Issues in Information Systems
Volume 22, Issue 1, pp.10-50, 2021

https://doi.org/10.48009/1_iis_2021_10-50

Convergence and divergence of regulatory compliance and cybersecurity

Angelica Marotta, *MIT Sloan School of Management, amarotta@mit.edu*
Stuart Madnick, *MIT Sloan School of Management, smadnick@mit.edu*

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.

Keywords: Compliance, Cybersecurity, Risk Management, Regulations.

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 analyzes the scope and complexity of specific compliance and security needs.

Background and literature review

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 a 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. The findings revealed that each sector presents critical and overlapping issues, showing the need to further investigate the related practical implications. Therefore, to exemplify the theoretical observations defined in the earlier work, we conducted eight case studies (described in the following section) of companies operating in different industries. In analyzing the compliance environment of each case study, we observed that it was necessary to find a key for interpreting the results. However, assessing the cases only from a procedural and legal perspective can lead to a myopic and distorted view of the complex universe that surrounds each case. Many studies have indeed 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 appraoch 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 & 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 at the base of this paper.

Main contributions

This paper aims to offer an overview for understanding different compliance environments and their impact on cybersecurity using a comparative analysis of eight interview-based case studies. The eight cases are briefly summarized below (a detailed description of the cases is provided in Appendix):

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 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.

We used these cases to 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. In the following sections, we first discuss the methodology adopted in our analysis, and then 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

Methodology

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:

Table 1. Interview Topics

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

In addition to the insights provided by interviewees, we used information from publicly available resources about facts and approaches mentioned during the interviews.

Stakeholders and conflicting goals

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:

- **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, 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.

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.

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.

Table 2. Stakeholders' Category and Conflicting Goals

	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

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.

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.

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

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

***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.

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

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 consultants	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

***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 practical 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 (i.e., the conditions that amplify the likelihood of an actual or potential breach of any regulatory control or requirement).

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

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

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 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 extended 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.

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

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

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.

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

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

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.

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 (i.e., 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). Table 8 summarizes the key results of the analysis.

Table 8. Comparative Analysis

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

Findings

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.

Discussion of findings

The case studies analyzed in this paper represent eight different views of dealing with compliance 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.

Limitations

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 services. However, we noted one limitation of the case study approach adopted in this study. A large portion of data collected during the interviews was confidential given the nature of the facts and practices under discussion. Therefore, due to the high degree of sensitivity of the matters involved in the cases, we had to limit our analysis to a more general and restricted information set.

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. However, these challenges should not mean that the role of regulators in the cybersecurity sector needs to be diminished. While regulators can't control every aspect of cybersecurity, they must position themselves as enablers more than enforcers and facilitate the development of cybersecurity based on the confrontation between past and contemporary approaches.

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. University of Pittsburgh Law Review, 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. *Boston College Law Review, 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*(2), 287-374.

APPENDIX: CASE STUDIES

The following eight case studies represent the real-life experience of a range of stakeholders working across different cybersecurity compliance environments and geographical locations. The approaches and situations described in the cases reflect the observations that emerged during interviews with experts in the field conducted over one-year period.

CASE #1: INTERPRETING COMPLIANCE RESULTS

A compliance journey generally starts with one question: "Where do we stand concerning the regulations?" In a survey conducted by Deloitte[1], it was found that nearly half of the respondents used self-assessment tools to answer this question. To be and remain compliant, organizations need to implement constant measurement, which is usually a challenge. Legal and consulting costs, pressure on achieving regulatory objectives, budgetary restrictions, and increased industry, and customer expectations are just some of the issues forcing organizations to consider the adoption of self-assessment mechanisms. These evaluation tools can offer a low cost, quick assessment, and are often technically accurate on topics that can be demanding for organizations of all sizes.

However, as tempting as it is for an organization to rely just on the results of a self-assessment tool, this method also includes weaknesses. For example, one of the disadvantages of relying on a self-assessment tool is that it is difficult to be objective. This consideration emerged in an interview with a cybersecurity expert whose role focused on compliance issues within an organization operating in the electricity sector. To exemplify this point, he shared a story about a company with a challenging mission: achieving compliance for their critical assets.

Overview

When the company established a corporate program to enhance cybersecurity posture, meeting cybersecurity requirements was one of the most crucial topics of discussion. In the beginning, building compliance into the organization's DNA seemed difficult, especially considering that their critical infrastructure included a high number of distributed assets. Among the most challenging tasks was, for example, dealing with the lack of organizational measures. Not only could a hack on a single portion of the infrastructure compromise a part of the system, but it could also compromise the entire system. This operation seemed to be impractical without external aid, so they decided to evaluate their compliance status through a self-assessment tool to measure their security controls. Thus, after setting a date for completion, they started the assessment, and during the procedure, they ran monthly meetings with local cybersecurity experts to check the progress. This strategy seemed to be successful, and when the deadline approached, almost all business units were reported to be "green." In other words, the assessment produced excellent results, according to the tool's scoring system. However, despite this positive outcome, unfortunately, an incident occurred. According to the interviewee, one of the reasons why this incident happened is the growing pressure to comply with the strict internal ICS Cybersecurity policy. In a rush to become compliant, the organization neglected fundamental security measures and practices and put scores that not completely reflected reality. One, for example, included relying on the tool's indicators without correctly interpreting their meaning. He explained,

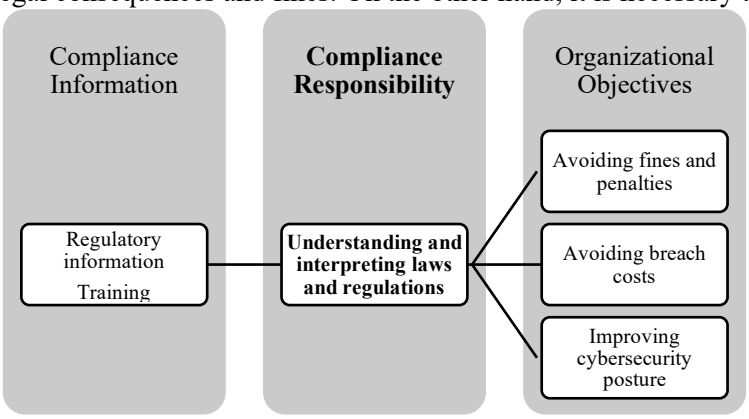
"If your outcome is 'green,' it means that your compliance level can range from 95% to 100%, but it doesn't necessarily mean that you are fully secure. In the case of the company, their reports indicated a

[1]https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/Deloitte%20Compliance%20Survey%20Report_Finland.pdf

compliance score of 98%. However, in interpreting this result, it is also necessary to remember that improvements are still required."

Interpreting compliance

As shown in Fig. 1, interpreting compliance also implies a responsibility, which, in this context, assumes a double meaning. On the one hand, organizations are responsible for correctly understanding laws and regulations to avoid legal consequences and fines. On the other hand, it is necessary to accurately interpret



the rules to address the cyber risks involved and avoid the high costs associated with potential data breaches (e.g., reputation damages, losses, etc.).

Figure 1. Compliance responsibility

To fulfill this responsibility, organizations need to be equipped with the appropriate regulatory information, and in parallel, be trained on how to turn this information into organizational objectives. However, taking accountability for the compliance function seems to be a challenge for many organizations as there is significant fragmentation across business units. According to the interviewee, companies lack a fluid, comprehensive compliance strategy that includes clear roles. A KPMG's study[2] on the topic also shares this view. The survey found that only 3% of the respondents said that the compliance function is the responsibility of a specially designated person within their organization and that 61% structured compliance as a separate function.

Most of the attitudes towards compliance operations — and the extent to which those operations contribute to keeping organizations secure — are mostly dependent upon people and how people perceive cybersecurity. The cybersecurity expert added,

"If organizations fail to allocate responsibility for overseeing compliance, they will never be secure. For example, let's assume that one of the regulatory requirements is to protect customer data by installing a firewall. Once you install a firewall, you can probably remove this task from your compliance checklist. However, although meeting this requirement seems to be sufficient from an audit perspective, it doesn't mean that it is also enough to guarantee security. What if the firewall is not configured correctly? What if no one knows how to manage it? Having the right person in charge is key to providing a comprehensive evaluation."

Results

Thus, integrating responsibility into compliance means moving from just viewing compliance as a checkbox exercise to a more value-based approach. However, values may vary from culture to culture.

[2] https://home.kpmg/content/dam/kpmg/ru/pdf/2017/07/ru-en-international-compliance-survey.pdf

According to the interviewee, different cultures have a different understanding of cybersecurity. For example, Western-European states generally share some regulations, but actual compliance practices may vary widely across countries and areas. A Western-European approach to compliance may, therefore, need regional adaptation to manage cybersecurity efficiently. Achieving a balance between compliance and cybersecurity is, therefore, determined by the cultural context in which companies operate and the people, practices, and beliefs that form the culture of each organization.

CASE #2: HARMONIZING CYBERSECURITY AND COMPLIANCE

When it comes to cyber threats, the financial sector is often one of the most exposed to cybercrime. Financial data are becoming more and more appealing to cybercriminals, and it is not surprising that the trend is growing[3]. According to a Ponemon research[4] conducted in collaboration with Accenture, the banking sector continues to have the highest cost of cybercrime, and the total number of attacks in this industry is rising steadily. For example, the most expensive and frequent attacks for financial institutions are banking Trojan botnets and Denial of Service[5][6]. Not only do the consequences of these types of attacks cost organizations an average of $200,000, but they also cause damages to intangible assets, such as customer trust and brand reputation[7]. Additionally, the time to recover from these attacks is getting longer due to several factors, including evolving complexity, interconnections among financial institutions, etc.[8]. Recognizing the critical nature of the financial sector and the significance of these threats is one of the top priorities on the regulatory agenda for many authorities around the globe[9]. The main goal is designing regulations to facilitate cyber risk mitigation and enhance cybersecurity resiliency[10].

