and organizational point of view.

2. Case Choice and Methodology

The past years have been very critical for many companies with respect to their cybersecurity needs. Recent cyber events - in various sectors - have exposed circumstances where poor regulatory management and ineffective regulations have contributed to significant negative consequences. Increased awareness has driven conversations about the importance of being compliant with current cybersecurity standards. However, as argued by Marotta and Madnick (2020), being compliant is not necessarily the same as being secure. Adhering to specific standards means meeting some base-level security requirements, and, for this reason, compliance itself might not replace an effective cybersecurity program. In previous work on the topic (Madnick et al., 2019; Marotta & Madnick, 2020), the authors looked at the literature concerning the compliance factors that have an impact on cybersecurity in different industry sectors. Each sector presented critical points and overlaps. To exemplify the theoretical observations defined in this work, we conducted eight case studies of companies operating in different industries. We compared different compliance considerations in terms of process goals, their problems, and stakeholder characteristics. The cases were selected for their variety of setting, purpose, and geographical area. Not only do they represent compliance on two continents – America and Europe – but they also represent the perspectives of professionals from different compliance cultures. Additionally, the cases reflect multiple problem domains at different scales, from state to national scale, and industries ranging from energy and utility sectors to biopharmaceutics and financial service.

The eight cases are briefly summarized below[1]:

Case #1*: *Interpreting Compliance Results. This case study in Western Europe was set up to investigate the adoption of self-assessment mechanisms for assessing cybersecurity compliance in the electricity sector. Typically, relying on the results of a self-assessment tool is a useful technique to reflect on what can be improved; however, this method also includes significant disadvantages. For example, an organization may overplay its strengths or focus too heavily on its weaknesses. This consideration was the main focus of the challenge at the base of the case study. To illustrate this point, the interviewee, a cybersecurity expert, shared a story about a company facing issues caused by compliance misinterpretation and cultural differences.

Case #2: ***Harmonizing Cybersecurity and Compliance.*** This case focuses on the need to evaluate regulatory fragmentation issues and improve compliance in the financial sector. It explores the problem through the lenses of Nadya Bartol and her colleague Charlie Weinberg, respectively Managing Director and Senior Manager at BCG Platinion, of Boston Consulting Group. Through a top-down approach, the two interviewees provided insights into the complex U.S. regulatory system, which is made of a patchwork of approaches, regulations, laws, and rules. The result is that most organizations do not have a unified way of efficiently dealing with cybersecurity and compliance. The lack of harmonization between regulations makes it challenging to keep pace with regulatory obligations, especially for multinational organizations that do business across different countries.

Case #3: A Culture of Compliance: Lessons from a Biopharmaceutical Company. This case examines the compliance environment of a biopharmaceutical company headquartered in the Boston area, MA. Traditionally, in pharmaceutical organizations, compliance responsibilities have been carried out by staff in different business units. Nevertheless, considering the interconnected nature

[1] Complete copies of the case studies are available as Supplemental Materials.

of the pharmaceutical industry, this approach is no longer an option, mainly because patient safety and product quality are highly dependent on information technology. Responding to this new compliance environment was challenging. However, the company developed a strong focus on innovation and security, which placed it at an advantage in creating a robust compliance program and cybersecurity posture.

Case #4: An overview of compliance in the electric utility sector. This case study includes an excursus on the main challenges surrounding compliance in the utility sector. In particular, it relies on the perspectives of industry insider, Dr. Kenneth Wacks. Dr.Wacks worked with companies and regulators from several states in the U.S. Through his consulting work with utilities, Ken had the opportunity to witness the evolution of the process of compliance over the past decades. His experiences are described in the case study and constitute the base in which to evaluate the significant shifts occurring in the electric industry.

Case #5: Understanding the compliance forces that influence cybersecurity in the banking sector, especially in the U.K. This case analyzes several real-life situations in which compliance and cybersecurity are not aligned in the U.K. banking sector. Among the factors that contribute to this misalignment are compliance costs, bank stability, and the interdependencies among European member states. The case also investigates the efforts that have to be made by U.K. banks in developing a compliance system that can measure compliance effectively.

Case #6: Breaking the Vicious Circle Between Compliance and Cybersecurity, especially in the utilities industries. This case is based on an interview with Chris Humphreys, CEO and founder of The Anfield Group, an Austin TX-based Cybersecurity and Regulatory Compliance Consulting firm. With over 18 years of experience in the enforcement and implementation of cybersecurity regulations for electric utilities within the Texas Region and across North America, Mr. Humphreys had the opportunity to observe several weaknesses in the regulatory system. He also noted that compliance is often trapped in a bureaucratic circle where actual cybersecurity is the least of concerns. This cycle is thoroughly described in the case through examples and facts.

