A Culture of Cybersecurity at Banca Popolare di Sondrio

Angelica Marotta and Dr. Keri Pearlson*

March 1, 2019

Abstract

Today, cybersecurity is no longer just a technical issue to be solved by the IT department. Organizations of all sizes are constantly breached or attacked, and the best defense is both technical and organizational. Business leaders, working alongside technology leaders, need tools and frameworks for building cyber resilience using multiple layers of security. Financial institutions are at particular risk and the consequences of a cyber incident can be far-reaching and devastating. This paper describes how one bank built a culture of cybersecurity to create values, attitudes and believes that drive cybersecure behaviors. The case study illustrates how cybersecurity leaders at Italian bank, Banca Popolare di Sondrio (BPS) motivated, built and measured success of efforts to create a culture of cybersecurity.

Introduction

Cybersecurity is no longer just a technical issue to be solved by an organization's IT department. The impacts of cyber breaches and exploited vulnerabilities impacts all business sectors, affecting everything from security to business development in organizations around the world. Cybercrime has evolved from the activity of a restricted number of fringe hackers trying to break into systems to to an ecosystem of service offerings on the dark web that any unscrupulous business person can access for profit, mischief or to disrupt, or worse, damage a business enterprise. The impacts are felt in public, private and even individual lives.

The current cyber environment is a domain characterized by boundless criminal activities that affect many different business units and functions, but especially so in the financial services sector. As one of our colleagues is fond of saying, "criminals go where the money is, and that's the financial services sector." Lagazio, Sherif, and Cushman (2014) focus on this phenomenon in the financial sector. They provide a definition of cybercrime as "all cyber activities that support crime in any of its aspects, while also emphasizing how the Internet has transformed traditional crimes and grown them to a much larger scale."

The financial industry is multifaceted, and the banking sector in particular is one of the most tempting and recurring targets for cybercriminals. According to a Bitdefender survey of over 118 companies, 47.5% of financial institutions were breached in 2018 and 58.5% have experienced an advanced attack or seen signs of suspicious behavior in their infrastructure (Pascu 2018). In one of the most notorious cybersecurity incidents, JPMorgan Chase, one of the world's biggest banks, was the victim of a cyber-attack that compromised the data of approximately 76 million households and 7 million small businesses (Silver-Greenberg et al. 2014). Thus, as banks increase the use of digital services, such as Internet and mobile banking, the number of threats aimed at assets and customers' personal information increases. But managers can play a role in reducing the vulnerabilities at their bank by building a culture of cybersecurity.

With appropriate behaviors, principles, values, norms, and skills, organizations can greatly minimize their chances of suffering severe cyber-attacks. To explain how this approach can be applied in practice, we describe how Banca Popolare di Sondrio (BPS) has created a culture of cybersecurity, which improved the organization's ability to guard against cyber threats. This paper helps add to the literature on cybersecurity practice in three ways. First, it provides an example of how an organization created this type of culture and highlights cybersecurity practices within a real-life context of an Italian bank. Second, it examines the ways in which security and trust work together to build a holistic approach to cybersecurity. Finally, it offers an

* The authors are grateful to Banca Popolare di Sondrio and Milo Gusmeroli, Giampiero Raschetti and other executives of the Bank for their support of this research. This research was sponsored in part by Cybersecurity at MIT Sloan, https://cams.mit.edu. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

in-depth analysis of a sample cybersecurity metrics used by one organization to determine factors leading to the success of an organization's cybersecurity.

Cybersecurity Culture

Culture is central to all aspects of organizational life, even in organizations where cultural values seem to receive little attention. An organization's culture is the unwritten rules that guide behaviors of all team members. The way executives and employees think, feel, evaluate, and act is guided by values, attitudes, and beliefs which make up the culture and is shared across organizational units. Analyzing the culture of an organization means assessing the organization's structure, management choices, strategic goals, and the employee conduct. Furthermore, since culture is often created and managed by the leaders of an organization, culture and leadership are two sides of the same coin. According to Schein (1985), the most important task of the leader consists of creating the company culture. Consequently, knowing how to manage the culture is an essential talent for a leader.

Schein (1985) defined organizational culture in the following way:

> "A pattern of shared basic assumptions that a group learns as it solves its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems."