Introduction

According to a report[11] from Boston Consulting Group (BCG), navigating the increasingly complex system of regulations is particularly challenging for financial institutions. BCG Platinion, a Boston Consulting Group company, has a tradition of working with leading organizations in the financial sector. Nadya Bartol, Managing Director at BCG Platinion, and her colleague Charlie Weinberg, Senior Manager at BCG Platinion, had the opportunity to examine the regulatory situation in the financial service industry first-hand. They believed that compliance follows a top-down approach; it starts with regulators assuming that supervised entities need help navigating the cybersecurity world. This assumption then turns into requirements, which manifest themselves in different ways, such as standards, regulations, etc. Organizations are the final component of this process as they need to meet and integrate these requirements according to their capabilities and maturity level. Charlie commented:

"I think compliance can be a positive change-driver in an organization; it creates a sense of urgency towards improving an organization's cybersecurity posture. Sometimes, regulations force executives to understand the importance of cybersecurity and represent an important first step from which to build on."

[3] https://www.centralbanking.com/fintech/cyber/4479511/cyber-attacks-on-financial-firms-rise-by-37-survey
[4] https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
[5] https://www.fblg-cpa.com/banking-library/it-and-security/2018-financial-industry-breach-analysis
[6] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
[7] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
[8]. https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf
[9] http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf
[10] https://www.fsb.org/wp-content/uploads/P131017-1.pdf
[11] http://image-src.bcg.com/Images/BCG-Radically-Simplifying-Regulatory-Compliance-in-Cybersecurity-Mar-2019_tcm9-217527.pdf

Compliance perspectives

Charlie also pointed out that regulatory compliance can negatively affect cybersecurity in some cases. He observed that recently, regulations are becoming too prescriptive, as opposed to descriptive. Descriptive regulations establish general requirements and security principles. Their language is generally easy to understand, although it needs continued interpretation. Conversely, prescriptive regulations state how to achieve cybersecurity in a detailed manner– what techniques or methods to use or where and how certain functions need to be performed. This approach is generally best used in guidelines or technical standards, but it may present some critical points. For example, depending on their level of detail, prescriptive regulations may present some risks. From a cybersecurity point of view, they can be ineffective as their inflexibility may limit the ways in which organizations may meet the evolving objectives of cybersecurity. Adhering to these rules may leave organizations exposed to cyber risks. Descriptive requirements, instead, enable organizations to fill the potential regulatory gaps around cybersecurity and improve cybersecurity posture to comply with or to go beyond what regulation requires, if so desired. Fig. 2 sums up these two approaches and shows how they influence compliance and cybersecurity.

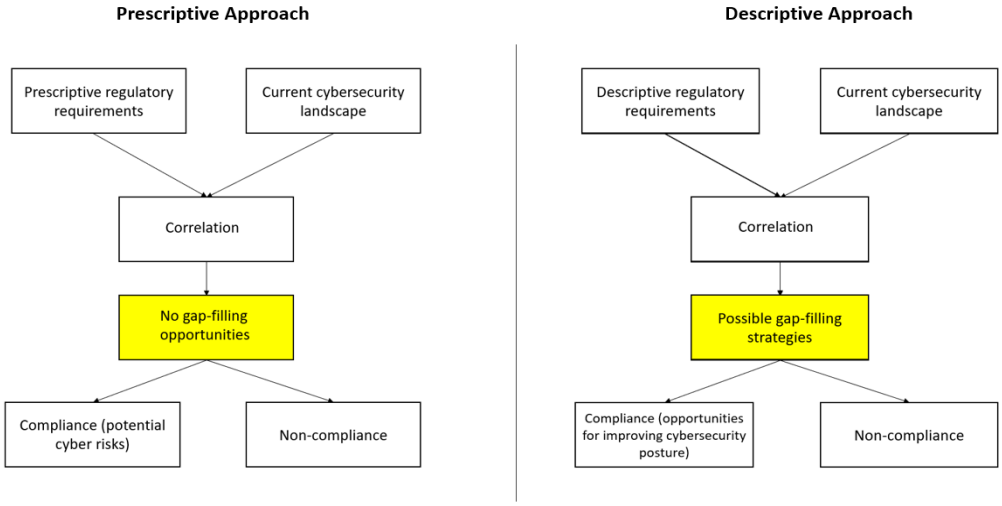


Figure 2. Descriptive and Prescriptive Approaches

Charlie explained,

"One of the problems with compliance is when regulations are too specific. A high level of specification is not always suitable for regulating the evolving cybersecurity landscape. If compliance doesn't provide organizations with opportunities to reach a higher maturity level, then it is only an overreaching task."

Compliance can often be very burdensome for some companies, especially when it requires organizations to dedicate resources, time, and energy towards compliance procedures instead of focusing on their actual cybersecurity needs. However, not all companies or industries have the same type of compliance. The size and type of company are an essential factor in determining compliance procedures. The financial service and energy sector, for example, are among the most regulated industries, and, therefore, the cost of non-compliance can be higher for companies operating in these areas. Additionally, larger companies tend to be more heavily regulated than much smaller companies, which contributes to increasing complexity and a significant number of possible compliance issues.

A Compliance harmonization Approach

BCG Platinion worked on a collaborative project to evaluate these issues and improve compliance in the financial sector. As part of this initiative, Nadya led a team of framework and standards experts to develop a harmonized cybersecurity regulatory framework (Financial Services Sector Cybersecurity Framework Profile – FSP or The Profile –). The main goal of this framework was helping organizations demonstrate compliance with multiple regulations while considerably reducing administrative burdens and associated compliance costs[12]. The primary reason that led Nadya and her team to diving into this project was the need for harmonizing overlapping regulations. As shown in Table. 1, implementing harmonization required significant effort in different regulatory areas.

Table 1: Harmonization Areas

Areas that require harmonization	
Categories	**Examples**
Language	Over 80% of the supervisory instructions contained in the NIST Framework, CPMI-IOSCO, and the ISO standards have a similar focus, but used different language[13]
Multiple regulators	Large global banks may work with 10, 20, or even more regulators around the world[14]
Culture	The UK has an outcome-based approach to compliance. India and Germany adopt a more detailed method

The first area that needed harmonization was language. Regulations are often thematically similar, but semantically different. Nadya commented,

"Different regulations use different vocabularies and jargon to indicate the same concepts and practices. Therefore, organizations are forced to demonstrate their compliance with each regulation and respond to multiple regulators. For example, the United States alone has 14 federal regulators for Financial Services. This complex environment may cause inefficiencies, including contradictory evidence for the same requirements."

According to Nadya, divergence has, therefore, become an increasingly important variable in planning compliance procedures. However, regulators are not the only causing divergence; there is also a cultural dimension involved. Depending on the state or area in which an organization is located, different factors may drive compliance. For example, some countries may tend to adopt a more detailed approach to compliance; others focus on the outcome. As a result, organizations have not only to comply with different requirements in the industry in which they operate, but they also need to adapt regulations to their own culture.

Thus, at a global level, most organizations don't have a unified way of efficiently dealing with cybersecurity and compliance. Instead, there is a patchwork of approaches, regulations, laws, and rules, which influence the outcome of many compliance programs. This lack of harmonization makes it challenging to keep pace with regulatory obligations, especially for multinational organizations that do business across different countries.

[12] https://fsscc.org/Financial-Sector-Cybersecurity-Profile
[13] https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf
[14] https://www.bcg.com/capabilities/technology-digital/simplifying-compliance-in-cybersecurity.aspx

In recent years, there have been several initiatives to facilitate a certain level of consistency in terms of best practices. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is considered one of the most comprehensive approaches to cyber-risk management and, therefore, a critical tool for international harmonization. For this reason, the NIST Framework, along with other standards, was one of the cornerstones around which the Profile was built.

Results

Creating harmonization is not an easy process. In addition to avoiding overreach, redundancy, and inconsistency, it is also necessary for regulators to work together and implement a transparent harmonization process. They need to identify common regulatory objectives and ensure that every organization achieves similar outcomes. Although a challenge, through coordination, coherence, and alignment, harmonization can be an essential tool to simplify compliance and help executives focus on strengthening cybersecurity.

CASE #3: A CULTURE OF COMPLIANCE: LESSONS FROM BIOPHARMACEUTICAL COMPANY

The combination of regulatory compliance and cybersecurity is proving to be a complicated issue for pharmaceutical organizations to overcome. The proliferation of healthcare data, usually stored in distributed data centers, and poor employee cyber hygiene have introduced new cybersecurity risks. The losses from a cyber-attack could be devastating for any pharma company. Consequences may lead to direct and indirect financial loss, ranging from stolen IP to disruption of production and supply chain shortages. In some cases, they can also compromise clinical trial data, and result in legal action related to the theft of sensitive information. Protecting patient data can be a challenge.

Due to the high liabilities associated with cybersecurity processes, organizations operating in this sector can't afford to accept the risk. For this reason, regulators started keeping a strict watch on the pharmaceutical organizations, which are experiencing a period of heightened regulatory scrutiny[15]. In addition to fines and penalties, any violation of regulatory requirements could affect an organization's reputation, causing damages to credibility and business operations. According to a survey[16] on reputation risk conducted by Deloitte, reputation problems have a severe impact on revenue, loss of brand value, and regulatory investigations. Avoiding compliance and cybersecurity breaches has evolved into a strategic task, impacting every business component, from corporate governance to risk management.

The approach

In the past, pharmaceutical organizations have traditionally managed compliance responsibilities by single teams or departments. This strategy worked for a while, but today, this approach is no longer a viable option. Founded around a decade ago, an American biopharmaceutical company headquartered in the Boston area, has grown significantly and, over the years, has implemented a strategy based on unconventional thinking to solve the challenges connected to cybersecurity compliance. The company covers a wide range of services, including developing medicines and therapies to treat disorders of the central nervous system. With the growing threat of hacking, the company couldn't ignore cybersecurity, especially because patient safety and product quality were highly dependent on their IT solutions. Responding to cybersecurity threats was difficult, but the biopharmaceutical company developed a strong focus on innovation and security, which placed it at an advantage in terms of creating a robust cybersecurity posture.