Case #7: Managing cybersecurity and compliance in a largely unregulated playing field. This case focuses on the story of an American organization, running one of the world's largest communications networks, operating in a largely unregulated field. The company considered its unique situation ideal to manage cyber risks. They had the capability of implementing regulations if they wanted to and still benefitting from the freedom of not being subject to potential penalties or mandatory audits. However, as the business expanded, the company started questioning its strategies and established a more structured compliance function to ensure that the company met customer needs.

Case #8: Re-evaluating the Approach to Self-Regulation in the Financial Industry. This case study describes how an international financial institution navigates the current cybersecurity environment through a self-regulatory approach. This work used the experience of the company's compliance expert to analyze several critical factors, such as compliance procedures, performance, risks, management practices, and client expectations. Findings revealed that the global interconnectedness of financial markets makes it very challenging for a self-regulated organization to compete and perform at the same level as other organizations.

A detailed description of the cases is provided in Supplemental Materials. Using Case studies was deemed to be a suitable research strategy for addressing the compliance versus cybersecurity issue

as the topic involves a contemporary phenomenon which is dynamic and subject to change. The cases utilize a combination of exploratory, descriptive, and explanatory methods. For the purpose of this work, we collected the data for these case studies through in-depth interviews with Subject Matter Experts, Regulators, C-suite members, and employees from different areas. Findings from our ealier work on compliance guided the development of the cases and research questions. An essential part of the interview process was capturing the participants' perceptions and experiences of dealing with compliance and cybersecurity procedures and complications. In answering questions, interviewees provided perspectives from both regulators' and regulatees' sides, when possible. *Table 1* shows the covered topics by perspectives:

Perspective	**Topics**
Regulators	**Regulatory impact on companies' efforts to be compliant**
	• Observations regarding companies' efforts to comply with regulations
	• The factors preventing organizations from complying with regulations
	• Reasons why regulations may not be sufficient to address cybersecurity issues in some cases
	• Types of effective and ineffective regulations
	Perspectives on regulatory work as regulators
	• Characteristics regulators look for in assessing cybersecurity issues
	• Developments in regulatory cybersecurity compliance over the past years
	• Privacy issues and regulations that come into play in the cybersecurity field
	• Issues in regulatory cybersecurity compliance that need to be addressed
	• Predictions for the future of the regulatory environment in cybersecurity
Organizations	**Perspective on compliance as organizations**
	• Compliance strengths
	• Compliance weaknesses
	• Organizational approaches to cybersecurity compliance
	• Mistakes made with compliance and cybersecurity programs
	• Conflicts between compliance and cybersecurity
	Measurement, improvements, and future plans
	• Key industry-specific regulatory frameworks
	• Measurement techniques to assess compliance efficiency for regulations
	• Decision-making methods related to compliance budgeting and investing

Table 1 - Interview Topics

In addition to the insights provided by interviewees, we used information from publicly available resources about facts and approaches mentioned during the interviews. In the following sections, we describe the stakeholders involved in each case and how their goals may overlap. We continue by illustrating the issues generated from these conflicts. Finally, we outline the similarities and differences that emerged from the case assessment and the lessons learned to improve the efficiency and effectiveness of cybersecurity and compliance functions.

3. Stakeholders and Conflicting Goals

Today's regulatory landscape is very dynamic. Analyzing the compliance development of an organization only from a procedural and legal perspective can lead to a myopic and distorted view of the complex universe that surrounds the organization itself. Many studies have reported on the effectiveness and importance of a multidisciplinary approach to analyze compliance. For example, Gelderman et al. (2010) elaborated a multidisciplinary framework to assess the factors affecting

compliance with E.U. directives in Europe. Coates and Srinivasan (2014) have also adopted a cross-disciplinary literature search methodology for conducting systematic reviews of the impact of the Sarbanes-Oxley Act over the years. In the literature, this type of methodology has been further strengthened by the study of the specific relationships and interests of an organization. The idea that lies at the foundation of this concept can be tied back to the Stakeholder Theory, a conceptual approach originally advanced by Robert Edward Freeman in the early 1980s. This theory paved the way for developing a line of reflection focused on the importance of the actors who can influence or be influenced by the strategies that the company puts in place (Freeman and Reed 1983). In particular, Freeman (2004) provides a comprehensive definition of "stakeholder" as "any group or individual that can affect or is affected by the achievement of a corporation's purpose." In recent years, to be responsive to current organizational needs, several international standards have included similar definitions in their requirements and guidelines. For example, the requirements specified under clause 4.2 of ISO 27001:2013 place particular attention to "understanding the needs and expectations of interested parties." This definition is common to many standards and is also applicable for analyzing the case studies described in this paper.