Here, Schein's foundational work underpins much of what is known about organizational culture. For example, several scholars, such as Kreps (1990) and Van de Steen (2010) built their theories around Schein's work. Kreps views culture as an adaptive environment that changes according to various unforeseen contingencies (Kreps 1990). Van de Steen, instead, proposes an interpretation of Schein's definition which focuses on the processes that determine the creation of a homogeneous organizational culture (Van de Steen 2010). Organizational culture is hard to define but the majority of theorists and investigators (Beckhard 1969; Crémer 1993; Martinez et al. 2015) agree that it is an important tool for achieving company objectives.

While these theories can be applied to all types of organizations and cultures, according to Huang and Pearlson (2019), the concept of cybersecurity culture requires additional analysis of both the components that form the culture and the factors that influence the culture:

> "Organizational cybersecurity culture is the beliefs, values, and attitudes in the organization that drive cyber-secure behaviors. These beliefs, values, and attitudes are influenced by both external factors outside of the organization and by mechanisms and actions managers can take inside the organization."

The case study described in this paper used this definition to study cybersecurity culture. Huang and Pearlson (2019) describe a cultural system that links employee behavior to culture and the managerial and external factors that influence culture (Figure 1). Culture and managerial mechanisms are reciprocally influenced. Likewise, behaviors and culture have a bidirectional relationship. Managers have control over a number of factors that influence culture, but external influences outside of the manager's direct control, such as national or regional culture, industrial sector regulations, and activities of peer organizations also have a direct impact on the culture.

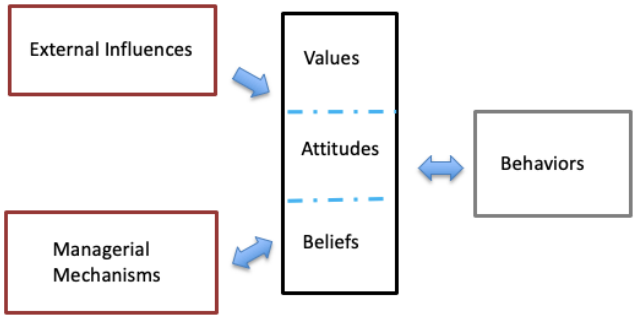

Figure 1. Huang and Pearlson Model of Cybersecurity Culture

Case Study

To illustrate the components of the model described in the previous section, we conducted a case study of an Italian bank, Banca Popolare di Sondrio. We collected the data for this case study through in-depth interviews with C-suite members, including the CIO and the CISO, and employees from different areas, including marketing and audit. Additionally, we used information from publicly available resources about the bank. In the following sections, we describe the case study, starting with the regulatory and organizational context in which BPS operated. We continue by illustrating the components of their cybersecurity culture using examples and stories. Then we present an overview of the role of trust within the Bank. Finally, we outline some of the cybersecurity metrics they used to ensure the efficiency of their cybersecurity and business functions.

Background: Banking Industry

Banks are subject to some of the highest standards available for cybersecurity. Banks control the flow of money in every sector, and hold individual and company financial assets. Managers and individuals expect their bank to keep their money safe, and banks spend significant resources on physical, and now cyber, security to live up to this expectation. Security is not just a business feature of a bank, it's a competitive necessity. No client would trust a bank that was not secure and in many real cases, the fall of a bank would have major consequences not only for those whose assets were under the care of the fallen bank, but potentially to the entire financial network. Keeping banks secure is both a managerial and a governmental priority.

Governments and regulators understand the implications of security breaches, and have set up some of the most stringent cybersecurity-related rules and regulations for financial services organizations. In Europe, the Network and Information Security Directive (NIS-D) was one of the most important steps taken by the European Union to strengthen cybersecurity and establish rules for critical service providers including banking and financial infrastructures. Another impactful regulation was the second Payment Services Directive (PSD2), which specifically focused on financial services by introducing security requirements to regulate payment services throughout the European Union. A more widely applied regulation, the General Data Protection Regulation (GDPR), not only set up guidelines, but specify consequences and fines for non-compliance. This has been a catalyst for cybersecurity measures for all industries, including banks, who have modified their business activities in order to comply. These regulations require banks to take action, such as measuring and tracing cyber events, defining processes and audits, classifying events, and monitoring parameters that exceed certain thresholds. Generally, these activities involve a series of dialogues between banks and supervisory authorities. For example, the ECB (European Central Bank), the Bank of Italy, and the Data Protection Authority have key roles in ensuring that supervised banks effectively address cyber risks for Italian banks.

