
# Analyzing the Interplay Between Regulatory Compliance and Cybersecurity (Revised)

Angelica Marotta, Stuart Madnick

**Working Paper CISL# 2020-15**

**March 2020**

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

# Analyzing the Interplay Between 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

Today, regulatory compliance is a critical component of any cybersecurity program. However, although compliance is often the driver for developing or improving cybersecurity, it may be incomplete as a cybersecurity measure itself. The result is that even a compliant organization may have gaps in its security posture. Through an in-depth literature review, this paper investigates the complexity surrounding compliance and the factors that have an impact on the interplay between compliance and cybersecurity.

## Introduction

Over the past decade, cyber threats have increased rapidly. Examples of notable cyber attacks include the massive blackout of the Ukrainian power grid in 2015, the Mirai botnet of 2016, which brought down many major websites, and the 2017 global ransomware attacks (e.g. WannaCry and NotPetya), which impacted governments, hospitals, and businesses around the world (Bonakdarpour et al., 2018). In 2019 over 11.4 billion data records were breached, an increase from 4.3 billion in 2018. These and many other cyber events accentuate the need to regulate cybersecurity practices and activities, and to impose penalties and sanctions for violating the regulations. However, relying solely on compliance to achieve security protection may not be sufficient since the success of cybersecurity operations tends to vary depending on several factors. For example, it may depend on how readily an organization facilitates the implementation of regulatory requirements or the monitoring capabilities of an organization. Thus, compliance is not black and white but rather a matter of a series of components, which may either minimize or maximize the impact of compliance on cybersecurity. This study examines the interplay between compliance and cybersecurity through a multidisciplinary structured literature review of 80 publications. In particular, this research offers three contributions. Firstly, it provides an overview of compliance, which shapes the basis for moving from the general concept of compliance to the current notion of cybersecurity compliance. Secondly, it addresses the results of a comparison between worker safety compliance and cybersecurity compliance. Thirdly, it investigates cybersecurity compliance in different sectors.

## Definition and Domains of Compliance

Compliance is a broad topic, and it is often hard to define as its operational boundaries can be varied. The term follows a philosophical tradition involving the belief that people lack self-governance ability and, consequently, it is necessary to establish a robust governing authority (Foorthuis & Bos, 2011). Today, there is not a generally accepted definition, even though many scholars and professionals typically refer to compliance as a method for ensuring that specific norms and rules are met (Kharbili et al., 2008). For example, according to Wright (2008), "compliance in the true sense of the word entails a legal requirement or a standard for context." Other authors pointed out that adhering to laws and regulations is a way of mitigating potential risks to society and encouraging ethical behavior (MacLean and Behnam, 2010; Abdullah, Sadiq & Indulska, 2010).

Increasingly, compliance has been integrated into the organization's day to day activities. We find it desirable to distinguish between *external (regulatory) compliance* and *internal compliance*. According to Nawar and Dagam (2015), regulatory compliance involves following the rules for a specific industry or field established by an outside authority. Internal compliance refers to the procedure of following internal processes and best practices established by an organization (Foorthuis, 2012) Unless driven by outside parties and particular industry requirements, internal compliance includes adherence to policies, protocols, codes, or procedures specific to the organization itself (Lyons, 2016). However, arguing

that regulatory compliance merely consists of meeting rules and regulations limits the notion to the legislative area, omitting related values, such as commitment and integrity. The existing literature provides definitions of regulatory compliance, although described in a fragmented manner and from different perspectives. The following categories, shown in Figure 1, represent some of the most common trends:

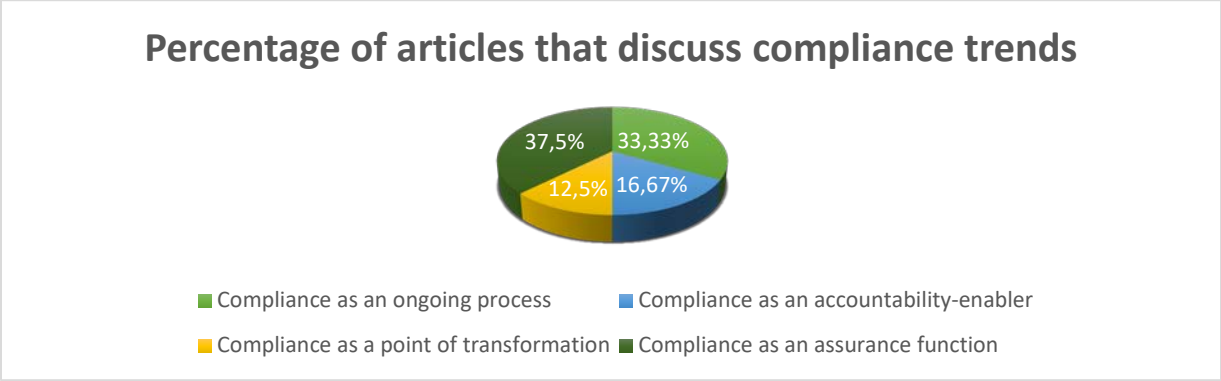


**Figure 1: Percentage of articles that discuss compliance trends**

### *Compliance as an accountability-enabler*

According to Breaux, Antón, and Spafford (2009), compliance is a tool to hold organizations accountable. These authors stated that compliance and accountability are intertwined because accountability involves the acceptance and assumption of responsibility for complying with regulations. However, being responsible in this context does not mean that compliance with the rules is also an act of accountability or that the rules themselves are an accountability mechanism. It means establishing enforcement procedures and ensuring that everyone is set to a standard expectation when it comes to regulations. From a broader perspective, other authors (Romzek & Dubnick, 1987; Romzek & Ingraham, 2000) extended this concept to all the participants involved in the regulatory chain, from the regulation originator to the regulated party. More specifically, they argue that, given the complexity and evolving nature of the regulatory environment, it is critically important to integrate the concept of accountability into every step of the regulatory process. For example, Scott (2000) suggested a devolved regulatory framework to ensure accountability. Lodge (2004) and Mashaw (2006) also discussed different methods to improve transparency and accountability in regulatory activities. More recently, May (2007) elaborated these concepts and classified regulatory accountability into four types: legal accountability, bureaucratic accountability, professional accountability, and political accountability. Each level differs in the unique challenges that they pose for ensuring regulatory accountability and contributes to the overall regulatory performance (May, 2007, p 8-26).

### *Compliance as an assurance function*

According to Loshin (2010), compliance means "demonstrating that the organization is in accordance with defined guidelines." Being "in accordance," just like Loshin stated, means being in a state of conformity with some established guidelines, specifications, or legislation (Kingsbury, 1997; Mushkat, 2009). Other authors claimed that compliance is driven by needs to demonstrate adherence to regulation, and, therefore, auditing is fundamental in determining its assurance function (Panitz, Wiener & Amberg, 2011). In particular, establishing and maintaining assurance involves helping management, the board, and other stakeholders identify and consider the critical risks arising from technology. In the literature, communicating assurance has been mainly addressed through the organizational reporting procedures and communication frameworks for notifying and monitoring compliance issues or changes. Examples of communication tools that emerged from the study of this topic include training sessions, emails, memos, and information sharing activities between stakeholders. Effective communication enables organizations to identify the causes of potential gaps and implement control mechanisms (Usnick & Usnick, 2013, p. 311).

### *Compliance as a point of transformation*

Other authors seem to refer to regulatory compliance as a way to initiate transformation of the organization. In examining compliance in the data security field, Kwon and Johnson (2013) defined it as "a snapshot of security about whether an organization exhibits controls." El Kharbili (2012) touched on this concept by defining compliance as "an interval between two states in the history of the evolution of the enterprise."

However, time is not the only element that scholars use to express the concept of transformation in compliance. Some also use the word "action" to explain how an organization, and more specifically, employees and teams can have the power to move from a state to another in terms of compliance. Compliance is, therefore, considered an action required by a supervisory authority that enterprises need to put into practice (Pererva et al., 2017).

### *Compliance as an ongoing process.*

Conversely, some authors, such as Caldwell and Eid (2007) defined compliance as a progression and emphasized their definitions by describing compliance as an integral part of the organizational structure and process. VanLengen (2008) stated that regulatory compliance is "not a one-time event," and business management and IT should make an active effort to maintain it over time. For example, Doganata and Curbera (2009) defined compliance as "an ongoing process that goes beyond testing and evaluating the internal controls of a sampled space." This concept illustrates that an organization needs to work consistently to align organizational goals and regulatory requirements (Bailey, Haq & Gouldson, 2002; Wells, 2013). The compliance process involves periodic checks to ensure adherence to regulations and constant monitoring (Pupke, 2008). In particular, according to El Kharbili (2012), the process of managing compliance "deals with the modeling, checking, enforcement, and analysis of compliance requirements (CRs) extracted from regulations of various kinds, such as laws (i.e., legislations), contracts, internal policies, etc." Additionally, according to Moeller (2011), "for enterprise management, compliance is the process of adhering to a set of guidelines or rules established by government agencies, standards groups, or internal corporate policies (Bailey et al., 2002, p. 245-256)."

## Cybersecurity and Safety: Common basis and Lessons Learned

In trying to understand the role of compliance on cybersecurity, we decided to look at other areas where compliance played an important and historic role. There were several possibilities, but we decided to focus on safety since it also requires active support throughout the organization. One of the most evident commonalities is that compliance is highly dependent on the relationship between regulators and the corresponding regulated industry, and the way organizations achieve the intended purpose of regulation.

In the context of cybersecurity, regulations are part of a complex combination of state and federal regulations, including different regulatory approaches and degrees of scope (Thaw, 2013, p. 287). Cybersecurity regulations have not found yet a commonly accepted classification in the literature on compliance. However, one of the closest terms to define this regulatory category is "cybersecurity law." While most authors refer to cybersecurity law as a set of cybersecurity standards, national frameworks, and relevant case law on cybersecurity, Kosseff (2017) provided a more purpose-oriented definition of cybersecurity law by defining it as a discipline that "requires an examination of the harms that the law seeks to prevent." The type and severity of possible harms also play a critical role in the safety regulatory environment, which seems to share similar principles and dynamics with the one related to cybersecurity.