As a first step, for each case, we identified the key stakeholders and their interests. In the context of compliance, the stakeholders are those who can affect or are affected by the regulations or the regulatory system in general. Examples may include, but are not limited to, those who own or run businesses, those who govern at the national, regional, or local level, those who manage the various internal aspects of compliance, and those who develop regulations. Stakeholders could also include the media, which can be an "enemy" or a "friend," depending on the way information is conveyed. For example, in Case 8, the media are described as a "trigger factor" when it comes to regulatory compliance as they drive reputation. As stated by the interviewee who participated in the case, "the media are often the first to know about a cyber incident, and the first to pronounce on it." Consequently, companies tend to rush to be compliant to avoid reputational damages. More broadly, stakeholders include countries that can be affected by cybersecurity events, international regulatory decisions, or interdependent issues occurring at the global level. Each of these different types can be categorized into one of the following six categories, which represent the stakeholders identified in the case studies[2]:

- **Legal and Compliance.** A compliance system includes a combination of internal and external mechanisms from a legal and compliance perspective. Internal mechanisms are carried out by those who deal with compliance management oversight, legal obligations, independent internal audits, and policy development (referred to as "internal enforcers"). External mechanisms are imposed on organizations by external stakeholders, such as regulators, governments, industry associations, external auditors, and financial institutions (referred to as "external enforcers").
- **Security professionals.** Security stakeholders help organizations understand how to translate compliance into actual security. Examples of security professionals belonging to this category include CISOs, IT security managers, IT security analysts, IT support managers, risk managers, etc.
- **Leadership and governance.** This category includes those who deal with the alignment of compliance requirements with business needs and results, business risk, processes, projects,

[2] It is important to note that these categories can get "blurred," depending on the tasks or the situation. In this case, the stakeholders assume a transversal role. For example, the Chief Risk Officer (CRO) can be a decisive force for combining company-wide efforts and creating more efficient compliance outcomes.

and people. These stakeholders are represented by C-suite members with business-related tasks, program managers, project managers, business analysts, etc.

- **Finance.** Depending on the industry in which they operate, companies may face considerable fines and business impacts if they fail to comply with laws and regulations or get hit by a cyber attack. Deciding on how to invest money in a way that is consistent with compliance and cybersecurity is one of the most critical responsibilities. This task is carried out by CFOs, finance managers, budget owners, etc.
- **Countries/international actors:** Until recently, little attention has been devoted to whether states and other international actors comply with regulations. The traditional view of international compliance assumes the presence of a hierarchical regulatory system composed of static interactions. According to this view, compliance moves from international agreements to national regulations and, finally, to local regulations. The main characteristic of this system is its staticity because it is based on the assumption that it is possible to capture and monitor the status compliance with regulations at any level of this hierarchy in an accurate way. However, the current realistic framework for global regulatory compliance is non-hierarchical and views compliance as a dynamic process changing over time. The current global system involves many actors other than single states, including intergovernmental and non-governmental organizations, private organizations, and individuals. All of these "non-traditional actors" interact in complex ways that go beyond agreements and legislation; they alter the balance in the existing regulatory schemes, thus playing a key role in how organizations and individuals interpret, implement, and comply with regulations. Consequently, the lines between international, national, and local compliance measures are fading, and mandatory compliance, although often necessary, is increasingly being perceived as a burden in this context.

In addition to identifying the stakeholders, connections between them need to be considered as they can significantly influence each other through their interactions. It is important to note that stakeholders often have different, often conflicting, goals and priorities, depending on their perspective on compliance and the role they have. Table 2 shows the problems associated with the stakeholder interactions detected in the case studies.

	Stakeholders' categories				
	Legal and Compliance	**Security professionals**	**Leadership and governance**	**Organizations**	**Countries/International actors**
Goals	Meet political, legal, and industry expectations	Implement modern and scalable regulations	Balance compliance and cybersecurity costs	Have a comprehensive overview of cybersecurity and compliance	Comply with national and international regulations
Observed Problems	Poor compliance oversight and management	Difficulty in developing/ implementing regulations	Challenging to allocate resources and budget	Lack of compliance culture (responsibility, collaboration, metrics, etc.)	Geographical implications cause high systemic risk

Table 2 – Stakeholders' Category and Conflicting Goals

Most of the issues derived from the analysis of the cases emerge when the interests of stakeholder categories are not appropriately balanced or harmonized. In addition, the pressure for organizations

to comply with regulations and address cybersecurity threats has grown over the past years. Consequently, the number of regulatory compliance challenges that need to be tackled is correspondingly growing. The factors contributing to these difficulties have been long-observed in the literature on cybersecurity compliance (Donaldson et al., 2015; Evans at al., 2016; Meglio, 2020; Mohammed, 1970; Thaw, 2014). Although most studies focused on practical aspects of cybersecurity compliance, they looked at compliance issues from a theoretical perspective, paying particular attention to the structuring of regulatory concepts and patterns. However, the reality of making compliance decisions is often more complicated than is portrayed in previous research. Therefore, due to the dynamic nature of cybersecurity compliance, it is necessary to expand these studies by conducting an in-depth investigation of the challenges to explore underlying principles' causes.