[15] https://www.pwc.com/il/en/pharmaceuticals/managing-regulatory-compliance.html
[16] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/NEWReputationRiskSurveyReport_25FEB.pdf

The Director of Data Compliance and Privacy, spent considerable time getting to understand her company, its people, and compliance activities. Her role involved looking at information and data governance across the company, including privacy regulations and laws in terms of technology, process, and awareness. With company growth, the Director had increasing concerns about data expansion and security of information. As their business models evolved, compliance risk became more interconnected and complex. This new environment created a unique challenge for the company because of the urgent need to develop a full understanding of compliance responsibilities.

However, the security function was an element that seemed to hinder compliance as employees perceived it as an overlap. The Director noted that compliance and security were part of the same organizational reality, but each of them required independent analysis and effort to be considered together and fill the potential gaps. She elaborated,

"I think compliance and security have to work hand in hand, support each other's scope of work, and partner together; they have to be a team; they don't have to be siloed."

The Director and her team realized that the best approach to managing compliance and security was building a culture of compliance, based information sharing, and collective value-derived principles. Embedding a compliant culture took more than assessing whether they complied with rules and regulations. The most difficult challenge was creating the main cornerstones of the culture and managing issues, such as changes in business focus, regulatory changes, and other developments pertinent to the company's operations.

As shown in Fig. 3, The team approached this task through communication, teamwork, engagement, and, finally, continued assessment.

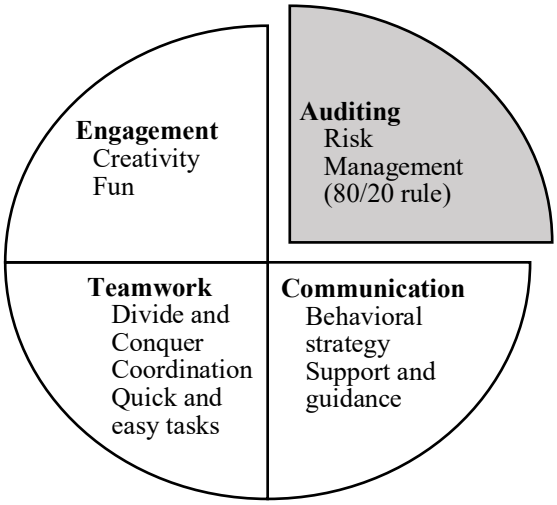


Figure 3. Compliance Culture

Communication

From a communications perspective, orientation training is typically the most common method that organizations use when they approach regulatory compliance. It starts when an employee is hired and continues with periodic training. In many cases, this approach may not be sufficient for driving change throughout the organization. One way to achieve effective communication at the biopharmaceutical company involved changing the way people behaved. This effort required a combination of behavioral strategy and support.

Communication was, therefore, added as one of the main pillars of the compliance culture due to the need that came up when employees started requiring specific guidance on cybersecurity compliance. The Director and her team took action to promote ongoing communication across all organizational levels. Employees were encouraged to proactively ask questions about regulatory requirements and make recommendations for improvements to compliance processes. In particular, talking about the negative and positive aspects of compliance and how to implement the regulations contributed to sensitizing employees to compliance procedures.

The key was to ensure that the entire workforce was on board with the company's compliance objectives. Regular communication about compliance initiatives and progress served to promote compliance as a key business strategy. The company was also successful in increasing knowledge transfer and integrating it with other risk management functions.

Teamwork: divide and conquer

Collaboration was a missing component in the complex compliance landscape that the company was navigating. One of the main problems was that teams were unclear on how to accomplish their task, thus resulting in misalignments and confusing outcomes. The Director found that achieving regulatory compliance required to break the work down into manageable activities and assign them to different people or teams. She then built her strategy around the idea of "Divide and Conquer." Having various people engaged in diverse compliance processes resulted in a successful practice that ensured a consistent and successful execution of the compliance process. For example, every time a new system came out, different teams were faced with varying tasks to ensure compliance. The infrastructure security team was one of the most active; it was in charge of the listing information technology assets, related accesses, operational responsibilities, types of data, etc. Additionally, keeping this list up to date was, in itself, a teamwork effort. The Director explained,

"Compliance means being able to provide defensible documentation, whether it's training records, whether it's showing due diligence on evaluating systems and technology, whether it's showing that you're working on being compliant with regulations. However, building a culture that embraces this mentality is not an overnight process. It must start with the steering committee, core teams, and leadership teams. Everyone must do their job in meeting requirements, supervising, mentoring, etc. People are the biggest hurdle to overcome in compliance, but also the most critical contributor to compliance effectiveness. They need to know what to do with their information and be able to demonstrate that when they are audited"

According to the interviewer, compliance is a chain-management process, which is successful only if there is synergy among the parts involved. She explained,

"Nowadays, the 'rule of thumb' for compliance is that everyone needs to ensure that their work doesn't slow anybody down. The lack of coordination may cause a pushback situation where a company is not able to be successful in implementing compliance. For example, if teams need to work on difficult or labor-intensive tasks, then their attention spans are likely to become extremely short, and they may not be able to get their work done correctly."

Engagement

There is a widespread assumption that forcing employees to follow the rules and regulations is the way to go to ensure compliance. Most organizational efforts around compliance focus on defending against sanctions and legal penalties rather than addressing what is effectively the real issue behind the regulation.

However, while implementing mandatory processes and oversight structures is essential, it is only a part of the whole compliance strategy and may not be suitable for all organizational environments. Not only could an organization be more exposed to breaches of compliance (and security), but they could also be subject to significant reputational damages than those that can demonstrate they have made efforts to promote engagement. Thus, the Director believed that a framework of feedback, review, and employee engagement could be fundamental to sustain the company's compliance culture. To achieve this goal, the company started moving away from narrow-focused methods. For example, they implemented creative ways to engage employees, such as rewarding good behaviors, interactively presenting new policies, offering fun training and giveaways, etc. the interviewer commented,

"Fun is the biggest goal. Of course, you can't take cybersecurity compliance non-seriously because your organization's survival depends on it, but I think making it fun is something positive for achieving good results in both compliance and cybersecurity. If employees have fun, they are more invested in what they do, reducing the risk of failure."

Auditing compliance

Engagement, communication, and teamwork are only successful if employees know that their actions are integral to the company's success. For this reason, an organization must measure the effectiveness of their compliance efforts. The Director shared her perspective on compliance measurement.

"Measuring compliance is generally more reactive than proactive. Companies don't spend enough time defining what success is when it comes to compliance, and often they don't identify appropriate metrics until there's been a disaster. This generally happens because measuring a culture of compliance is incredibly hard, mainly because there are different perspectives of compliance. For example, there may be contrasting interpretations regarding how long you need to keep records and data points. From a business perspective, you need to keep the information for a certain amount of years, but from a regulatory perspective, you need to keep it for a different amount of years. It is in situations like this that it is necessary to evaluate your organizational risk tolerance and pose questions, such as 'Are we a risk-taking organization?', 'Are we willing to pay fines.?"

Although it is impossible to eliminate risk, according to the interviewer, one way to overcome this issue is to apply the "80/20 rule," which provides some guidance on how to tackle most of the risk-related compliance challenges. In other words, she observed that, when assessing compliance, not all risks carry the same consequence. However, by applying the 80/20 rule to compliance risk management, an organization can select the main risks that pose the highest potential for damage and focus most of the efforts on those. This method enables organizations to better allocate their time and resources to the most impactful areas.

Conclusion

As regulatory changes continue to impact compliance procedures, the pharmaceutical sector must evolve to stay competitive and ensure fast implementation of compliance processes. The Director and her team are considering different ways to develop their approach to building their culture. They aim to ensure that their compliance values align with clear and consistent communication, common and understood goals, and measures to mitigate cybersecurity risks.

CASE #4: AN OVERVIEW OF COMPLIANCE IN THE ELECTRIC UTILITY SECTOR

Background

In the United States, there are 3100 electric utilities. According to the U.S. Energy Information Administration (EIA), utilities can be classified into three ownership types: publicly owned utilities (often called municipal utilities or "munis."), cooperatives ("co-ops"), and investor-owned utilities (IOUs)[17]. About 100 IOUs supply 75% of the electric power in the US. IOUs are regulated by state agencies. The federal government regulates the interstate transmission of electricity.

About 2000 companies of the 3100 are publicly owned utilities (POUs, also called munis) run by state or local government agencies. Most of them are distribution and customer-service utilities (they buy power at wholesale from generation companies) owned by municipalities[18]. For example, the Los Angeles Department of Water and Power (LADWP) is the largest municipal utility. The Sacramento Municipal Utility District (SMUD) in Sacramento, California is well-known for innovative programs. Municipal utilities are not subject to state regulation. However, they are controlled directly by city governments.

Additionally, cooperatives or co-ops (also known as electric membership corporations) are owned by the rate-payers. Cooperatives were created to promote the development of rural electrification[19]. Nearly 1000 cooperative utilities were established starting in 1937 during the Great Depression under an act of the US Congress, called the Rural Electrification Act (REA). This act, passed in the administration of Franklin Roosevelt, provided electricity to rural areas through cooperatives at a time when only 10% of rural Americans had access to electricity.

Finally, the remaining 100 utilities are investor-owned utilities, or IOUs, which are large electric companies that issue stock owned by shareholders. Examples of popular brand names include Consolidated Edison of New York, Inc., (ConEd), Eversource, which serves Boston and other areas, National Grid, which serves Cambridge and other parts of the state, Pacific Gas and Electric Company (PG&E) (northern California), Southern Company (Georgia and some nearby states), Commonwealth Edison (Illinois), Florida Power & Light Company (FPL), etc[20]. As regulated utilities, these companies are required to comply with state and federal regulations[21].