One similarity between safety and cybersecurity is the underestimation of their impact. For example, in the distant past, there was little attention to improving worker safety since it was cheaper to replace a dead or injured employer than to introduce safety measures. Later on, the combination of higher accident costs occurred during the years between the First and the Second World Wars, along with the growing safety concerns in large organizations and society, led to the implementation of safety-related legislation, such as the Occupational Safety and Health Administration (OSHA) and the Mine Safety and Health Administration in 1970. Lawmakers designed the law to encourage safer workplace conditions and ensure that work environments were free from hazards (Bradbury, 2006). For many years now, working safely has been at the forefront of issues that regulators address. For example, the introduction of rules to encourage improvements in worker safety has sharply redefined and influenced the concept of compliance over the years, from reducing stress and risks of incidents and occupational injuries in the workplace to the development of more comprehensive insurance plans.

Similarly, the emergence of advanced cyber threats has been a catalyst for the enactment of rigorous security rules. Preserving the Confidentiality, Integrity, and Availability of information systems (also known as the CIA Triad) has been one of the motivating forces behind most of the regulatory efforts (Adams et al., 2015; Cojocaru, 2019; Deelman et al., 2019, p. 13-15). For example, the 2014 cyber-attack against Sony Pictures Entertainment compromised all three principles of the CIA Triad. According to Kosseff (2017), the

attackers harmed the confidentiality of employees' personal information and compromised the integrity and availability of Sony's systems by altering their interface and limiting access to the network. After cyber events like the Sony attack, regulators began developing more regulatory initiatives to adapt to the current landscape. Regulators decided to look back on many of the lessons that safety has taught over the years. Thus, in some cases, safety represented a departure from which regulators defined rules on cybersecurity and cyber risk. For example, one of the achievements in safety regulations was recognizing that even minor vulnerabilities can result in devastating damages, injuries, lost production, and significant fines. Regulators started considering organizations not simply as part of the solution to improve safety. Rather, they viewed them as the main actors in handling risk (Regens, Dietz & Rycroft, 1983). In the context of safety, the term "risk" is generally defined as the likelihood of hazard occurrence (Smith, 1992). Risk has always become the cornerstone of safety management, and therefore, is an important component of safety compliance. For example, safety regulations require risk assessments in areas, such as hazardous substances, lifting equipment, noise management, and so on. Today, cybersecurity regulations and standards integrated this concept into their regulatory principles and require risk management as a foundation. For instance, ISO 27001 considers risk as the basis for implementing appropriate information security controls; the GDPR requires a Data Protection Impact Assessment (DPIA), etc. Another fundamental lesson learned by cybersecurity regulators is the "implementation of safeguards or countermeasures against a hazard scenario." (Hildenbrandt & Van Beurden, 2019, p. 625-630). Just like compliance obligations for safety require organizations to provide employees with training and proper protective equipment, cybersecurity regulations require the adoption of measures, such as firewalls, antivirus software, encryption measures, intrusion detection systems, etc. (Kosseff, 2019).

Despite risk-driven fields, cybersecurity and safety have been generally addressed separately from a regulatory point of view. However, the rise of cybersecurity as a concern for sectors, such as Industrial Control System (ICS), has encouraged a conversation about the integration between cybersecurity and safety into the regulatory environment. For example, safety standards are now beginning to require cybersecurity controls. For example, the second edition of IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector), includes clauses on security risk assessment and cybersecurity resilience (Paul & Rioux, 2015, p. 335-349). Additionally, now the majority of cybersecurity requirements apply to systems, which are already subject to well-established safety obligations. Regulators are beginning to understand that applying safety knowledge to the cybersecurity function, in turn, can have a positive effect on safety as well.

Consequently, to successfully achieve the desired regulatory goals in both fields, not only do cybersecurity regulations have to ensure confidentiality, integrity, and availability, but it also has to go beyond by addressing the concept of dependability. The term dependability is commonly used to indicate the measurement of a system's attributes, such as availability, reliability, safety, integrity, and maintainability (Trivedi et al. 2009). Threats affecting a system subject to safety and cybersecurity requirements may affect its entire life cycle and, therefore, cause a drop in dependability (Laprie, 2005). Examples of threats include, but not limited to, operational risks, such as human errors, system errors, improper management, etc. (Tattam, 2017). While traditionally, regulations have focused on compartmentalized approaches to operational risk, recently, an increasing number of regulatory bodies are considering integrated strategies that foster convergence between safety and cybersecurity.

## Cybersecurity compliance differs in different industries

On the one hand, cybersecurity regulations inherited positive principles from safety; on the other hand, safety also passed down some of its issues to cybersecurity compliance. For example, one issue is the misalignment between safety and compliance. In some situations, the line between the two can be blurred. For instance, in the construction industry, just because workers are required to wear protective equipment under a particular regulation, it doesn't mean that they are safe. Although the bare minimum offered by safety rules can be acceptable to be compliant, it may not be the same in certain circumstances. Similar considerations are also part of the current discussion on cybersecurity compliance. For example, Kwon & Johnson (2011) investigated whether the level of compliance affects security performance. Surprisingly, they found that an organization's level of compliance doesn't significantly affect actual security performance, although "a combination of cybersecurity and compliance strategies is better than that of either alone (Kwon & Johnson, 2011)."