Italy-based Banca Popolare di Sondrio (BPS) is an Italian banks subject to these regulatory and supervisory systems. Founded in 1871 as a small bank in the Italian Alps, BPS has grown significantly. In 2018 BPS employed more than 2,700 people and had more than 340 branches in Italy and Switzerland. BPS services a wide range of customers including families, professionals, small and large companies, and public institutions, according to their website. Services also cover a wide variety of banking, financial, and insurance services and promote prestigious cultural initiatives. BPS conducts its business following three fundamental values: customer centricity, trust, and efficiency. Their business model operationalized these values by keeping a "local bank feel." In 2018 they remained committed to the principles of local banking, despite having grown into a large organization with many clients.

Milo Gusmeroli, Vice President and Chief Information Officer (CIO) at Banca Popolare di Sondrio, was charged with driving significant transformation of the bank's business operations. In 2018, his top priorities included enhancing cybersecurity defenses, implementing new business models, and dealing with new regulatory requirements.

In order to accomplish some of his strategic objectives, Milo relied upon the bank's Chief Information Security Officer (CISO), Giampiero Raschetti, and internal auditor Sergio Tagni for support and risk evaluation. The rapidly evolving nature of cyber threats meant that Giampiero and Sergio had a number of

key cybersecurity responsibilities including responding to breaches, ensuring the effectiveness of cybersecurity controls, and assessing cybersecurity risk.

Milo's leadership style incorporated a holistic approach to managing his organization. He believed his role was to articulate a clear vision about managing cybersecurity to every business unit within the bank. His vision was that cybersecurity was everyone's responsibility. To ensure his organization was as cyber resilient as possible, he wanted all bank employees to share this vision and make it an essential part of their daily working activities. The bank invested a significant amount of time and resources to build a cybersecure infrastructure. Achieving increased resilience, however, required Milo and his colleagues to build a culture in which every employee took responsibility for reducing cyber risk, promoting teamwork, and creating a cybersecurity mentality.

Building a Culture of Cybersecurity at the BPS

The senior leader responsible for developing a cybersecurity culture was Milo himself, in his role as the CIO. Five core factors were the basis for their cybersecurity culture: responsibility, motivation, individual participation, CIA-approach, and change management.

Responsibility

Since cybersecurity impacted every aspect of the bank's supply-chain, each team, from executive management to internal audit and frontline employees, had responsibility for aspects of cyber defense. As shown in Fig.2, responsibility for cybersecurity was distributed among four major organizational levels: senior-level executives, security executives, general managers, and general employees.

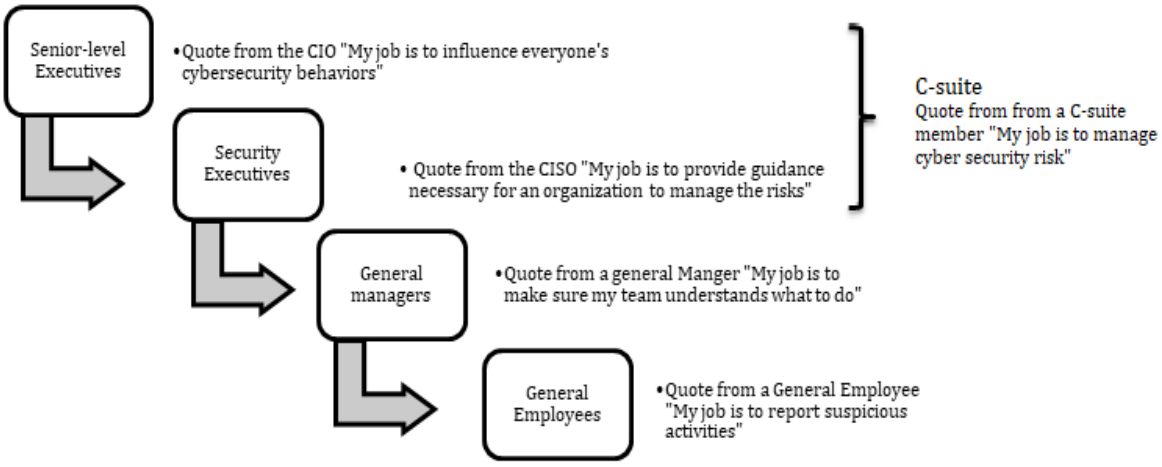

Figure 2. Levels of Cybersecurity Responsibility

This distribution ensured that the defined roles and competencies were appropriate for each organizational level. At the highest organizational level, executives were responsible for the management, implementation, and applicability of technologies as well as setting policies and practices for employee behaviors. Security executives were responsible for security management and governance. Security management meant managing multiple layers of security, also called defense in depth, as shown in Fig. 3. Security professionals also provided guidance on organizational activities that would influence the cybersecurity values, attitudes and beliefs of employees.