4. Observed problems

One challenge with compliance is that it can be an opportunity for a company (or a regulator) to grow or can be the setback that leads to failure. The outcome depends on how compliance is addressed. To understand how compliance problems are dealt with, we analyzed each issue identified in Table 2 in each case study, starting from their root causes, to the ways they impact the business, practices, or relevant stakeholders. Additionally, we examined the methods used or proposed by interview participants to address the problems arising from regulations or inefficient procedures.

***Observed Problem #1: Poor compliance oversight and management*:** There is a very delicate balance in the relationship between regulatory and industry needs. Ideally, this interaction involves a confrontation between the regulator and the industry, especially when it comes to new problems that have not previously been explored. The reality is that, whether they are cooperative or conflictual, regulators are inevitably less efficient than industry in incorporating changes and implementing the right oversight and management measures. For example, as shown in Table 2, this issue is mostly discussed in Case 7. According to the interviewee, there can be a significant misalignment between auditors external to organizations (external enforcers) and organizations themselves (internal enforcers).

This divergence stems from the lack of knowledge that is available to auditors as opposed to those who actually work on the systems. Such a conflicting situation is subject to a lack of accuracy and a false sense of security. One way to address this problem involves focusing on the company-specific cyberthreats while keeping compliance as a guide. Another example of misalignment is described in Case 4. Political implications and differences between state and federal regulators are likely to create confusion with respect to which regulatory body is responsible for overseeing compliance. Case 8 also discusses how privacy requirements dictated by standards and regulations create barriers to compliance oversight and data security. Consequently, privacy restrictions limit customer data security. Finally, other factors are reported to contribute to compliance management issues, such as unclear internal compliance structures and the excessive number of regulations and regulators. The methods that interview participants used to improve these situations include allocating and coordinating appropriate compliance roles, engaging in diverse compliance processes, and prioritizing inspections where there is a lower level of control or a higher risk in certain areas (e.g., safety) is perceived.

Problem #1	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8
Causes	Unclear compliance roles and information	Multiple regulators and regulations	Single compliance function	Political difficulties	Misalignment between compliance and business goals	Regulators place compliance responsibilities on companies	Misalignment between auditors and organizations	Privacy limitations
Impact	Vulnerable cybersecurity posture	Administrative burdens and high compliance costs	Confusing compliance outcomes and evidence	Inadequate inspections and consequent incidents	Conflicting situations, non-compliance	Focus on compliance but neglect security	False sense of security	Ineffective security
Solution Methods	Improve compliance responsibility	Establish a common framework	Engagement in diverse compliance processes	Prioritize inspections	Handle compliance as a business decision	Develop a "compliance through security" mindset	Focus on company-specific cyberthreats	Data flux measurements

Table 3 – Analysis of Observed Problem #1: *Poor compliance oversight and management*

***Observed Problem #2: Difficulty in developing/implementing regulations*:** Excessively complex and numerous regulations contribute to increased misalignments between regulatory and security goals. For example, Case 1 discusses the problems arising when organizations do not have a correct understanding of laws and regulations. Case 2 and 7, instead, examine the variations and issues in the implementation of regulations. In particular, Case 2 focuses on the ambiguous regulatory language. It illustrates how regulations are thematically similar but semantically different.

On the one hand, complex regulatory frameworks provide the illusion of a more controlled and comprehensive regulatory system; on the other hand, it creates incentives for regulated entities to circumvent the system. Most importantly, such a complex environment risks providing requirements that are not well perceived. As a result, companies are often blamed for not implementing the appropriate controls (Case 6). To address this issue, Case 4 suggests developing a more organized regulatory approach to understanding companies' needs, developing knowledge, and promoting institutional memory. However, Case 3 provides a different perspective and places the attention on employees rather than regulations. Employees may not be clear on how to accomplish their compliance tasks, leading to inadequate compliance decision-making.