Conversely, Muckin, and Fitch (2014) argue that much of the mandatory controls required by regulations may negatively drive cybersecurity behaviors. Being the result of analyses and assessments conducted on a large scale, these controls may not be suitable for each unique organizational environment, and may, therefore, prevent organizations from implementing procedures that effectively address their particular needs. Similarly, Scully (2011) stated that "compliance standards should not rigidly mirror long-accepted security measures that have failed us; rather, compliance standards should be based on evidence of successful security practices." Along with this line of thought, other studies (Oltsik, 2011; Donaldson et al., 2015, p. 27-44) examined the reasons why compliance is not a guarantee for security protection. Some of these argue that, regardless of whether good compliance coincides with good security, relying on compliance provides a false sense of security (De Guzman, 2007; Grossman, 2008, p. 24-27). Yimam & Fernandez (2016), instead, provided a different perspective. They claim that, in some cases, compliance and security are only assessed either at the testing phase or at the last stage of application development. According to the authors, this practice may result in gaps in identifying potential threats.

However, given the high number of contexts in which cybersecurity regulations are applied, paths to compliance and security are in practice diverse. One way to comprehend the dynamics of the relationship between compliance and security is to focus on some of the key industries which are heavily regulated.

### *Financial service*

Regulations within the financial sector vary greatly based on the financial service. According to Mohammed (1970), some of these regulations focus only on investment products, while others deal with credit and liquidity functions. However, since the financial industry is highly dependent on information technology, cybersecurity has now become one of the most significant components of financial regulatory compliance. In particular, protecting asset data, managing the use of sensitive information, monitoring electronic payments are just some of the main regulatory priorities in financial services. For example, the Gramm-Leach-Bliley Act (GLBA) imposes liability for data breaches and provides obligations on how organizations must collect and share information in the financial services sector (Mohammed, 1970, p. 1-11; Cuaresma, 2002, p. 497). The Act, originally introduced to "modernize" the financial service industry, requires financial institutions to adopt "administrative, technical, and physical safeguards" to "ensure the security and confidentiality of customer records and information" and "protect against unauthorized access to or use of such records" (Smith, 2002). Additionally, ensuring accountability is a constant requirement for financial service organizations. The Sarbanes-Oxley (SOX) Act of 2002 places, for instance, emphasis on this concept as it requires organizations to be accountable for the security, accuracy, and reliability of all information systems that they use when reporting financial information. However, despite these regulatory initiatives, Arner, Barberis, and Buckley (2017) found that, following the 2008 Global Financial Crisis, the nature of financial markets, services, and institutions have changed dramatically. While information sharing concerns, users' cyber protection, and secure digital transactions are still some of the principal goals of regulatory compliance in the financial sector, there is an increasing need for new or updated measures to address new cybersecurity threats. For example, Hornbuckle (n.d.) discussed how standards, like the Payment Card Industry Data Security Standard (PCI DSS), are not sufficient to protect companies from cybersecurity events, such as the Target store breach (Dissanayake, 2019). The increasing need to address these issues in financial service has led to the rise of the "FinTech" phenomenon, which is described in the literature as "the use of technology to deliver financial solutions (Douglas, 2016, p. 17; Jenik & Lauer, 2017)." As FinTech becomes more and more advanced, it is necessary to address more cybersecurity demands to ensure that companies continue to deliver secure services.

For this reason, the rapid evolution of FinTech is also influencing the regulatory environment in many financial sectors, such as banking and capital markets. Some authors argue that this phenomenon has caused the need for a new approach to addressing security through compliance, referred to as "RegTech." This term, which is a contraction of "regulatory" and "technology," describes the use of technology in the context of regulation and is used by regulators and supervisors to address the compliance issues raised by FinTech (Jenik & Lauer, 2017 ). Supporters of this new movement claim that the potential of RegTech is significant as it provides the basis for a more suitable and applicable regulatory framework that identifies and addresses regulatory risks while also facilitating more efficient regulatory compliance (Arner et al., 2016 )". Conversely, others (Packin, 2018, p. 193) believe that the adoption of RegTech is difficult. Examples of challenges include the difficulties of removing ethical issues resulting from organizational culture or the increase in regulatory requirements and their related costs.