Overview of investor-owned utilities

At the turn of the 20th century, there were attempts to set up private utility companies, but most of them failed because they were too small, and they grew too fast[22]. Therefore, municipals were taking over electric companies that failed. In this context, the munis were the leading players around 1920 as the economy started improving after World War One. However, it was during these years that industry leaders like Samuel Insull saw investment opportunities in power systems and began to shape fundamental economic concepts, which still govern the modern utility environment[23]. Insull proposed that the states regulate investor-owned utilities. In exchange, investor-owned utilities would be given a monopoly in regions of the

[17] https://www.eia.gov/todayinenergy/detail.php?id=40913
[18] United States Congress, Senate Select Committee on Intelligence, Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System and for Other Purposes: Report (to Accompany S. 2507), (Vol. 106, No. 279), US Government Printing Office, 2000.
[19] Willis, H. L., & Philipson, L., Understanding electric utilities and de-regulation (Vol. 27). CRC Press, 2018.
[20] https://content.next.westlaw.com/8-525-5799?isplcus=true&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1
[21] Brown, R. E., Business essentials for utility engineers, CRC press, 2017.
[22] http://sites.utexas.edu/energyinstitute/files/2016/09/UTAustin_FCe_History_2016.pdf
[23] Zimmerer, K. S. (Ed.), The new geographies of energy: Assessment and analysis of critical landscapes. Routledge, 2013.

country, and the regulators would be allowed to control the profits that investor-owned utilities made. Following this critical change, the electric power industry grew very fast between the 1920s and the 1980s. Most of this growth derived from the fact that investor-owned utilities set up a regime through the regulators where they were guaranteed a return on assets (typically 12 to 14% profit on their assets). This process was regulated on a state by state basis; every state in the United States set up a regulatory commission (e.g., the Department of Public Utilities) to monitor these activities[24].

Electric utility challenges

The electric utility industry has changed very little since the early days when AC (alternating current) and DC (direct current) power distribution were developed by George Westinghouse and Thomas Edison respectively. In this century the electric power industry has started to investigate smart grids to overlay the electric grid with a communications network. The intent is to provide improved grid monitoring, especially important with the introduction of power generated by customer-installed solar, wind, and storage technology (called DER: Distributed Energy Resources). The integration of new technology into the electric system is creating new opportunities for utilities, eventually enabling the collection of massive volumes of data and better performance[25]. However, although the increased efficiency and proliferation of DER are bringing substantial advantages, the impact of the technology on the electric power field is making the utility system more complex[26].

According to industry insider Dr. Kenneth Wacks (www.kenwacks.com), a utility system consists of a "tree" structure that includes generators, transmission lines (typically on steel towers), distribution lines (typically on telephone poles), and meters serving customers. It was originally designed with the capacity to generate more power than customers needed so customers would be encouraged to buy more electricity-consuming equipment. Dr. Wacks argues that one of the main problems affecting this system is running "open loop" meaning the system operator is not able to monitor or measure the condition of the output. Therefore, the accuracy or success of the system in delivering power depends on the user experience[27]. He explained,

"Simply put, if your lights go out, there's a very good likelihood the utility has no idea that it happened. What they do is they wait for customers to call and complain. If you and a bunch of neighbors call, the utility figures out that there is a problem in that part of the town, and they'll go check out what's wrong."

One solution to address this issue is integrating more automatic control or feedback features to monitor the process and maintain the desired output level. The installation of sensors and communication networks for smart grid applications provides opportunities for the utilities to have a much better handle on the network's operation. A smart grid also helps the utility industry deal with recent developments where customers are starting to generate their own power with solar panels and wind turbines. In some jurisdictions, these customers are allowed to sell the excess power back to the utility. According to Dr. Wacks, one of the smart grid goals involves a futuristic scenario called Transactive Energy, where customers are allowed to sell their excess locally generated power to their neighbors. Ken elaborated,

"If there is a cluster of factories and they have flat roofs equipped with solar panels, one factory that may not need as much power could sell their excess solar power to a neighboring factory."

Most regulators have started to realize that major shifts are occurring in the electric industry, and some have already taken significant action[28].

[24] Shah, B. J., McCann, C. M., Odom, J. S., & Richardson, T. P., Restructuring the Electrical Industry, 2007.
[25] https://energy.mit.edu/wp-content/uploads/2016/06/MITEI_WP_2013-01.pdf
[26] Weron, R., Modeling and forecasting electricity loads and prices: A statistical approach (Vol. 403), John Wiley & Sons, 2007.
[27] Siemens, Electrical Engineering Handbook. New Age International, 1998.
[28] http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf

Ken Wacks' experience: Interviews with regulators

About ten years ago, Ken was chosen to be one of the 13 experts working with the Department of Energy on a project called the GridWise® Architecture Council. He was invited into this initiative because of his knowledge of the customer interface to the grid. As part of his work with the GridWise Architecture Council, Ken interviewed companies and regulators from several states. During these conversations and through his consulting work with many utilities, he gained an understanding of the main challenges surrounding compliance in this field.

1. ***Poor regulatory oversight***. Pacific Gas and Electric Company (PG&E) is an energy-based holding company based in San Francisco, California[29]. About ten years ago, the company had major gas explosions on its high-pressure gas lines near San Francisco.[30]Among the main causes of the pipeline rupture was bad management by the state and federal regulators who did not notice the problem[31]. For example, investigations revealed that there were several defective welds in the pipeline, which probably weakened over time until their complete failure. PG&E, the utility that installed the pipes, had started a pipeline replacement work to reduce the probability of the pipeline to fail. However, the replacement procedure was unexpectedly stopped. An independent audit conducted by the California Public Utilities Commission revealed that PG&E allegedly diverted more than $100 million from a fund intended for gas safety and operations and spent it for other purposes[32]. By cutting back on projects related to pipeline-replacement and maintenance, the company failed to prioritize safety during the three years before the incident. Not only does this incident showed that pipeline safety was underestimated, but it also indicated the lack of adequate regulatory inspections.
2. ***Poor regulatory planning.*** In 2010 Ken attended a presentation by the PG&E president, who addressed a conference of state regulators about the installation of "smart meters." The US federal government had provided $4.5 billion in 2008 to the electric utility industry as part of a stimulus bill following a severe recession. Many utilities used these funds to replace analog meters with digital electric meters claiming more accurate billing and lower servicing costs, plus benefits for yet-to-be specified customer-service programs. PG&E quickly installed millions of meters. Customers started complaining about higher bills. Some meters were defective, but 2010 was also a hot summer, so consumption was higher. The PG&E president admitted his timing was bad, his meter testing was faulty, and his public relations were poor. He made no reference to oversight by the California Public Utilities Commission, which received thousands of complaints. In May 2010, CNET reported an explanation from Helen Burt, PG&E senior vice president and chief customer officer, "We've let some of our customers down with the quality of customer service they received. While 99 percent of our SmartMeter devices are installed and working properly, we recognize that even having less than 1 percent of meters with issues is still 50,000 customers, and that's too many."[33] The president of PG&E was fired within a year.
3. ***Need for regulatory modernization and flexibility.*** In some circumstances, the evolution of utility organizations can be limited by the difficulty of implementing a proactive and adaptable regulatory approach. The state of Hawaii's utility regulators, for example, are faced with significant challenges due to the high demand for solar and wind power, which changes dramatically depending on the time of the day. According to Ken, the fundamental problem with a lot of people generating solar is explained as follows:

[29] The California Public Utilities Commission (CPUC) in San Francisco has a staff of full-time engineers who advise the regulators. In addition, there is a separate state agency in California called the California Energy Commission, which provides strategic planning for the state of California. Southern California Edison, Pacific Gas & Electric, San Diego Gas & Electric, and Pacific Power are the regulated, investor-owned utilities (IOUs) in California.

[30] https://www.nbcbayarea.com/news/local/pge-investigating-complaints-of-gas-smell-in-san-bruno/1852300/

[31] https://www.nytimes.com/2011/08/31/science/earth/31pipeline.html

[32] https://www.sfgate.com/bayarea/article/PG-E-diverted-safety-money-for-profit-bonuses-2500175.php

[33] https://www.cnet.com/news/pg-e-admits-to-flaws-in-some-smart-meters

"The demand for utility power goes way down on a sunny afternoon because solar panels are generating power, and suddenly spikes way up as the sun sets because, in combination with the sun setting thus stopping solar-power generation, people are arriving home and starting energy-consuming appliances such as air conditioners, cooktops, ovens, consumer electronics, and lighting. Additionally, if they have electric cars, they plug in their vehicles to recharge the batteries."

The term used to describe this phenomenon is the "duck curve[34]," often represented through a graph highlighting the effect of the imbalance between demand and energy production throughout the day. With the increasing use of solar panels and electric vehicles, the control and protection of the power distribution grid need to be managed not only during normal conditions, but also under other difficult situations that may range from demand intermittency issues to cyber-attacks. In this context, utility regulations are essential for determining rules that govern the management of utility operations. However, the biggest challenge is that the existing regulatory structure driving traditional utility business models has not kept pace with new technologies. Furthermore, many utility managers have not developed the appropriate skill sets to prevent the related threats[35].

4. ***Misaligned expectations.*** Another issue is that there is a discrepancy between what the utilities expect and what they are obtaining from the regulators. Utilities and their regulators are aware that they need to work together to address investment challenges and protect utility revenue streams. However, because their approaches and visions differ, establishing clear ways to collaborate is not an easy task. There are several gaps in the perception between regulators and utilities. For example, although both may see potential benefits from new technologies such as solar energy, their perspectives differ on practical applications of these technologies. Some regulators are under political pressure to encourage green technologies such as solar. Not all utilities are prepared to accommodate solar, especially solar power generated by customers. The utility loses business during the day followed by a sudden increase in demand in the evening. Furthermore, some regulators mandate that utilities purchase excess solar power generated by customers during the day. These types of divisions between utility business goals and public goals as expressed by politicians generally complicate the adoption of innovative solutions. Ken elaborated,

   "The ultimate defense for utilities is to go to the state legislature and lobby for legislation to overrule the regulators. This procedure has been applied in many states across the U.S. The result is regulators are over-ruled or some more cautious regulators accede to utility demands. Attempts to encourage customer-generated solar energy, for example, have been stymied in three major states: Nevada, Arizona, and Florida, despite the great potential for solar energy in these sunny states. The result is a confusion of who is regulating whom."