Problem #2	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8
Causes	Unclear laws and regulations	Unclear regulatory language	Unclear compliance tasks	Lack of adequate skillsets	Organizations are unprepared for new regulations	Outdated and slow regulatory model	Too many regulatory variations	Too much bureaucracy and governmental intervention
Impact	Legal consequences, fines, breaches	Contradictory evidence for the same requirements	Inadequate decision-making	High dependence on consultantants	Wrong practices, liability issues, data exposure	Blame is placed on companies	Lack of objectivity	Ineffective and slow implementation of requirements
Solution Methods	Adequate training	More focused regulatory language	Implement compliance as a chain-management process	A more organized regulatory approach	Identify essential areas of compliance	Proactive strategy	Scalable assessment of security capabilities and deficiencies	Training and increased support from the top

Table 4 – Analysis of Observed Problem #2: *Difficulty in developing/implementing regulations*

***Observed Problem #3: Challenges to appropriate allocate of resources and budget*:** Budgets and the resources necessary for compliance functions are profoundly intertwined in an organization, as presented in Case 3. For this reason, a significant compliance challenge organizations face is balancing budgets in the face of increasing compliance and cybersecurity costs. Budgetary restrictions, external pressures (e.g., increased industry and customer expectations), and fear of penalties play a crucial role in budgeting choices. For example, financial organizations often are called to make difficult decisions, such as prioritizing financial stability over cybersecurity (Case 5).

Additionally, investing in cybersecurity and compliance is objectively a different process than other business investments. For example, in a field where regulations are too descriptive, costs to meet the high level of regulatory specification is hardly sustainable (Case 2). Sometimes, requests for these types of investments need special authorizations, which slow down operations, procedures, and developments (Case 8). However, tackling this problem is not just a task reserved only to the finance department; it requires cooperation between risk and compliance functions. In particular, Case 8 suggests engaging the cybersecurity, legal, and compliance department to assess which risks have the greatest potential for damages and prioritizing investments. A different approach is illustrated in Case 7 as it proposes to dedicate resources to identifying requirements that may apply to the organization and creating a customized plan. From a regulatory point of view, Case 2 and Case 6 describe two possible solutions. The first recommends to simplify compliance requirements and help organizations focus on the resources that matter most. The second points out that tax cuts benefits would help minimize the effects of the current punitive regulatory model and, consequently, enforcement exposure[3].

Problem #3	**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**	**Case 7**	**Case 8**
Causes	Budgetary restrictions and external pressures	Regulations are too descriptive	Compliance risk is interconnected	Misalignment between regulators and companies	Pressures prioritize to financial stability	Fear of penalties and fines	Unregulated industries provide budget freedom	Special authorizations for certain investments
Impact	Adoption of unreliable/inadequate compliance measures	High Costs	Issues related to budget preparation and tracking	Wrong investments	Cybersecurity budget cuts, broader risks to stability	Cuts in areas, such as training and awareness	Lack of focus	Slow operations, vulnerabilities
Solution Methods	Set realistic expectations to identify gaps, and allocate resources accordingly	Simplify compliance requirements	Apply the 80/20 rule to compliance	Adequate incentives for long-term innovation and security	Prioritize investments	Tax cuts benefits	Create a customized plan based on regulations	Engage the cybersecurity, legal, and compliance department

Table 5 – Analysis of Observed Problem #3: *Appropriate allocate of resources and budget*

***Observed Problem #4:* Lack of compliance culture (responsibility, collaboration, metrics, etc.):** A culture of culture comes from the top of an organization. The role of the board is critical to the long-term success of a compliance program. However, as new regulations emerge, it is often hard for an organization to establish the appropriate training programs to educate employees on new regulations and the related changes. One of the problems is that organizations struggle to

[3] Enforcement exposure refers to the conditions that amplify the likelihood of an actual or potential breach of any regulatory control or requirement.

communicate regulators' expectations and fail to plan compliance procedures efficiently (Case 2). Aligning employees to compliance culture is in every organization's interest, but there may be difficulties in allocating responsibility to establish a culture that encourages the successful implementation of regulations.

For example, Case 3 focuses on why employees do not talk about compliance and are slow in implementing requirements. Therefore, internal issues are among the most critical hindrances to compliance culture. Although high turnover can create obvious problems for an organization, low turnover is also an area organizations need to keep an eye on when it comes to compliance. By retaining employees for long periods of time, companies are unlikely to have the necessary new talents needed to deal with changing technologies and related compliance requests and challenges (Case 4 and 8). However, external issues also have an impact on the overall compliance culture. In the utility sector, for instance, regulatory commissioners' competencies are often not comprehensive enough to operate in the real-world utility environment. This fact may severely limit their ability to relate to companies' needs and motivate them to achieve compliance. The development of clear regulatory objectives and private-public cooperation are some of the solutions suggested by interviewees.