Defense in Depth: Layers of Security	
Categories	**Examples**
Security vulnerabilities and risks	Assessing vulnerabilities, evaluating the level of risk associated with each vulnerability
Front management security	Managing customer issues, reporting cyber activities
Logical security	Password access, authentication activities
Operational security	Identifying potential threats, analyzing and monitoring online behaviors
Application development security	Testing, implementation activities
Security incident management	Identifying incidents, managing escalations
Security defense management	Assessing defense capabilities, enhancing operational preparation

Figure 3. Security Layers at Banca Popolare di Sondrio

Looking at security management through the lens of these layers gave executives a way to better evaluate issues. The CISO, for example, was the executive with responsibility over all of these layers. That gave him significant influence over the allocation and management of technology resources to ensure secure operations. General managers within the bank had a key role in ensuring that team members were able to understand organizational cybersecurity objectives and long- and short-term consequences. This layer helped individual employees do the right thing at the right time to help keep the organization secure, and held individuals accountable for their behaviors. Barbara Martinelli, an employee in the marketing area, shared a story about her experience working in a team tasked with finding a way to distribute products via third-party platforms. She commented,

> "The marketing team's business idea was to allow our customers to access third-party sites from their home banking page to learn more about the bank's products. However, when we started discussing this solution with the IT department, this idea didn't seem viable because of data security issues associated with procedures such as our registration processes where issues such as credential management, data transfer systems, standards, and certificate management could compromise security. This was a new perspective for us. Our marketing team joined with our IT department on this project, and that made it possible to understand needs and find a compromise."

Finally, general employees were responsible for cybersecurity awareness and alerting managers if they saw something suspicious. Because employees used the bank's systems every day, Giampiero believed they had an essential role in ensuring security.

Motivation

Because employees represented a fundamental line of cyber defense, executives were often focused on keeping people motivated to behave in ways that promoted stronger cybersecurity regardless of their background and role. Employees were motivated to report suspicious email and behaviors because they wanted to play an important part in keeping customers satisfied and safe. In addition, they felt empowered to do something to keep the bank secure and that motived them to action.

There were many ways employees could help keep the organization safe. Reporting anomalies was one of the most common activities that employees did to keep the bank cyber-safe. Employees had two dedicated e-mail addresses they could use to report any type of problem (for example, they could report a suspicious email or anomalous user behaviors). These sensitized and empowered frontline employees who received emails and other messages from customers and others outside the Bank.

Individual participation

Individuals were empowered to take action. Managers coached them and the security professionals encouraged and provided guidance on what individual employees could do. For example, if an attacks or

identity/data thefts occurred, employees cooperated by sharing information and internal knowledge. Everyone felt they had a clear understanding of their role in creating a cybersecurity culture. Employees knew that making the bank cyber secure was a collective challenge and they willingly participated.

The Confidentiality-Integrity-Availability (CIA)-based approach

Trained employees with the appropriate credentials carefully managed customers' information, such as their financial needs or asset situation. Part of the training for these employees was based on the well-known cybersecurity principles of confidentiality, integrity, and availability (also known as the CIA Triad Model) (Agarwal and Agarwal 2011). Part of the CISO's strategy was incorporating these principles in the Bank's cybersecurity culture. According to Giampiero, all three of the CIA components were required to ensure that the right people accessed customer information (confidentiality), that the bank had appropriate processes in place to test the accuracy of information (integrity), and that the bank prevented any loss of data (availability).

Change management

Advancements in digital technologies and new regulations led to transformations in how the bank operated and how employees did their work. The introduction of GDPR, for instance, forced employees to pay more attention to how they handled sensitive customer information. However, like many, bank employees often resisted change unless they were part of the process to create the change. Making sure employees did what was necessary for both business and cybersecurity objectives was a primary responsibility of both the CIO and the CISO. For example, BPS leaders placed restrictions on accessing social networks, such as Facebook, for security and productivity reasons. As expected, some employees resisted this change. In some cases, such as marketing, team members used these sites to reaching customers and their work was impacted by the restriction. Others were simply unhappy to no longer have this access during their workday. Simply banning access to social networks may have been good for security reasons but managers were forced to be more thoughtful in their change management plans to find creative solutions to keep team members productive.