5. ***Political appointment challenges.*** A final concern is the dynamics of the structure in which regulators operate. In the U.S., the majority of utility regulations are established at the state level through regulatory bodies led by commissioners[36]. Commissioners are either political appointees of the state governor or directly elected by voters[37]. According to Dr. Wacks, as political appointees, most commissioners have to deal with a set of challenges associated with the nature of the political system in which they operate.
   a. ***Background.*** One of the criticisms that are increasingly directed against regulatory agencies is that their commissioners' competencies are not comprehensive enough to operate in the real-world utility environment. Being political appointees, the majority of commissioners have a law or public service background[38]. While possessing skills in these

[34] Named after a chart published by the California Independent System Operator (CAISO) in 2013 resembling the profile of the back and neck of a duck
[35] https://www.nga.org/wp-content/uploads/2018/08/Energy-Innovation-Roadmap-August-2018.pdf
[36] http://econ.lse.ac.uk/staff/tbesley/papers/regpap_prev.pdf
[37] Brown, R. E., *Business essentials for utility engineers*, CRC press, 2017.
[38] Gormley Jr, W. T., *The politics of public utility regulation*. University of Pittsburgh Press, 1983.

fields helps make decisions that are consistent with existing public utility law, some often lack engineering expertise to understand the technical details of how the power grid works. For these reasons, although many commissions have taken steps to improve their training policies, it remains difficult for regulators to develop appropriate technical skills. Therefore, they are highly dependent on consultants and the commission staff.

b. ***High turnover.*** Regulatory bodies are inherently subject to high turnover. For example, it is not unusual to have new regulators appointed when a new governor takes office. Moreover, many regulators realize that there are several business opportunities outside their operating area and may decide to work for the industries that they previously regulated or related private companies.

Conclusion

The compliance requirements within the electric sector are going through a considerable evolution process. Ken added,

"Regulators not only have to do the traditional business of monitoring whether utilities are spending rate-payer (customer) money wisely, but they also have to deal with all the technical and security issues involving solar, wind, and battery storage., Furthermore, we have electric vehicles coming into the mix. Because of the need to ensure effective compliance implementations, as well as the security of these services, regulators are now challenged to stay at the forefront of compliance and security developments. So the question is, how prepared are the regulators to understand and handle all these issues? The answer is generally not well. There are just a few states that are known for having enlightened regulations."

According to Dr. Wacks, one of the key points of departure for regulators is to create an arm's length distance between them and the utilities. He added,

"Regulators need a more organized approach to understanding utilities' challenges in order to create and adjust policies in ways that eliminate the existing barriers. They would benefit from more knowledge, institutional memory, and experts to advise them so that they can ask the right questions."

The imperative for a more attentive consideration of the utilities' needs is particularly important for critical infrastructure, given the potential for both physical and cyber damages. Cybersecurity is a recent concern for the electric utility sector, primarily because the utilities were not connected to public networks like the Internet. Today, addressing cyber threats is a fundamental dilemma in moving towards smart grids. It has only been in the past few years that utilities have found it convenient to put their substations on the Internet so that they can control them remotely. However, as networks become smarter, they also become more vulnerable to cyber-attacks.

Regulators are starting to become more aware of the potential risks associated with vulnerable IT systems in the utility sector. For example, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are currently one of the primary set of specifications with which electric utilities must comply for operational cybersecurity[39]. NERC designed a set of security rules with the purpose of keeping the U.S. power system safe from physical and cyber-attacks[40]. Recently, some of the largest utilities have been fined by federal regulators for violating NERC CIP rules. Among these, Duke Energy, a utility-based North Carolina, was fined $10 million by the NERC for severe and pervasive violations of security rules[41]. These violations ranged from a lack of implementation and management to accountability issues relating to the CIP compliance program.

[39] http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf
[40] https://www.ispartnersllc.com/blog/nerc-cip-standards-overview/
[41] https://www.utilitydive.com/news/duke-fined-10m-for-cybersecurity-lapses-since-2015/547528/

However, the increase in the NERC CIP rule violations has shown that the regulatory framework requires some improvements to prevent cyber-attacks[42]. While potential solutions exist to some of the most common issues, the challenge is designing an architecture that ensures cyber and physical resilience, which will likely be indistinguishable in the near future. According to Ken, encouraging private-public partnerships between industry and the government is essential to achieve this goal[43]. For example, the Smart Electric Power Alliance (SEPA), a trade association of which Dr. Wacks is a member, has a technical committee that includes government scientists exploring cybersecurity issues in the utility sector. More specifically, Ken has been part of a subcommittee examining cybersecurity issues with a particular focus on cybersecurity resiliency, the ability to recover quickly and effectively from a cyber-attack.

Ken shared his thoughts on the topic,

"I am not convinced that connecting utilities to the Internet is the best way to run a system. As we saw in the cyber-attacks on the Ukrainian power grid[44], if you put a system on the grid and you don't understand cybersecurity, or even if you understand it but miss something along the way, a cyber incident can be devastating."

Having a secure energy system is essential to modern societies. Not only are gas and electricity needed for any daily activities, but they also enable other services to function, such as telecommunications, defense, transport, healthcare, etc. Regulatory frameworks must, therefore, be adapted to align better the incentives with the challenges utilities are facing. Regulators should be creating adequate incentives for long-term innovation and security.

CASE #5: UNDERSTANDING THE COMPLIANCE FORCES THAT INFLUENCE CYBERSECURITY IN THE BANKING SECTOR, ESPECIALLY IN THE UK

Developing resilience to cyber risk has emerged as one of the primary investment priorities for financial organizations in the United Kingdom[45]. However, in practice, extensive work is necessary for both regulators and regulated entities. One of the reasons for this is that the Financial Conduct Authority (FCA), the financial regulatory body in the U.K.[4647], has seen a significant increase in cyber-attacks reported by organizations over the last few years.

According to a survey conducted by data security firm Clearswift[48] in 2019, 70% of U.K. financial companies suffered a cybersecurity incident over the last year. The study also highlighted that nearly half (43%) of security incidents within the financial sector had been caused by employee failure to follow data protection requirements. According to a cybersecurity subject matter expert (SME) expert who worked for multiple global banks in the U.K., protecting systems from cyber-attacks while keeping up to date with developing regulations and procedures is a complex challenge for banks operating in this country. Over the past decade, the primary responsibilities of the SME involved overseeing how major banks complied with cybersecurity-related regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) [49], Sarbanes-Oxley Act (SOX)[50], etc. During their time working in the field of banking, the SME had to deal

[42] https://www.utilitydive.com/news/us-power-sector-recognizes-cyber-risks-but-violations-show-enforcement-iss/552558/
[43] https://sepapower.org/knowledge/wanted-an-integrated-approach-to-cybersecurity-and-physical-resiliency/
[44] The Ukrainian grid suffered major blackouts as a result of cyber-attacks in 2015 and 2016, attributed to Russian state-sponsored groups.
[45] https://www.ey.com/en_gl/banking-capital-markets/why-banks-must-view-operational-resilience-as-a-strategic-imperative
[46] The FCA is the conduct regulator for the banking sector in the U.K. and works closely with the Prudential Regulation Authority (PRA), which is the principal regulator of bank. Both the FCA and the PRA and the FCA have disciplinary and enforcement powers.
[47] https://www.lexology.com/library/detail.aspx?g=4e55a6bc-5f01-4abd-b242-d6e0bdf3f405
[48] https://www.clearswift.com/about-us/pr/press-releases/70-percent-companies-suffered-cyber-security-incident-in-last-12-months
[49] The Payment Card Industry Security Standard addresses card issues and ensures safe storage, processing, and transmission of data. Even though the PCI DSS originated in the US, it has global implications as the card providers operate in many different countries.
[50] The Sarbanes Oxley Act, which was introduced in the U.S. in 2002, has far-reaching implications on any business with a U.S. listing, including companies in the U.K. In particular, the banks mentioned in the case study have a presence in the United States, which makes them fall under SOX. For example, they have operations in New York and most of their infrastructure is held here.

with several situations in which compliance and cybersecurity were not aligned. The following factors contributed to this misalignment.

The cost of compliance

Cybersecurity compliance generally helps an organization protect its assets. However, in some cases, being compliant with an industry-specific set of standards can be costly. Consequently, it may lead to having an ineffective information security posture. For example, being compliant with PCI DSS means making investments in specific security activity; particularly with how data is stored and encrypted[51]. To exemplify this issue, the SME shared a story about a challenging situation involving compliance with the PCI DSS standard,

"To ensure the financial services organization was as compliant as possible, we had a robust compliance function in place where any regulatory requests were analyzed and subsequently sent to the respective teams. Additionally, all related compliance reports were presented to the board on a monthly basis. However, one of these reports once stated that certain security controls (e.g., those related to cardholder data stored) were reported as "red[52]," meaning "not compliant" with PCI DSS. Eventually, after a review, it was decided that it would have costed more money to improve compliance with these security requirements than it would have if we had to leave it as it was. We then decided to accept that risk."

Achieving or maintaining compliance is often handled as a business decision where the cost of implementing compliance controls is assessed against the cost of not complying. However, it is not often easy to balance the business interests of a company and specific compliance requirements. In some cases, this conflicting situation represents a sore point for many financial organizations and may affect the overall cybersecurity strategy.

Bank stability

Regulators are increasingly concerned about the overall stability situation. For example, in the wake of COVID-19, the Bank of England (BoE), which is the U.K. regulator responsible for financial stability, demanded that banks suspend their dividends to provide the bank stability to the crisis. However, the mandated dividend cut came with substantial consequences. On the one hand, it served as a way to stabilize the sector; one the other hand, it probably weakened independent organizations. The SME shared his thoughts,

"Generally speaking, the role of a bank is to generate profit. Some of that profit is paid out to shareholders for dividends, some of it is invested in infrastructure and operations as well as cybersecurity. Investors buy shares, and that adds value to the bank. However, when a global pandemic comes along, to ensure the resiliency of banks, regulators may force banks to keep their money. However, while this helps maintain capital adequacy, it also means that banks have less opening capital and less money to invest in their IT security posture."