Problem #4:	**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**	**Case 7**	**Case 8**
Causes	The compliance function is fragmented	Difficulty to understand regulators' expectations	Lack of conversations on compliance	Regulatory commissioners do not have comprehensive skills	Compliance functions and board members are not aligned	Misalignment between compliance and security divisions	Lack of efficient exchange of information between departments	Low turnover
Impact	Failure to turn regulatory information into organizational objectives	Communication issues	Legal penalties, bad behaviors, lack of feedback, room for vulnerabilities	Lack of motivation, accountability issues	Wrong business decisions, non-compliance, vulnerable security	Compliance misunderstandings, loss of competent professionals	Partial view of cyber risk and compliance	Lack of "fresh knowledge"
Solution Methods	Establish clear compliance roles	Common and clear regulatory objectives	Promote collaboration, regular communication exercises	Encourage private-public partnership	Cost-benefit analysis in compliance	Encourage internal information sharing	Establish a separate compliance function	Focus on behavioral change

Table 6 – Analysis of Observed Problem #4: *Lack of compliance culture*

Observed Problem #5: **Geographical implications cause high systemic risk:** Regulations uniquely impact organizations and the global actors connected to their operations. However, the existing regulatory structure does not consider the individual characteristics and values of the organizations' context (Case 4). Although most these regulations are managed locally, their scope and impact can be global. This issue was also the subject of a speech on "Regulators need to develop global cyber security standards" by Daniel Pinto, Chief Executive of JPMorgan's Corporate & Investment Bank (Reuters, 2017).

> "Each country has a different standard, but we have a global problem [...] When you go to point where you have to have different standards in every place, you put yourself in a vulnerable position."

His comment shows growing concerns about compliance with cybersecurity standards across different countries. Organizations have many complex challenges to address, ranging from demonstrating compliance with international regulations to adapting regulations to their culture (Case 3 and 2, respectively). The lack of a global supervisory system also increases organizations' exposure to threats. Case 7 suggests adopting a global framework (e.g., the NIST framework) and integrating it into the organization's security strategy to minimize the risk of exposure. Finally, one point noted in Case 8 is that regulations should permit different degrees of choice in how to integrate cultural and operational differences.

Problem #5	**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**	**Case 7**	**Case 8**
Causes	Countries have different perceptions of cybersecurity	Lack of a unified cultural approach	Demonstrating compliance differs from context to context	The existing regulatory structure does not consider the single state's characteristics	High-level interdependencies between countries	Lack of a global regulatory oversight	Unregulated industries are still subject to cross-country cyber risks	Compliance expectations differ depending on the geographical area
Impact	Hard to promote compliance responsibility in the same way	Difficulty to adapt regulations to different cultures	Liability issues	Regulations do not apply to every environment	increased bureaucracy, liability issues, and compliance work	Increased exposure	Possible lack of reputation /competitive advantage at a global level	External pressures, forced compliance adaptation
Methods	Value-based approach	Assess organizations' global impact	Accountability-based approach	Flexible regulations to cover all situations	Focus on the regulation scope and legal implications	Develop a risk-based approach	Opt for a global framework	Possibility to integrate compliance differences

Table 7 – Analysis of Observed Problem #5: *Geographical implications cause high systemic risk*

Each case study presents a description of the approach taken by every company or interviewee towards the previously mentioned issues. The following sections aim at analyzing these problems and the multiplicity of approaches and conclusions among the different cases.

5. Comparison analysis

To measure the relationships between the problem variables emerging from the cases, we conduct a comparative analysis. In particular, given a unit of comparison (represented by key concepts extracted from the observed problems), we explain similarities between cases in terms of common features or processes, and differences according to the principle of variation[4]. Table 8 summarizes the key results of the analysis.

[4] The principle of variation involves comparing different characteristics of a single phenomenon to find differences among variables and demonstrate a standard of variation in the nature, frequency, or intensity of that phenomenon (Pickvance, 2005).

Comparative analysis		
Unit of comparison	**Observed similarities**	**Observed differences**
Management	Incorporating multiple compliance regimes is difficult	The same management action can lead to different outcomes
Budgeting	Leadership is unwilling to commit the money and time needed for compliance and cybersecurity efforts	Compliance investment decisions are often caused by different factors (punitive regulatory system, organizational priorities, etc.)
Enforcement and Implementation	Interpretation issues can be difficult due to fragmented/outdated regulatory development	Different industries have different requirements
Culture	Unclear roles and responsibilities impact compliance communication and operations within organizations	The way compliance functions and reporting lines are implemented determine the type of compliance culture
Geographical influences	Compliance programs face challenges in balancing global requirements with local needs	The effects of geographical factors vary depending on the security culture of a country

Table 8 – Comparative Analysis

The results of the analysis are described in the following summary:

- ***Management:*** The most common management issues faced by the organizations described in the cases involve dealing with multiple compliance regimes and coordinating with internal and external enforcers for reporting on compliance outputs. Companies struggle to achieve their desired outcomes and understand the parameters within which they have to integrate regulatory requirements into their compliance programs. Improving compliance responsibility. Among the methods suggested to address these management flaws, implementing transparency and improving responsibility seem to be the most efficient. The first involves being upfront and visible about the compliance actions an organization takes and ensuring that those actions are consistent with its core values. In an organization where there is alignment between regulations and their values, it is easier to raise or disclose difficulties. The second implies making every employee aware of their responsibilities in relation to adhering to or implementing regulations and the importance of compliance to the success of the organization as a whole. An interesting finding is that this management issue has different impacts depending on the organizational context. Consequences range from legal and liability issues to slow compliance procedures and confusing compliance outcomes. This consideration places a high level of importance on training, which needs to be based on real-life cases and delivered according to specific contexts.
- ***Enforcement and Implementation:*** Most of the participants reported a generally negative experience towards interpreting compliance requirements correctly. The most common examples included issues associated with fragmented or unclear regulatory information, outdated regulations, and overly technical language. These issues are particularly worrisome to organizations as they contribute to increasing enforcement risks, leaving them vulnerable to violations of regulations and reputation damages. The technique used by the majority of the interviewees to improve this aspect involved proactive compliance strategies to anticipate or fill potential regulatory gaps. Additionally, harmonizing regulatory language

and concepts is a commonly desired long-term goal, although several complicating factors complicate the achieving of this objective (e.g., politics, bureaucracy, etc.). However, one point of variance is that different industries have different requirements, and, therefore, different metrics to interpret regulations. Additionally, implementing compliance value and managing expectations vary depending on business goals.

- ***Budgeting***: It was observed that the many cases struggle to commit appropriate resources to compliance and cybersecurity efforts, leaving organizations vulnerable and subject to fines. The main problem lies in the fact that organizations fail to implement a comprehensive budgeting and risk assessment strategy. To address this problem, most participants agreed that all assets in the organization do not have to be assessed and protected in the same way. From a regulatory point of view, instead, one of the recurrent suggestions was encouraging compliance efforts and placing greater emphasis on incentives. However, while all the interviewed companies share this problem, the difficulties associated with compliance budgets are caused by different factors. Examples include issues associated with a punitive regulatory system, organizational priorities, descriptive regulations, fear of penalties, etc.
- ***Culture:*** Unclear organizational roles and responsibilities seem to play a significant role in all cases. These factors have a significant impact on compliance communication and operations within organizations. Two frequent approaches to addressing this issue include engaging the full set of stakeholders to ensure appropriate compliance support and decision-making and promoting information sharing and collaboration. Nevertheless, the greatest range of variation on this issue is represented by the compliance structure and reporting lines, which seem to drive the way compliance culture is built in different ways. How regulated organizations structure their compliance functions to respond to complex challenges plays a crucial role in establishing a strong compliance culture and developing an identity. Not only is the function's composition important, but also its role within the organization. For example, in some circumstances (e.g., Case 1), organizations must show that compliance is a separately identifiable function within the organization, with clear reporting lines to senior management. In other cases (e.g., Case 3), placing the responsibility for implementing controls solely on the compliance team might not be a practical approach. Thus, it may be more suitable for them to get the C-suite involved to integrate compliance into the "fabric" of their culture.
- ***Geographical influences:*** The analysis identified a commonality in participants' experiences with balancing global requirements with local or organizational needs. The cases also presented a common level of discussion on the need to develop more flexible, adaptable, and dynamic regulations. However, the effects of geographical factors vary depending on the security culture of a country. Several cases discuss how each country's concept of security has a different impact on the effectiveness of a company's efforts to promote consciousness on cybersecurity issues. For example, raising awareness is a legal requirement under some regulations (e.g., GDPR), and cultural differences may result in different compliance outcomes. One suggested way to address this variation is a combination of rules-based and principles-based approaches as well as strengthening cooperation among foreign authorities.

6. Conclusions

Although compliance is a critical component of any cybersecurity program, new challenges and issues keep emerging, which require the attention of both regulators and organizations. For

organizations, it is problematic to collaborate and align all processes and goals to comply. It takes a considerable amount of time and effort to stay on up of the regulatory changes and get everyone prepared to support the compliance process. Organizations often see compliance and security in a very different light. Thus, dealing with the nuances of an ever-changing technology-driven society is becoming complicated and is forcing organizations to consider solutions that go far beyond what industry regulations are asking for. The regulatory side is also facing pressure from increased industry changes, which are becoming more and more cross-sectoral. In particular, regulators are faced with two different but interconnected challenges, one relating to the almost impossible task of determining criteria to ensure security and the other relating to the legitimacy of cybersecurity procedures.