The Role of Trust at the Banca Popolare di Sondrio

No bank can succeed without the trust of its customers. If building and maintaining trust was fundamental to BPS's strategy, a cybersecurity breach would undermine it. BPS executives understood this and worked hard to be trustworthy. In particular, the Bank built trust on three levels, as shown in Figure 4.

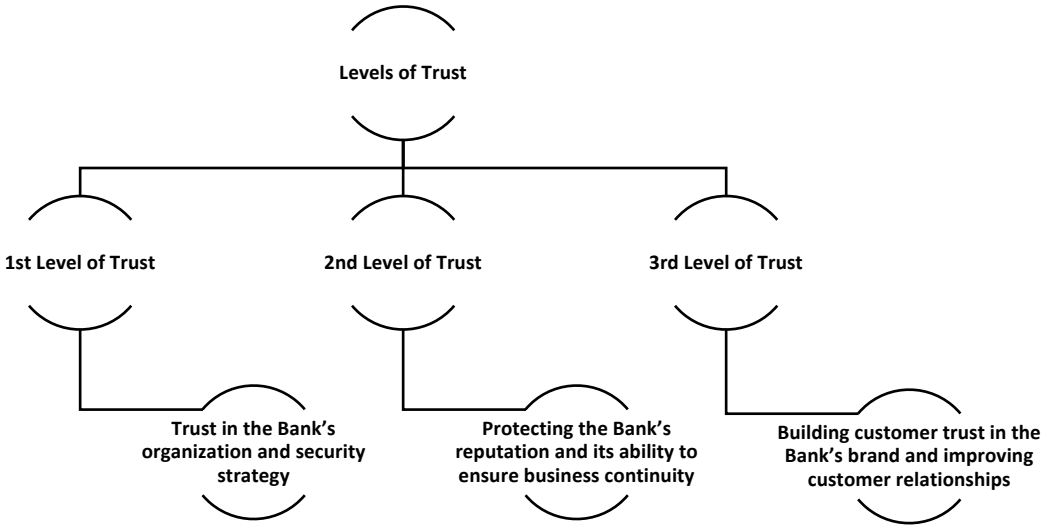

Figure 4. Levels of Trust

Organization and Security Strategy

Banks need to provide a secure place to manage money and assets on their customers' behalf. The **first level of trust** was to build trust in the bank's organization and security strategy. Milo believed that the essential elements of trust and security went hand-in-hand. Milo explained,

> "Nobody would trust a bank that is not secure. Therefore, trust and security represent two essential elements that are often intertwined. Whether it is a cybersecurity issue or physical security threat, the most important thing is providing guarantees in terms of agility, speed, and user experience. For example, customers are more willing to take extra steps to access their online account if it means minimizing the possibility of a cyber-attack and losing their money."

Bank Reputation

The **second level of trust** was based on the bank's reputation and the expectation set to ensure operations and maintain its essential functions over time. To achieve this, leaders were forced to accept that guaranteeing 100% secure operations was impossible. Building the bank's reputation was based, in part, on how the bank responded to incidents. Milo shared one story:

> "A customer once reported that his cash card became non-operational after typing the PIN number on the automatic teller machine (ATM) screen. We immediately suspected something was wrong. As a consequence, the bank immediately stopped the machine from operating and prevented other customers from using it. In addition, they monitored and blocked all the PIN numbers that had been used at this ATM during the past half an hour. When we dug deeper into the machines' logs, we noticed that these machines were operative during particularly unusual periods, and we found evidence of a partition used by third parties to monitor memory activity/usage. We diagnosed that this was actually a cloning activity, and some information may have been compromised. We were able to contain this issue before any damage was done. But if this happened again, trust and reputation would suffer, and customers might lose confidence in the bank's ability to keep their financial information secure."

Customer Expectations and Relationships

The **third level of trust** was to build customer trust in the bank's brand through improving customer relationships. Executives at the BPS thought of trust as the basis of any interaction between employees and customers. Translating the bank's cultural values, such as transparency, into activities that customers could see, such as sharing information, was one way BPS managed expectations and customer relationships. Giampiero shared his perspective on customer trust,

> "Trust begins when customers entrust the bank to keep their savings and increases over the years. Trust is built through attentiveness, preparation, and speed of answer. Additionally, the fact that the bank is aligned with regulatory systems provides customers with guarantees."