If a bank cannot invest in cybersecurity, internal cybersecurity budgets could be cut - arguably making the organization less secure. A potential attack or incident could have many consequences, which, in turn, can affect the overall stability of the bank and its stakeholders as well as posing a broader risk to the balance of the financial system.

[51] https://blog.rsisecurity.com/cyber-regulations-for-banking-in-europe-vs-america/
[52] In the dashboard that the cybersecurity expert used to show to the executives, compliance analyses were represented through a chart displayed in a Red, Amber, Green (RAG) format, showing which controls needed remedial action (red) and which were at risk but were being monitored (amber) or which were progressing as planned (green).

Geographical influences

The banking regulatory environment is particularly complex in Europe (and in the U.K. to some extent[53][54]) due to the high level of interdependencies among the Member States. This situation introduces a high systemic risk. Consequently, cyber threats are not restricted by national borders, and, in some cases, their spread cannot be easily controlled by national regulations and laws. To address this issue and harmonize the regulatory environment, EU regulators introduced broad-reaching regulations, which, however, resulted in a double edge sword outcome. On the one hand, they created uniformity among practices and updated the existing national legislation; on the other hand, they increased bureaucracy, liability issues, and compliance work for banks significantly. The SME commented on this issue,

"Due to the introduction of regulations at the international level, financial organizations are adapting to comply with security requirements and administer security policies. However, many of them are struggling to understand the scope of their obligations. For example, new requirements relating to European data privacy and protection regulations are extra-territorial in scope. The General Data Protection Regulation (GDPR) broadly applies to European businesses and organizations in the same way as extra-EU organizations, with some exceptions[55]. The geographic location dictates what regulations and compliance the organization must adhere to; failing to understand the scope and implications of what is required may lead to significant consequences in terms of liability and data exposure."

Another example of multi-scope legislation is the Network and Information Security (NIS) Directive [56][57]that establishes security and notification requirements for Operators of Essential Services (OoES), including banking organizations. Many firms are often unprepared for these new requirements, and those embarking on a "compliance path" to meet these regulatory challenges are called to face difficult choices about priorities and investments. For example, being in scope doesn't necessarily mean the directive applies to the entire organization – only those organizational units that provide critical services may be involved in the compliance process; it may be necessary to identify essential areas and prioritize investments to optimize and balance cyber risk protection.

Conclusion

Regulatory activity in the banking sector is set to grow in the next few years. During this period, regulators in the U.K. and Europe have expressed their intention to establish new regulatory practices. Some early signs show that regulators are looking at ways to make cyber risk monitoring a routine process. Some agencies have provided cybersecurity guidelines, including the International Chamber of Commerce, the UK's Department of Business, Innovation & Skills, the British Cabinet Office[58]. Additionally, the BoE has also outlined a set of guidelines on cybersecurity-related topics, introducing the CBEST framework[59], which is one of the primary methods for British financial organizations to identify vulnerabilities and test their protection measures using advanced intelligence and attack simulations.

[53] Now that the UK is no longer in the EU and is in a transition period until 31 December 2020, there is some confusion over whether banks need to operate differently to ensure compliance with data protection legislation
[54] https://www.theukdomain.uk/gdpr-after-brexit/
[55] Similar to GDPR, if an organization is located in a non-EU country but provides essential services in the EU, it will still be subject to the NIS Directive
[56] On 10 May 2018, the NIS Directive was enacted in UK law as The Network and Information Systems Regulations 2018 (also known as "NIS Regulations")
[57] http://www.legislation.gov.uk/uksi/2018/506/made
[58] https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice
[59] https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

However, as these initiatives are being further shaped and developed, several issues are likely to emerge. For example, regulatory opinions differ on the need to regulate cyber-risk specifically[60]. One view is that the evolving nature of cyber-risk does not require specific regulations because cybersecurity risk is considered as any other risk. Consequently, according to this view, cybersecurity issues can be managed with existing risk-related laws, and it is more important to focus on them rather than build new ones. Conversely, the other perspective is that it is necessary to provide a specific regulatory structure to handle cyber-risk to cope with its particularities properly.

Existing cybersecurity-focused regulations both in the EU and in the UK are relatively recent and, therefore, are not well-developed enough to deal with the unique threats resulting from an increasingly connected financial sector. This difference could translate into practical issues, such as confusion and limited coherence in terms of compliance procedures, especially following the coronavirus pandemic. The recent crisis has prompted multiple financial organizations to take measures in the financial industry to avoid future economic disasters. According to the cybersecurity and privacy professional, the best practice, although not yet commonly adopted in the banking sector, is for banks themselves not to simply follow the rules but to understand processes and identify where strengths and weaknesses exist in relation to a cost-benefit analysis. Efforts will have to be made by banks in developing a compliance system that can measure compliance effectively to encourage strategic decision-making and investments associated with their cyber risk appetite.

CASE #6: BREAKING THE VICIOUS CIRCLE BETWEEN COMPLIANCE AND CYBERSECURITY, ESPECIALLY IN THE UTILITIES INDUSTRIES

Since the probability of a cyberattack is generally very high, the question for companies operating in the utility sector becomes not whether an organization will be affected, but how? Answering this question requires moving beyond a technical assessment of cybersecurity practices. The technical challenges are indeed a reality, but it is also necessary to consider broader views on cybersecurity issues. Even though the immediate consequences of having cyber attackers compromise a utility's operations may be obvious, the potential long-term effects of a successful breach may be subtle. For example, there may be potential impacts on a company's reputation, even if a cyber-attack was not completely successful or had a low impact. If, for example, a company's website gets hacked, its reputation for cybersecurity might be significantly hit. Customers might tend to believe their security is poorly run even though critical systems have not been compromised, resulting in negative publicity. One of the tools to keep the extent of these long-term effects relatively limited is regulatory compliance; it can help companies save time and effort in damage control of their reputation in terms of cybersecurity. However, while demonstrating to be compliant can be an effective method to ensure or restore reputation, the way compliance is actually achieved in practice is not enough to eliminate the root cause of cybersecurity issues. Chris Humphreys, CEO and founder of The Anfield Group[61], an Austin TX-based Cybersecurity and Regulatory Compliance Consulting firm, is an advocate in promoting awareness around this issue. He commented,

"Utilities are under a constant scare of cyber-attacks, not only because they can cause significant damages to their infrastructure, but also because they fear being exposed in the media as being vulnerable. Media are often the first to know about a cyber-attack or issue and the first to pronounce on it. By the time a senator or a representative in Congress or the Senate or any other politician is talking on the news about a cybersecurity issue, it's way too late. For example, there was a big ransomware attack here in Texas that affected several Texas State agencies and utilities. By the time authorities learned about the incident, the local news had already been informed. Today, everybody is a reporter, and there are no reference checks beforehand, which is the way reporting was done years ago before the Internet. The media have a

[60] https://www.bis.org/fsi/publ/insights2.pdf
[61] https://theanfieldgroup.com

dangerous impact on communications around cybersecurity; they have the power to turn a small incident into a disaster for a company's good name. Consequently, one of the biggest mistakes that electric utilities make is to achieve compliance with standards out of fear of facing reputational risk[62]."

According to Chris, fear is often the main driver behind regulation enforcement and the primary route by which companies are exposed to a vicious circle where the adverse effects of compliance cause other issues in a series of loops.

The vicious circle

In 2018, Chris provided testimony to the House Committee on Cybersecurity, where he expressed the struggles around compliance that he has witnessed in the electric utility sector. 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, Chris found himself in a privileged position to observe the compliance process from a regulator and company perspective. In particular, he noted that compliance is often trapped in a bureaucratic circle (Figure 4) where actual cybersecurity is, unfortunately, the least of concerns.

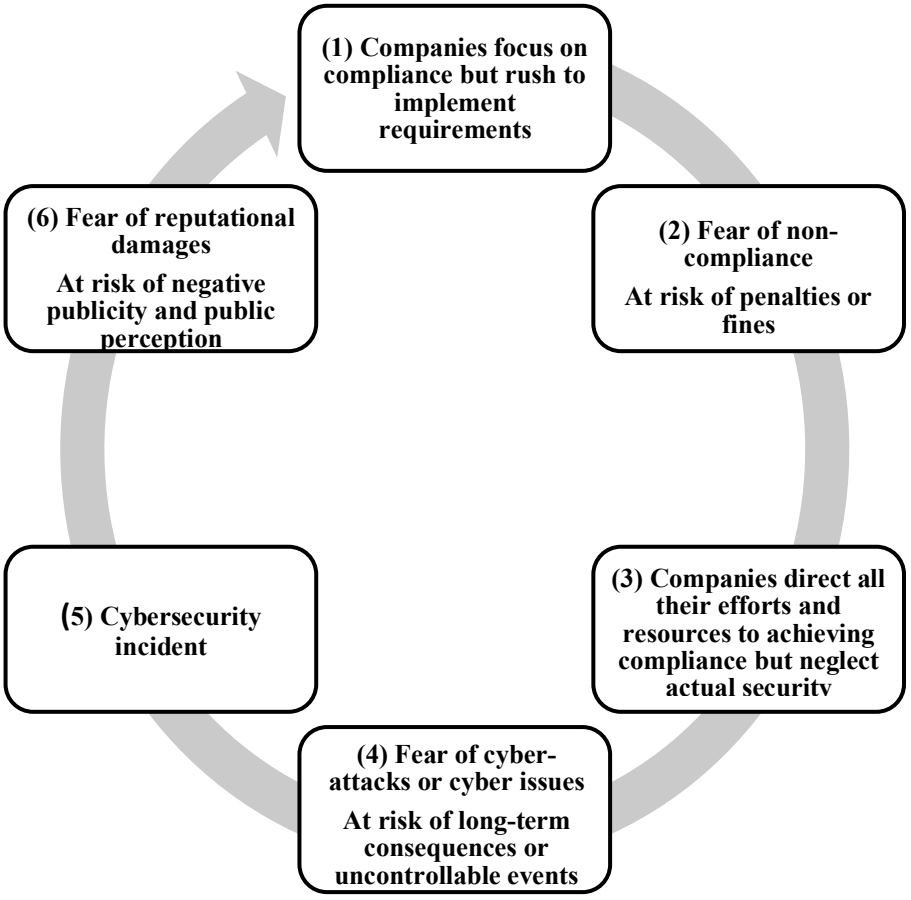


Figure 4. The Vicious Circle

This circle starts at step (1), at the top of the circle, with companies rushing to be compliant to avoid reputational damages. However, complying with a patchwork of compliance rules is burdensome, which results in companies being under pressure, and therefore, focusing solely on passing audits (2). This attitude