The case studies analyzed in this paper represent eight different views of dealing with these challenges. After conducting the comparative analysis, one way to look at the complicated cybersecurity versus compliance dilemma is that compliance and cybersecurity are both "flawed," but for different reasons. Cybersecurity and compliance have similar goals around securing data and assets by managing risk. Both deal with measures and controls to reduce risk. However, the cases suggest that compliance is primarily driven by enforcement risk, while cybersecurity is generally driven by business risk. Compliance from the standpoint of cybersecurity means making sure business meets the security requirements that are applicable to specific industries. By achieving cybersecurity compliance, organizations avoid fines and sanctions as well as financial and reputational damage associated with breaches. However, while both enforcement and business risk may play a role in contributing to the security of an organization, there is a perception that cyber risk does not seem to rise to the same level of priority as other business areas that are apparently disconnected from the cybersecurity realm, such as quality, market, customer satisfaction, etc..

Many, if not most, of the professionals interviewed mentioned that risk is managed separately and that each risk area has different risk-rating and controls. However, a realistic evaluation is that risk is interconnected and requires a broad understanding of internal and external factors that can impact business goals. In this context, companies struggle to find a method to assess cyber risk in a way that enables them to compare it to other business and compliance risks. As a result, misalignments between those charged with compliance and security responsibilities become deeper and deeper. The findings provided in this work have led to the consideration of a more holistic approach to risk, allowing organizations to determine a more realistic and acceptable threat-threshold to be used in analyzing exposure to legal penalties, financial issues, and cybersecurity. Future studies are needed to understand the optimal approach for managing the multiple risks involved in cybersecurity compliance and evaluating the potential of this change in strategy.

Acknowledgements

The research reported herein was supported in part by the Cybersecurity at MIT Sloan initiative, which is funded by a consortium of organizations, and a gift from C6 bank. The authors are grateful to Nadya Bartol, Charlie Weinberg, Kenneth Wacks, Chris Humphreys, and other subject matter experts for their availability to be interviewed and their support of this research.

References

Coates, J. C., & Srinivasan, S. (2014). SOX after ten years: A multidisciplinary review. *Accounting Horizons, 28*(3), 627-671.

Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). *Security solutions for hyperconnectivity and the Internet of things.* IGI Global.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). *Meeting the cybersecurity challenge. In Enterprise Cybersecurity (pp. 27-44).* Apress, Berkeley, CA.

Duncan, B., & Whittington, M. (2014, September). Compliance with standards, assurance and audit: does this equal security?. In *Proceedings of the 7th International Conference on Security of Information and Networks* (pp. 77-84).

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679.

Freeman, R. E. (2004). The stakeholder approach revisited. *Zeitschrift für wirtschafts-und unternehmensethik, 5*(3), 228-254

Freeman, R. E., & Reed, D. L. (1983). Stockholders and stakeholders: A new perspective on corporate governance. *California management review, 25*(3), 88-106.

Gelderman, K., Ghijsen, P., & Schoonen, J. (2010). Explaining non-compliance with European Union procurement directives: a multidisciplinary perspective. *JCMS: Journal of Common Market Studies, 48*(2), 243-264.

Hardy, I. T. (1993). *The proper legal regime for cyberspace*. U. Pitt. L. Rev., 55, 993.

Madnick, S., Marotta, A., Novaes Neto, N., & Powers, K. (2019). Research Plan to Analyze the Role of Compliance in Influencing Cybersecurity in Organizations. Available at SSRN: https://ssrn.com/abstract=3567388

Marotta, A., & Madnick, S. (2020). Analyzing the Interplay Between Regulatory Compliance and Cybersecurity. *The 19th Annual Security Conference*, Las Vegas, NV. Available at http://029e2c6.netsolhost.com/II-Proceedings/2020/1.pdf

Marotta, A, Pearlson, K. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. In: *Proceedings of AMCIS 2019* (Americas Conference on Information Systems), Cancún, Mexico. Available at https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/24/

Meglio, M. (2020). *Embracing Insecurity: Harm Reduction through a No-Fault Approach to Consumer Data Breach Litigation.* BCL Rev., 61, 1223.

Mohammed, D. (1970). Cybersecurity compliance in the financial sector. *The Journal of Internet Banking and Commerce, 20*(1), 1-11.

Pickvance, C. (2005). The four varieties of comparative analysis: the case of environmental regulation. *Paper for Conference on Small and large-N comparative solutions*, University of Sussex.

Reuters (2017), Regulators need to develop global cyber security standards. Retrieved from https://www.reuters.com/article/usa-iif-banks/regulators-need-to-develop-global-cyber-security-standards-jpms-pinto-idUSL4N1MP093.

Thaw, D. (2014). *The Efficacy of Cybersecurity Regulation.* Georgia State University Law Review, 30.