Measuring Cybersecurity: How Do They Know They Are Secure?

When the European Central Bank (ECB) released a self-assessment questionnaire in 2015, the CISO and his team used this opportunity to discuss the importance of measuring security. One question, "What is the degree of maturity of your security systems?", caused them to reevaluate the way they thought about cybersecurity management. Giampiero believed the best way to answer this question was to use a reference model, which provided different levels of maturity and a language for discussing cybersecurity management, to make a comparison. They chose the NIST framework as a way to assess, measure, and benchmark their security level (National Institute of Standards, 2019). Bank leaders decided to use this framework further, as a tool to analyze the security maturity of their suppliers, and to evaluate other critical security points in their business ecosystem. This approach became their starting point for creating metrics for cybersecurity and vulnerability management.

Measuring and Assessing the Impact of Vulnerabilities and Incidents

The CISO and the CIO measured the performance and effectiveness of the bank's vulnerabilities in a number of ways. For example, they performed periodic analysis of risk factors in their systems. These analyses enabled IT specialists to consider the potential effects that cybersecurity risks could have on the bank's objectives and what was required to manage or mitigate them. This type of analysis was done by both audit experts and penetration testing experts to get a more well-rounded image of risk factors. One risk factor was how frequently and effectively system patches were applied. While system patches were a frequent occurrence and difficult to keep current, patches increased the security and reduced or eliminated a vulnerability in a system. Giampiero explained the importance of a robust patching process:

> "Updating patches of the most vulnerable applications may prevent potential attacks. Failure to update means being exposed to risks and therefore being more vulnerable."

Other metrics analyzed cybersecurity incidents and system malfunctions. These were among the most useful measures used by bank leaders. A sophisticated incident management system based on the concept of "analysis by process" was used to monitor the layered IT infrastructure. The analysis began with an initial assessment of the actual and potential cybersecurity incidents that impacted bank processes and services. This assessment was then followed by a deeper evaluation of the Bank's infrastructure and the behaviors of their team members, if necessary. Incidents were analyzed and classified, increasing the quality of data and allowing security experts to identify and predict trends. Predicting peaks or troughs associated with these categories allowed leaders to more effectively plan cybersecurity improvements and to keep managers and general employees vigilant and aware of potential threats.

When communicating with their Board of Directors, cybersecurity leaders found that periodic (quarterly) analysis of cybersecurity information was useful. The board was briefed on metrics about incidents, cyber-events, threat evolution, countermeasures, organizational behaviors and tracking procedures as a way to assist with risk management. They used these metrics to for strategic planning and evaluating IT operations.

Measuring the Success of Cybersecurity Culture Initiatives

The CIO and CISO continued to work on the best ways to answer the question "how secure are we?" using their standard business frameworks such as the balanced scorecard and business relationship management metrics. But a key component to answering this question was to find a way to measure the success of cybersecurity culture initiatives. The reports focused on the most problematic applications and systems, giving Giampiero insight into where to spend resources to increase security. In addition, the bank observed trends over time, and these gave indications of the success of the cybersecurity culture initiatives. Giampiero explained:

> "The easiest way to measure success of our cybersecurity plans was to measure the results of our processes, the number and impact of incidents, and the way we manage fraud. Fraud management means analyzing the number of fraud incidents, ways we have contained and controlled them, and the interventions we have done. Interventions are identified by comparing and contrasting before and after states, to understand what the impact has been, and then creating mechanisms to address them. We then report out how the fraud occurred, how we recognized it, what indicators were used, and what mechanisms we used to mitigate it. We can then assess the success/failure metrics, and this indicates effectiveness of the Bank's interventions. This all becomes part of our cybersecurity incident reports."

Multiple assessments and methods were used to track the maturity of the Bank's cybersecurity culture over time to ensure strategic goals and regulations' requirements were met. Using traditional management tools such as ongoing planning, reviewing, monitoring, auditing, and information sharing, at all levels of the bank, highlighted the continuing cybersecure behaviors of employees and encouraged leaders that their initiatives were working.