[62] Reputational risk occurs when a loss causes reputational damage

is generally caused by a punitive compliance model established by regulators[63]. Although the imposition of financial penalties for regulatory violations is a mechanism to ensure compliance, it may lead companies to directing their efforts to avoid fines, instead of reflecting on the real meaning of compliance (3). For example, based on his experience as a regulator[64], Chris noted that the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) was the first regulatory framework that was put in place that carried the highest punitive penalty of any regulatory framework in North America[65]. According to Mr. Humphreys, punishing non-compliance through the use of strict sanctions is counterproductive and prevents companies from being proactive in addressing cybersecurity risks. He also pointed out that regulatory compliance moves far too slowly to keep pace with cybersecurity threats. Chris explained,

"Our regulatory model is continually behind in terms of security. The standards are developed so slowly that, in many cases, by the time they are in place, what you were trying to mitigate has far since evolved into a new issue or is no longer an issue. This regulatory approach dictates security to critical industries. It creates a false sense of security, which ends up with regulators placing responsibility on utilities for not implementing the appropriate controls and being vulnerable."

This means that many organizations are often forced to give up on cybersecurity to prevent any issues associated with compliance penalties. Consequently, budgeting and resourcing to address cybersecurity become a problematic task for utilities, resulting in significant cuts in areas, such as training and awareness. Organizations with inadequate security personnel and limited budgets for cybersecurity are likely to become extremely vulnerable and exposed to cyber-attacks. For example, CIP-004 "Personnel and Training" is one of the highest violated NERC Standards due to the lack of alignment between compliance and security departments within organizations. For instance, there is a gap between utilities' lawyers, focused on compliance, and cybersecurity professionals, focused on security. While lawyers are tasked to write cybersecurity policies with a view to avoiding penalties and fines, those who are responsible for following and executing those policies (e.g., engineers and the technical employees) find them challenging to understand and apply in practice. According to Mr. Humphreys, knowledge transfer and information sharing practices often fail to happen in organizations, and even if they are implemented, they are inadequate or out of date. Therefore, this complex regulatory environment may result in significant impacts on organizations. Potential attackers can take advantage of poor security protection, but also of the poor security of controls and systems in place (4 - 5). A mishandled response to a cyber incident can generate, in addition to disruption of operations, more reputational damage, leading organizations to start the vicious cycle again (6).

Regulatory considerations

The current method to regulate the utility industry and critical infrastructures has been increasingly overwhelming for companies over the last ten years. The challenge utility operators continue to face is that by the time a regulation becomes enforceable, the long bureaucratic and tedious procedure behind compliance becomes a hindrance to the development of good cybersecurity practices. This process creates a fear-based risk posture for utilities where companies view compliance as a risk component itself. This approach also produces negative outcomes, such as loss of competent professionals, compliance misunderstandings, financial and liability issues, etc.

Having worked in the federal space before going to the private sector, Chris realized that what he learned as an active member of the US intelligence community would be needed in the context of compliance as well. His experience led him to observing that managing compliance requires a proactive strategy to

[63] Yeung, K. (2004). Securing compliance: A principled approach. Bloomsbury Publishing.
[64] in 2008, Chris was the first regulator for all the electric utilities in Texas for the NERC critical infrastructure protection regulatory framework.
[65] It involved 1 million dollars a day per penalty, and utilities were audited on three years cycles.

circumvent problems before they occur. To do so, it is necessary to develop a "compliance through security" mindset that views compliance in function of cybersecurity[66].

"A premise of implementing effective regulations for utilities is taking a holistic, risk-based approach that integrates the right tools and controls and can incorporate changes quickly. Compliance should be an input; it should not dictate security," said Chris.

A first step in developing this approach would be creating security-based controls that satisfy multiple regulatory frameworks and leveraging them as a foundation to be secure and compliant[67]. In addition, incentives, such as tax cut benefits, would be a solution to encourage organizations to work through and maintain compliance and minimize the effects of the current punitive regulatory model. Adopting this method would be far more effective in developing compliance programs that ensure not only complete regulatory compliance coverage but also secure systems against new and more sophisticated attacks that could occur in the future.

CASE #7: MANAGING CYBERSECURITY AND COMPLIANCE IN A LARGELY UNREGULATED PLAYING FIELD

Some cybersecurity regulations are mandatory and vary in scope and focus. For example, any organization in the U.S. dealing with credit card information needs to comply with the Payment Card Industry Data Security Standard (PCI DSS), and those dealing with health information must meet the Health Insurance Portability and Accountability Act (HIPAA) requirements. However, in some industries, compliance with cybersecurity standards are, at times, a voluntary option[68]. In this case, non-mandatory regulations represent an opportunity for executives to show due diligence in the management of an organization's security processes and may be an ally in their fight for security. The Head Of Information Security in the organization described in this case took advantage of this factor.

Assessing the impact of vulnerabilities

The organization, one of the world's largest networks, considered their business structure sufficient to navigate the compliance environment with relatively little pressure; The company 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. The company's Senior Manager explained,

"We're from a heavily unregulated environment. As a public company, we are subject to the financial regulations of SOX (Sarbanes-Oxley Act)[69]. But beyond SOX, compliance requirements are optional. For example, if we wanted to handle credit cards, then we still would not need to be compliant, but customers that wanted to give us credit card information would force us to assume PCI DSS compliance. FedRAMP (the Federal Risk and Authorization Management Program)[70] is another example of an optional compliance framework. To us, compliance is purely a business decision."

For example, as achieving compliance with the SOX requirements was a large task, having a SOX steering committee was key to the success of the company. This committee was formed to ensure that all SOX compliance projects were following the right methodology. More specifically, the compliance model involved the creation of a team of professionals to coordinate the legal, financial, communication, and

[66] https://www.hstoday.us/channels/federal-state-local/electric-industry-urged-to-take-new-approach-to-cybersecurity/
[67] https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493745181.pdf
[68] Scarfone, K., Benigni, D., & Grance, T. (2008). Cyber security standards. Wiley Handbook of Science and Technology for Homeland Security, 1-10.
[70] https://www.soxlaw.com
[71] https://www.fedramp.gov/faqs/

security side of the project. Additionally, having senior management members, such as the Senior Business Operations Manager, at the top of the process provided a more comprehensive perspective of compliance. However, even considering the flexibility of this type of environment, not only did compliance not seem to offer any advantages to the company, but it could also turn into an obstacle. The manager elaborated,

"Auditors don't have a complete familiarity with the specific security processes that they audit. A company may provide a simplified explanation of a security incident or verbally respond to the auditor on its cybersecurity procedures and programs. While this may satisfy an auditor, it doesn't provide enough information about a company's actual security. It doesn't reflect the overall kind of work that goes on in a day. Unless you can show that at any point in time, you can look back and see the history of the controls, an audit only provides an overview of the systems in scope during the period in which it is conducted. In this case, compliance becomes a mere tick-box exercise and is not a practical benefit to cybersecurity."

The manager gave an example in one of their system. In their environment, they used SSH with each user having their own SSH key. Access controls were used to limit who can access the system, but the access control relied on a file on the host that should have had a list of users and their permissions. The manager noted there were limitations to this approach, stating that, for example, someone (e.g., system administrators) could use the configuration management and replace the file with a malicious one.

Auditing and alerting on changes in the such a system would be complicated and but without that they may cause a false sense of security; the manager stated,

"It is not that the standards or regulations would not be useful, but there are simply too many variations and issues in the implementation of these processes that there would be a certain lack of accuracy in the audit assessment."

Adopting an "Inside-Out" Approach to Compliance and Cybersecurity

As the business expanded, the manager and his team were continually asked to change focus and direction to maintain customer confidence and demonstrate the maturity of their business. Therefore, questions started arising regarding whether a compliance structure could be an aid in ensuring that the company met customer needs. However, they started to realize that compliance was not just about customer expectations but was also about covering gaps that would otherwise leave the organization vulnerable. In particular, it was the discovery of a security vulnerability impacting operations that revealed the need for supplementary compliance in their environment. The root cause was identified as the employees having a sectional view of compliance controls and their possible impacts. More specifically, this incompleteness was due to a lack of efficient exchange of information between the different departments. The manager's team was successful in avoiding damages, but this resulted in a partial view of cyber risk that only took into account some of the factors that affected the real level of risk. The manager commented,

"Last year, our company went through an exercise where we discovered more SSH keys[71] in our environment. Our team knew that everyone individually was aware of them, but this didn't seem to be an issue from a risk point of view. Therefore, despite this, we were happy with the overall level of risk that we had in the business area. Effectively the risk was being decided at the engineering level, not at the business level. Eventually, we realized that our risk perception wasn't quite right because the rest of the company wasn't aware of these vulnerabilities. This means that, in reality, we weren't satisfied with that level of risk as our risk tolerance was exceeded. We then went through an internal audit; we cleaned up our keys, and we put in place some technical controls to hopefully mitigate the risk in the future. But, probably, we would have caught these flaws if there was a compliance framework, such as NIST, in place."

[71] SSH, or Secure Shell, is a network protocol used to securely connect a computer over an insecure network (Internet) in order to send commands to it. SSH keys are a way to authenticate users to a system. In the example, having more SSH keys than needed is an issue for the company as it means that it is more difficult to keep track of them. For example, they could potentially be compromised or used by a rogue former employee.