### *Healthcare*

Traditionally, healthcare regulations have incorporated the need to maintain the confidentiality of medical information. However, the Health Insurance Portability and Accountability Act (HIPAA) has raised the importance of safeguarding personal medical information and has provided a more comprehensive regulatory framework and penalties to encourage compliance in the healthcare field. HIPAA defines a broad set of rules and procedures, many of which require proper technology that provides the security features suggested by HIPAA guidelines (Appari & Johnson, 2010, p. 279-314). The Act has also placed more attention on the concept of responsibility of those who transmit health data electronically. However, while the establishment of HIPAA and other health-related regulations, such as the Health Information Technology for Economic and Clinical Health (HITECH), was the catalyst for the development of improved medical information requirements, some scholars argue that there are several issues that prevented them from being a complete solution to effectively securing Personal Health Information (PHI). Mohammed (2017) stated that various factors might affect compliance in healthcare. For example, in the case of HIPAA, the regulation focuses more on the areas to protect rather than specific methods to implement security in those areas. Additionally, the author pointed out that guidance for some cybersecurity concepts is absent, and that some rules fail to keep up with the evolving cybersecurity threats. Other authors (Shen et al., 2006; Grandison & Bhatti, 2012, p. 108-124 ) also examined the comprehensibility of the regulation. They argued that, although privacy and security rules cover enough areas to enable healthcare organizations to define themselves compliant, the language of the procedures in the regulation, such as those related to privacy and consent, doesn't facilitate comprehension by health operators and patients. More broadly, Johnson and Kwon (2012) described how the overall regulatory environment for the healthcare sector requires modifications. They noted significant disparity both in security practices and in perceived compliance with federal and state regulations. According to the authors, low levels of perceived compliance may cause uncertainty towards medical practices and the required path to compliance. Compliance perception in healthcare is also a topic that other authors addressed (Bauer & Latzer, 2016 ). Miller and Tucker (2011) indicated that the "safe harbor provisions in breach notification regulations" may cause a false sense of security because they encourage people to be "careless." (Warkentin et al., 2006, p. 326) found that employees of public healthcare organizations reported higher levels of perceived compliance than those of private facilities. Their study also suggested that public healthcare administrative and medical staff members are likely to be more capable of protecting private health information.

### *Automation*

Cybersecurity is becoming an increasingly important component of all forms of automation. The term automation identifies the technology that uses control systems for managing processes and reducing the need for human intervention. Not only is automation applied to execute repetitive or complex operations and boost productivity, but also to make specific procedures more secure. According to Joshi et al., (2019), "automation includes the combination of instrumentation, electrical, electronics, and computer systems to control the process." It covers applications in a vast range of fields, such as Industrial Control Systems (ICS), home automation (or domotics), robotics, Internet of Things (IoT), communication, automotive, etc. Traditionally, automation systems were not designed with specific cybersecurity characteristics in mind (Tuptuk & Hailes, 2018, p. 93-106). For this reason, these systems became extremely vulnerable to cyber-attacks over the years. In a detailed report on the status of IoT, the Federal Trade Commission (FTC) staff identified privacy and security concerns related to the use of IoT devices. Some of these involved collecting sensitive information (e.g., geolocation, financial data, health information). For example, the report identified significant vulnerabilities with home automation systems and smart appliances. Likewise, other scholars indicated that home automation, although being an interdisciplinary science aimed at improving the quality of life in domestic environments, creates unique risks to properties as well as critical risks for people (e.g., physical harm and even loss of life) (Kirtley & Memmel, 2018, p. 455; Croce, 2017; Millán et al., 2014, p. 239-254; Weber & Studer, 2016, p. 715-728).

Although much of the technological equipment used in automation is often the same as that employed in other information system environments (e.g., software, gateways, wireless access points, routers, computers, etc.), the cybersecurity goals and needs of automation are not the same as those for other fields. Protecting automation systems requires considerable experience and knowledge of automation technologies as well as their related operational functioning. General industry regulations and cybersecurity best practices don't seem to secure automation systems accurately. Instead, standards have seen a constant evolution over the last few decades. There have been, for example, several initiatives from the International

Society of Automation (ISA). Among these, IEC 62443, developed by both ISA99 and International Electrotechnical Commission (IEC) committees, is one the most widely used set of standards at the international level. Its purpose is to protect components or systems used in industrial automation and control against cyber risks (Dayabhai, 2017). Standards like IEC 62443 provide a flexible framework to address current and future cybersecurity vulnerabilities in industrial automation and control systems (IACSs) and are generally applicable to all industry fields and critical infrastructures. However, according to Leander, Čaušević, and Hansson (2019, p. 101), there are several issues that organizations might face when trying to keep compliance with IEC62443, especially in the context of Industrial Internet of Things (IIoT). For example, they noticed a lack of guidance concerning the handling of cross-zone communication and software updates. Just like Leander et al., other authors (Frotzscher et al., 2014, p. 67-72; Mathavi, 2012, p. 1-8) agree that the majority of standards on automation need improvements and, in some cases, specific automation industries have no regulatory protection. Frotzscher et al. (2014) argue that companies operating in the industrial wireless automation sector have no regulatory coverage regarding some specific issues, such as wireless interferences, leaving them more vulnerable to cyberattacks.

## Conclusions

Compliance and security have moved from being general topics of interest to representing an increasing concern within specific industries. Looking at the literature, it emerges that each sector reflects a combination of issues affecting the relationship between compliance and cybersecurity. Evaluating these issues presupposes the establishment of compliance metrics, according to which the industry in question is measured or assessed. Some authors used several approaches to determine whether or not compliance procedures are effective with respect to regulations and security characteristics (Frotzscher et al., 2014; Grandison & Bhatti, 2012; Johnson & Kwon, 2012; Leander et al., 2019; Mathavi, 2012; Miller & Tucker, 2011; Mohammed, 2017; Shen et al., 2006; Smith, 2002). The following criteria summarize the fundamental considerations that guided them in their evaluations.