Discussion and Conclusion

Executives at Banca Popolare di Sondrio (BPS), like every bank in the financial sector, noticed increased cybercriminal activity as they increased their use of digital services. In response, executives made cybersecurity a strategic priority. However, leaders faced challenges in deciding on what to prioritize and how to properly deploy resources. Building a culture of cybersecurity in which each employee of the bank knew what to do to keep the Bank's information and systems secure was fundamental to their plan.

At the end of 2018, the initiatives to increase cybersecure behaviors seemed to be working at BPS. However, there was still work to be done. The toughest challenge facing the leadership team continued to be managing change, in particular, how to help employees understand the value and importance of introducing new cybersecurity policies. Executives were working on ways to strengthen collaboration between their employees and their leaders, and constantly seeking ways to increase awareness of the need to be secure.

This case study presents an important example for managers to utilize in building their organization's cybersecurity culture, and suggests ways to define objectives of investments to create cybersecurity culture program. For example, one of the key outcomes that emerged from this research is that, in order to build an effective cybersecurity culture, it is necessary to influence people and create a solid and effective human firewall. To achieve this goal, BPS focused on the following:

- Creating a network of technical employees to assist all teams with learning more about cybersecurity and motivating them to exhibit the right behaviors;
- Implementing consequence management, which involved regularly reinforcing cybersecurity behaviors and holding people accountable to expectations;
- Implementing mechanisms for building and retaining trust.

Another important consideration is that cybersecurity and business issues were treated in a unified manner at BPS. The alignment between business needs and cybersecurity needs evolved over time. For example, the role of the CISO evolved from being focused solely on the security structure of the organization to supporting a holistic approach. He gradually embraced two main functions: the first was to look after cybersecurity projects, the second was new, and included strategy, policy, and governance, as well as cooperating and interacting with external regulators. This sent a clear signal throughout the Bank's units that cybersecurity is not at odds with business, but enables it, and should be viewed as an important business responsibility.

BPS, like all banks and like many other organizations, needed to be sure every employee was an active, integral part of their cybersecurity defenses. Building a cybersecurity culture was the primary approach their executives used to drive values, attitudes and beliefs in the importance of security as part of just being employed by BPS. Other organizations can use this case to drive similar behaviors in their organization.

REFERENCES

Agarwal, A., Agarwal. A. 2011. "The Security Risks Associated with Cloud Computing," *International Journal of Computer Applications in Engineering Sciences* (1), pp. 257-259

Beckhard, R. 1969. *Organization development: Strategies and models,* Reading, MA: Addison-Wesley.

Camillo, M. 2017. "Cybersecurity: Risks and management of risks for global banks and financial institutions," *Journal of Risk Management in Financial Institutions* (10:2), pp. 196-200.

Crémer, J. 1993. "Corporate Culture and Shared Knowledge," *Industrial and Corporate Change* (2:3), pp. 351-386.

Huang, K., and Pearlson, K. 2019. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pp. 6398-6407.

Kreps, D. M. 1990. "Corporate Culture and Economic Theory," in *Perspectives on Positive Political Economy*, J. E. Alt and K. A. Shepsle (eds). Cambridge, Cambridge University Press, pp. 90-143.

Lagazio, M., Sherif, N., and Cushman, M. 2014. "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Computers and Security* (45), pp. 58-74.

Martinez, E. A., Beauliez, N., Gibbons, R., Pronovost, P., and Wang, T. 2015. "Organizational Culture and Performance," *American Economic Review* (105:5), pp 331-335.

National Institute of Standards. 2019. "Five Functions." *NIST*. (available at https://www.nist.gov/cyberframework , accessed February 26, 2019).

Pascu, L., 2018. *Top Security Challenges for the Financial Services Industry in 2018*, Bitdefender. (available at https://www.bitdefender.com/files/News/CaseStudies/study/240/Bitdefender-Top-Security-Challenges-for-the-Financial-Whitepaper-EN-interactive.pdf, accessed February 26, 2019).

Schein, E. H. 1985. *Organizational culture and leadership*, San-Francisco: Jossey-Bass Publishers.

Silver-Greenberg, J., Goldstein, M, Perlroth, N. 2014. *JPMorgan Chase Hacking Affects 76 Million Households*, New York Times. (available at https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ accessed, accessed February 26, 2019)

Van den Steen, E. 2010. "On the origin of shared beliefs (and corporate culture)," *The RAND Journal of Economics* (41:4), pp. 617-648.