Certainly, relying solely on compliance to provide the advanced cybersecurity protection that the company needed wasn't an option as it could carry considerable risk. However, not having compliance procedures in place could also throw the company off-track. Therefore, given the problematic situation, the manager was called in to develop an approach that took advantage of the knowledge behind compliance requirements as well as the company-specific cyber threats. He started reviewing his company's security environment and looking at internal risks. After an in-depth investigation, he found that the first step was pushing for the implementation of the NIST (National Institute of Standards and Technology) CSF (Cybersecurity Framework). Thus, the company used the NIST framework to tie together their security operations. However, their approach wasn't limited to achieving NIST compliance. They mapped their practices to the CSF and used it as a complement to their cybersecurity strategy. They created a target profile to identify the desired end state of their cybersecurity program, which did not necessarily include the entire framework. Instead, it comprehended the most critical, impactful cybersecurity practices that enabled them to achieve their cybersecurity objectives. For example, among the NIST's five functions[72], identify, prioritize, and respond were the most important to the company. The reason for this is that they consisted of practices about identifying risks to their critical services, determining criteria for measuring those risks, and managing those risks. These practices have been essential to building a practical risk management function within the company.

"Our goal is to steer our company towards a scalable assessment of our current security capabilities and deficiencies. We often find ourselves drowning in a sea of different techniques to measure security programs, so it is necessary to find a flexible scheme that provides a common language and a common understanding of what's essential from a security point of view. And NIST is a good balance between efficiency and accuracy," the manager said. "No matter the scale you're looking at, the NIST CSF is applicable to that scale. You can implement it in any environment."

The adoption of this framework allowed the company to create a customized implementation plan, which also helped them budget for cybersecurity improvement activities.

Conclusion

In the beginning, the organization was secure in a limited way. The organization considered itself to be cyber protected, and executives did not feel the need to take up the challenge of becoming compliant with any non-mandatory security standards as they thought their internal methods were the answer to all their security requirements.

"We have a distributed architecture that's designed from the ground up to be resilient so that there aren't many single points of failure. However, we realized that this structure might not be sufficient as we identified a lack of maturity in certain implementations, which we're trying to address through mandatory guidelines and internal audits."

Different risk assessments and techniques were used to track the maturity of the company over time to ensure organizational goals and compliance requirements were met. Also, they started establishing compliance as a separate function, which allowed them to oversee compliance procedures more efficiently.

"My biggest goal is to implement a 'living framework' that we can review and monitor every day," the manager commented. "Implementing the NIST CSF now and other security frameworks later could put the company in a much better position in the future."

The company is still maturing and changing, but recent compliance efforts to align with non-mandatory cybersecurity frameworks like NIST produced results; they showed the organization its main security gaps and what to do to ensure a more robust security posture, while also maintaining an objective perspective of the overall security goals.

[72] The NIST framework includes 5 main functions: identify, protect, detect, respond, and recover. These functions represent the highest level of abstraction included in the framework and are applicable to cybersecurity risk management as well as risk management in general.

CASE #8: RE-EVALUATING THE APPROACH TO SELF-REGULATION IN THE FINANCIAL INDUSTRY

In recent years, economic, social, technological, and regulatory dynamics have led to profound structural changes in the banking industry. Faced with this trend, the banking and, more broadly, the financial system has started implementing self-regulatory arrangements and controls to avoid reputational risks and retain customers. These practices have been embedded into business functions, from strategy and governance to risk management processes and cybersecurity.

The efforts made to consolidate and bring consistency to such self-regulatory principles and frameworks have proven to be efficient in some cases. For example, self-regulation allows for greater flexibility and more diversity in methods of compliance with rules. Additionally, requirements are drafted by internal participants with an intimate knowledge of the industry and procedures. These factors permit financial organizations to respond to changes in an innovative, timely, and appropriate manner. However, while self-regulation mechanisms are necessary to safeguard the financial system, recent global and cybersecurity threats have introduced complexity and uncertainty into banking[73]. As a result, the task of developing efficient rules has become inevitably more complicated. Because of the ever-changing nature of banking business, financial institutions are continuously required to evaluate current regulatory concepts and to design better frameworks.

One question that arises in this context is whether the current largely self-regulatory approach is the right one for a modern financial system. This question has been posed to a compliance expert at an international financial institution that provides investment and management services. In particular, this organization aims to finance various projects in the private sector, facilitate productive private enterprises' growth in the territories of its members, and further economic development. As one of the largest public sources of financial investment, it is authorized to operate as a financially autonomous entity and make independent decisions, even from a regulatory point of view. However, through his experience working on a number of projects aimed at mitigating risks, the compliance expert learned that the existing self-regulatory scheme only partially met the challenge of protecting the financial system.

Ineffective procedures and performance

The compliance expert argued that the current system struggles to adapt to changes and the current supervisory mechanism is slow in taking action.

He commented,

"We are self-regulated. That means that we do not follow regulations and standards, such as the FCPA[74][75], or the anti-corruption law; we have our own policies and procedures that are based upon other regulations. However, although we are a self-regulated organization, we are still subject to government intervention to a degree[76]. Therefore, our operations are sometimes governmental and very bureaucratic. I think that is why it takes time for us to catch up with the private sector. I think that is why it takes time for us to catch up with organizations operating in the private sector. For example, there's no way we work as efficiently as Google, HSBC or JP Morgan. They are probably quicker in terms of how they analyze risks, transactions, and do business in general."

[73] https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-9930.t01-1-00033
[74] The Foreign Corrupt Practices Act (FCPA) is a federal statue that was enacted in 1977. It was designed to designed to combat corporate bribery.
[75] https://www.sec.gov/spotlight/foreign-corrupt-practices-act.shtml
[76] As an international organization providing services in multiple jurisdictions, depending on the country in which a financial project is carried out, some operations may be subject to governmental influence to some extent.

In addition, he felt there was a perception that their performance was not matching many of their efforts due to a low turnover rate within his department. Employee turnover tends to be a major issue that characterizes public institutions, and the financial organization was no exception. By retaining employees, it was losing the many benefits that external hires could bring to the institution, including new ideas, new skills, and competitive intelligence.

"I have only been here for five and a half years, but I have noticed this growing trend that people join early in their career and stay here for a long time. Therefore, we are not getting the new fresh knowledge coming from the outside that may help to improve our processes internally," he explained.

Another challenge described by the compliance expert is the lack of a strong culture of compliance. Despite being a self-regulated organization, it has a specific set of compliance principles in addition to the typical group of norms applicable to any other institution operating in the financial sector. He commented,

"One of the critical points is that those who tend to run the organization are economists and development bankers who have not spent much time in a highly regulated environment. Compliance procedures tend to be pushed by the internal compliance department or our general counsel. So, there is not strong support in tone from the top, which makes it quite challenging. I think that is a huge mistake."

Different compliance expectations

Depending on their designs and scope, rules developed by self-regulated organizations could be different compared to those established outside[77]. For example, external regulations could impose more rigid restrictions on the functioning of the financial system or may require different procedures, causing conflicting expectations for clients. The interviewee provided an example,

"We are not covered by regulations, such as the General Data Protection Regulation (GDPR). In Europe, however, we have lots of clients who expect us to follow the same business standards that they do. So if they give us their personal data, then they expect us to handle it the same way that they would in Europe. This external pressure is forcing us to correct ourselves in terms of becoming more efficient and more conscious of these types of issues, even though we are in a different business line."

Given the global interconnectedness of financial markets, it is necessary to develop a global understanding of regulations and ensure that the "rules of the game" are the same to compete at the same level.

Different risk management practices

Regulation and regulatory management must be sensitive to risks in self-regulated organizations. This means that an organization that takes more significant risks and treat different risk profiles must also be able to manage risk accordingly.

" For example, we once had to manage a transaction between two African countries that presented a range of potential risks. However, we thought that that transaction would have made a positive and significant impact, and we decided to take the risk. While our corporation takes compliance risk seriously, at the end of the day, it is necessary to have a very high-risk tolerance for it. Other institutions, such as big Western banks, instead, may not have that luxury because they have to consider more compliance risks, including the regulatory enforcement aspect. Ultimately, for us, it is a business decision regarding whether or not to accept the risk and do a project regardless of the risks involved."

In this context, regulating cybersecurity presents an interesting quandary as self-regulated entities often possess larger budgets than other organizations, such as private financial institutions. However, according to the interviewee, this factor does not mean that investments are easier to manage. Leaving the responsibility for setting and managing cybersecurity to individual actors may be complicated. He explained,

[77] https://www.sciencedirect.com/science/article/abs/pii/S0267364913000575

"Budgeting choices are determined by our CEO, who uses a priority-driven process to decide on where the money should go. The general counsel has the task of dividing the budget between different departments, such as the legal department, the compliance department, and others. Additionally, requesting certain investments may be a long and complex process. We have a budget, for example, for some IoT initiatives, which we have to put in special requests for. Therefore, despite having a sizeable original budget, we are limited in the way we can use it individually."

To provide a better baseline for tracking cost, it became essential for the organization to have mechanisms to monitor the achievement of a cybersecurity strategy, with measurable outcomes to be achieved. The organization has made a significant effort and investment over the past few years in the area of expanding and enhancing cyber threat monitoring and response capabilities to strengthen their overall security posture. The compliance expert pointed out that in his department, there are cybersecurity professionals who serve, for example, on an incident response team for data breaches.

Conclusions

Self-regulation is generally seen as the most efficient and best mechanism for managing most financial activities. However, when they operate in areas involving wide-ranging matters – such as the global digital environment – it becomes challenging. Because of the scale and variety of risks and problems deriving from cybersecurity issues, effective self-regulation may seem hard to implement. For this reason, government-led mandatory regulations are often considered to be the way forward on matters that involve far-reaching risks. However, according to the compliance expert, establishing an approach based on common grounds would provide a useful lens through which to solve these problems in self-regulated industries. Not only are improved internal rules necessary, but it also essential to implement a well-functioning management system that exercises reasonable control to ensure a stable financial system and a level cross-border playing field.