- **Clarity.** The clarity of the language or concepts introduced by regulations or standards and how it applies to the industry and the corresponding cybersecurity environment.
- **Implementation capability.** The ability to implement regulations or standards into action.
- **Consistency.** The consistency of regulations or standards between the industry and the related cybersecurity needs.

Table 1 shows the major issues by industry derived from the analysis of the financial, healthcare, and automation sectors.

**Table 1: Compliance Characteristics for Industry Sectors**

| | **Industries** | | |
|---|---|---|---|
| **Compliance Criteria** | Financial service | **Healthcare** | **Automation** |
| **Clarity** | The language and concepts of regulations are sometimes outdated, resulting in unclear or misaligned terminology | Regulatory language doesn't facilitate comprehension by health operators and patients (e.g., privacy and consent concepts) | Lack of guidance about some industry concepts (e.g., cross-zone communication management and software updates) |
| **Implementation capability** | Ethical issues, the high number of regulatory requirements, and their related costs is an obstacle to compliance implementation | Difficulties regarding the enforcement of privacy rules but good response from public healthcare administrative employees | Good applicability and flexibility in all sectors |
| **Consistency** | Discrepancy between current cybersecurity goals in the financial sector and actual FinTech needs | Disparity between security practices and perceived compliance due to a false sense of security | Regulatory gaps or no regulatory protection against specific issues (e.g., wireless interferences) |

The results of this analysis show that some industries are considered to need more attention than others in some compliance areas. It is also observed that some criteria depend on others. This dependency may contribute to complexity regarding compliance issues. For example, the extent to which regulatory language is clear has a direct influence on implementation capability and consistency in the majority of industries. More specifically, in the financial sector, the increasingly regulated environment and the lack of updates to regulations are some of the problems that may significantly affect the effectiveness of cybersecurity procedures and may make compliance more problematic and costly. Because cybercriminals are persistent and use advanced techniques, the development of these regulations may not be sufficient to stop them. In the healthcare sector, instead, there seem to be inadequate compliance procedures to communicate understandable privacy practices or provide adequate security safeguards. Communication issues may, therefore, affect the employees' ability to implement security controls accurately and create a false sense of cybersecurity awareness. As for the automation sector, there seems to be a lack of comprehensive regulatory coverage in some industries. However, based on the literature review as well as the overall findings of the comparative analysis, it is noted the automation industry is likely to have a more privileged position in the compliance landscape due to its versatile nature. Despite some issues associated with the novelty of the field, it has the potential to successfully navigate most of the cybersecurity regulatory compliance issues that have an impact on organizations. In addition, being a subject closely related to both safety and cybersecurity, automation can benefit from a broader and more mature regulatory environment.

## Acknowledgements

The research reported herein was supported in part by the Cybersecurity at MIT Sloan initiative, which is funded by a consortium of organizations, and a gift from C6 bank.

## References

Abdullah, N. S., Sadiq, S., & Indulska, M. (2010, June). Emerging challenges in information systems research for regulatory compliance management. In *International Conference on Advanced Information Systems Engineering* (pp. 251-265). Springer, Berlin, Heidelberg.

Adams, S. A., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B. J., Bert, J., Leenes, R., Schellekens, M., E Silva, K., Skorvánek, I. (2015). *The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands, and the UK*. Tilburg University.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management, 6*(4), 279-314.

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2016). The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data. *Journal of Financial Transformation, 44*, 79-86.

Arner, D. W., Barberis, J., & Buckley, R. P. FinTech, RegTech and the Reconceptualization of Financial Regulation'(2017). *Northwestern Journal of International Law and Business, 37*, 371.

Bailey, P. D., Haq, G., & Gouldson, A. (2002). Mind the gap! Comparing ex ante and ex post assessments of the costs of complying with environmental regulation. *European Environment, 12*(5), 245-256.

Bauer, J. M., & Latzer, M. (Eds.). (2016*). Handbook on the Economics of the Internet*. Edward Elgar Publishing.

Bonakdarpour, B., Deshmukh, J. V., & Pajic, M. (2018, November). Opportunities and challenges in monitoring cyber-physical systems security. In *International Symposium on Leveraging Applications of Formal Methods* (pp. 9-18). Springer, Cham.

Bradbury, J. C. (2006). Regulatory federalism and workplace safety: evidence from OSHA enforcement, 1981–1995. *Journal of Regulatory Economics, 29*(2), 211-224.

Breaux, T. D., Antón, A. I., & Spafford, E. H. (2009). A distributed requirements management framework for legal compliance and accountability. *Computers & Security, 28*(1-2), 8-17.

Caldwell, F. & Eid, T. (2007) *Magic Quadrant for Finance Governance, Risk and Compliance Management Software, 2007*. Gartner Inc.

Cojocaru, I., & Cojocaru, I. (2019). *A BIBLIOMETRIC ANALYSIS OF CYBERSECURITY*. Paper presented at Programme CEE e|Dem and e|Gov Days 2019, Budapest, Hungary. doi: 10.24989/ocg.v335.12

Croce, T. (2017). From Bitcoin to the Internet of Things: the role of the Blockchain. *Annali della Facoltà Giuridica dell'Università di Camerino, 6*, 17.

Cuaresma, J. C. (2002). The gramm-leach-bliley act. *Berkeley Tech. LJ, 17*, 497.

Dayabhai, S. (2017). Application vs Security: The cyber-security requirements in a modern substation automation system. *Proceedings of the Southern African Power System Protection and Automation Conference, Johannesburg, South Africa*.

De Guzman, M. L. (2007). Compliance looms over IT security. *Network World Canada, 23*(5), N_A.

Deelman, E., Stodden, V., Taufer, M., & Welch, V. (2019, June). Initial Thoughts on Cybersecurity and Reproducibility. In *Proceedings of the 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems* (pp. 13-15). ACM.

Doganata, Y., & Curbera, F. (2009, September). Effect of using automated auditing tools on detecting compliance failures in unmanaged processes. In *International Conference on Business Process Management* (pp. 310-326). Springer, Berlin, Heidelberg.

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.

Douglas, J. L. (2016). New wine into old bottles: Fintech meets the bank regulatory world. *NC Banking Inst., 20*,17.

El Kharbili, M. (2012, January). Business process regulatory compliance management solution frameworks: A comparative evaluation. In *Proceedings of the Eighth Asia-Pacific Conference on Conceptual Modelling, 130* (pp. 23-32). Australian Computer Society, Inc.

Foorthuis, R. M. (2012). Tactics for Internal Compliance: A Literature Review. Project Compliance with *Enterprise Architecture*, 153-198.

Foorthuis, R., & Bos, R. (2011, June). A framework for organizational compliance management tactics. In *International Conference on Advanced Information Systems Engineering* (pp. 259-268). Springer, Berlin, Heidelberg.

Grandison, T., & Bhatti, R. (2012). Regulatory compliance and the correlation to privacy protection in healthcare. In *Innovations in Data Methodologies and Computational Algorithms for Medical Applications* (pp. 108-124). IGI Global.

Grossman, W. M. (2008). Complying to a false sense of security. *Infosecurity, 5*(7), 24-27.

Hildenbrandt, K., & van Beurden, I. (2019). Integration of Automation Lifecycles: Leveraging Functional Safety, Cybersecurity, and Alarm Management Work Processes. *Chemical Engineering Transactions, 77*, 625-630.

Hornbuckle, R. (n.d.) Security vs. Compliance. Retrieved from http://www.infosecwriters.com/Papers/RHornbuckle_Security_Compliance.pdf

Jenik, I., & Lauer, K. (2017). *Regulatory sandboxes and financial inclusion*. Washington, DC: CGAP.

Joshi V., Patel, R., Adhikari, M., Singh, R., Gehlot, A. (2019). *Industrial Automation*. Delhi, India: BPB Publications.

Kharbili, M. E., Medeiros, A. K. A. D., Stein, S., & van der Aalst, W. M. (2008). Business process compliance checking: Current state and future challenges. In: *Proc MobIS'08*, 107–113

Kingsbury, B. (1997). The concept of compliance as a function of competing conceptions of international law. *Mich. J. Int'l L., 19*, 345.

Kirtley, J. E., & Memmel, S. (2018). Rewriting the Book of the Machine: Regulatory and Liability Issues for the Internet of Things. *Minn. JL Sci. & Tech., 19*, 455.

Kosseff, J. (2016). Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System. *Chap. L. Rev., 19*, 401.

Kosseff, J. (2017). Defining cybersecurity law. *Iowa L. Rev., 103*, 985.

Kosseff, J. (2019). *Cybersecurity law*. John Wiley & Sons.

Kwon, J., & Johnson, M. E. (2011). The impact of security practices on regulatory compliance and security performance. In *Proceedings of the 32nd International Conference on Information Systems*, AIS.

Kwon, J., & Johnson, M. E. (2012). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association, 20*(1), 44-51.

Kwon, J., & Johnson, M. E. (2013, January). Healthcare security strategies for regulatory compliance and data security. In *2013 46th Hawaii International Conference on System Sciences* (pp. 3972-3981). IEEE.

Laprie, J. (2005, July). Resilience for the scalability of dependability. In *Fourth IEEE International Symposium on Network Computing and Applications* (pp. 5-6). IEEE.

Leander, B., Čaušević, A., & Hansson, H. (2019, August). Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (p. 101). ACM.

Lodge M (2004) Accountability and Transparency in Regulation: Critiques, Doctrines, and Instruments. In: Jordana J, Levi - Faur D (eds) *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*, pp. 124–144. Edward Elger, Cheltenham, UK.

Loshin, D. (2010). *The practitioner's guide to data quality improvement*. Elsevier.

Lyons S (2016). *Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program*. Auerbach Publications.

MacLean, T. L., & Behnam, M. (2010). The dangers of decoupling: The relationship between compliance programs, legitimacy perceptions, and institutionalized misconduct. *Academy of Management Journal, 53*(6), 1499-1520.

Mashaw, J. L. (2006). Accountability and institutional design: Some thoughts on the grammar of governance. *Public Law Working Paper*, (116), 115-156.

Mathavi, M. S., Vanitha, D., Jeyanthi, S., & Senthil, P. (2012). The smart home: renewable energy management system for smart grid based on ISM band communications. *International Journal of Scientific& Engineering Research, 3*(3), 1-8.

May, P. J. (2007). Regulatory regimes and accountability. *Regulation & Governance, 1*(1), 8-26.

Millán Anglés, S., Ganah, A., García Santos, A., Jiménez Leube, F. J., & Higuera Rincón, Ó. (2014). Determination of the influence of specific building regulations in smart buildings. *Intelligent Buildings International, 6*(4), 239-254.

Miller, A. R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management Science, 55*(7), 1077-1093.
Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (Vol. 560). John Wiley & Sons.
Mohammed, D. (1970). Cybersecurity Compliance in The Financial Sector. *The Journal of Internet Banking and Commerce, 20*(1), 1-11.
Mohammed, D. (2017). US Healthcare Industry: Cybersecurity Regulatory and Compliance Issues. *Journal of Research in Business, Economics and Management, 9*(5), 1771-1776.
Muckin, M., & Fitch, S. C. (2014). A Threat-Driven Approach to Cyber Security. *Lockheed Martin Corporation.*
Mushkat, R. (2009). Dissecting International Legal Compliance: An Unfinished Odyssey. *Denv. J. Int'l L. & Pol'y, 38*, 161.
Nawar, Y. S., & Dagam, O. V. (2015). Organisational Culture Perspective. *Practice, 2*(4).
Oltsik, J. (2011). The ESG Information Security Management Maturity Model. *Enterprise Strategy Group, Milford, Massachusetts.*
Packin, N. G. (2018). RegTech, compliance and technology judgment rule. *Chi.-Kent L. Rev., 93*, 193.
Panitz, J. C., Wiener, M., & Amberg, M. (2011, October). Factors facilitating compliance implementation case study results from multinational enterprises. In *ECIS* (p. 3).
Paul, S., & Rioux, L. (2015). Over 20 Years Of Research Into Cybersecurity And Safety Engineering: A Short Bibliography. In *Safety and Security Engineering* (Vol. 5, pp. 335-349). WIT Press.
Pererva, P. G., Kosenko, O., & Tkachov, M. (2017). Compliance Program of An Industrial Enterprise: The Essence and Content. In *Mérleg és Kihívások" X. Nemzetközi Tudományos Konferencia*, 87-93
Pupke, D. (2008). *Compliance and corporate performance: the impact of compliance coordination on corporate performance*. BoD–Books on Demand.
Regens, J. L., Dietz, T. M., & Rycroft, R. W. (1983). Risk assessment in the policy-making process: environmental health and safety protection. *Public Administration Review*, 137-145.
Romzek, B. S., & Dubnick, M. J. (1987). Accountability in the public sector: Lessons from the challenger tragedy. *Public Administration Review, 47*(3), 227–238
Romzek, B.S., Ingraham, P.W. (2000) Cross Pressures of Accountability: Initiative, Command, and Failure in the Ron Brown Plane Crash. *Public Administration Review, 60*, 240–253.
Scott, C. (2000) Accountability in the Regulatory State. *Journal of Law and Society 27*, 38–60.
Scully, T. (2011). The cyber threat, trophy information and the fortress mentality. *Journal of business continuity & emergency planning, 5*(3), 195-207.
Shen, J.J., Samson, L.F., Washington, E.L., Johnson, P., Edwards, C. and Malone, A. (2006) 'Barriers of HIPAA regulation to implementation of health services research', *Journal of Medical Systems, 30*,(1), 65.
Smith, K. (1992). *Environmental Hazards: Assessing Risk and Reducing Disaster*. Routledge, London
Smith, R. (2013). *Compilation of state and federal privacy laws.* Providence, RI: Privacy Journal.
Tattam, D. (2017). *Short Guide to Operational Risk.* Milton: Taylor & Francis.
Thaw, D. (2013). The efficacy of cybersecurity regulation. *Ga. St. UL Rev., 30*, 287.
Trivedi, K. S., Kim, D. S., Roy, A., & Medhi, D. (2009, October). Dependability and security models. In *2009 7th International Workshop on Design of Reliable Communication Networks* (pp. 11-20). IEEE.
Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of manufacturing systems, 47*, 93-106.
Usnick, L. E. E., & Usnick, R. (2013). Compliance program auditing: The growing need to insure that compliance programs themselves comply. *Southern Law Journal, 23*, 311.
Warkentin, M., Johnston, A., & Adams, A. (2006). User interaction with healthcare information systems: Do healthcare professionals want to comply with HIPAA?. *AMCIS 2006 Proceedings*, 326.
VanLengen, C. A. (2008). What should IS majors know about regulatory compliance? Working paper series--08-12.
Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review, 32*(5), 715-728.
Wells Jr, J. W. (2013). Commitment, Ethics & Compliance: A Look at Perceptions in the SH&E Profession. *Professional Safety, 58*(09), 62-68.
Wright, C. (2014). *The IT Regulatory and Standards Compliance Handbook*. Burlington: Elsevier Science.
Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications, 7*(1), 5.