Addressing the Complexities of Cybersecurity at Fintech Enterprises

Former US Federal Bureau of Investigation (FBI) Director Robert Mueller once said, "There are only two types of companies: those that have been hacked and those that will be."[1] But this sentiment may be outdated. Consider instead that there are two types of enterprises: those that have been hacked (knowingly or unknowingly) and those that will be hacked in the future. An organization may not immediately realize it has been a victim of a cyberattack. There are many cases in which a cybercriminal breaches an organization's infrastructure and remains undetected for a considerable length of time.

For several years, the average time of data breach detection was more than 200 days.[2] The most recent data demonstrate that in 2021, the average time of data breach detection was 287 days,[3] including the time needed for containment (approximately 80 days). These numbers show that discovery of sophisticated cyberattacks is still a challenge for most enterprises, including financial institutions.

For example, in February 2016 , a cyberattack occurred at the Central Bank of Bangladesh that was so massive it threatened the financial stability of the entire country and forever changed the cyberlandscape for the financial industry around the world.[4, 5] Access to the bank's network was established in December 2015 and reconnaissance probes were conducted including monitoring of system usage for more than a month to observe the daily SWIFT usage patterns and activity during normal business hours. Credential theft was tested and conducted during this period.[6]

Although in recent years there has been a significant increase in the number of cyberattacks targeting critical infrastructure (e.g., healthcare, education, energy), the financial industry has always been and likely always will be one of the most alluring targets for cybercriminals. Banks and other financial institutions, both individually and together as parts of the financial ecosystem, face the serious challenge of coping with the acute risk posed by the contemporary digital world. Many small, medium and large fintech enterprises are not ready to mitigate modern cyberrisk.

The University of Hong Kong (Pok Fu Lam, Hong Kong) Professor Douglas W. Arner once noted the "[Rapid] growth of [fintech] companies from 'Too small to care' to 'Too large to ignore' to, finally, 'Too big to fail.'"[7] Although some financial system regulators may not initially pay much attention to fintech organizations, they can no longer ignore enterprises that have gained momentum. Fintech

KOMITAS STEPANYAN | PH.D., CRISC, COBIT FOUNDATION, CRMA

Is the deputy director of corporate services and development at the Central Bank of Armenia where he leads several key functions including IT, cybersecurity, business continuity management, project management and service quality control. He also assists the International Monetary Fund (IMF) and the World Bank as a short-term expert for cyberrisk management, regulation and supervision. Stepanyan has led several technical assistance and capacity-building missions for a diverse range of countries. He has more than 20 years of experience in internal audit, IT audit and information/cybersecurity. He has been a speaker at many international events around the world.

organizations can become significant players impacting the entire financial system, and regulators cannot afford to let them fail.

It is critical that central/national banks do their part to address such risk through timely regulation and supervision and that organizations do their part by prioritizing good governance and cybersecurity awareness.

Good Governance for Good Cybersecurity

Effective IT governance is the cornerstone of cybersecurity as it is about leadership: how leaders treat IT as a cost-center vs. as an enterprisewide strategic asset. Governance is made more complex for central banks and regulatory and complex supervisory authorities due to regulation, supervision and compliance. There are many global models, frameworks and standards that can be referenced for complete cybersecurity governance and management, but ultimately, a mature organization chooses its own preferred guidance. The US National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF),[8] the US Federal Financial Institutions Examinations Council (FFIEC) Cybersecurity Assessment Tool,[9] the International Organization for Standardization (ISO) standard ISO 27000[10] and COBIT®[11] are valuable resources for effective IT governance. These frameworks clearly describe roles and responsibilities of top management, importance of IT strategic alignment to achieve the enterprise objectives, importance of leadership and top management support to address IT and cybersecurity issues, importance of effective IT risk management, and proper reporting strategies.

For example, ISO 27001 has been used by many financial organizations for years, but questions have been raised surrounding its effectiveness. ISO 27001 is a management standard, so its practical effectiveness is dependent on the perception of an organization's top management. However, some people consider it a technical standard and argue that mere ISO 27001 certification is not enough to keep the organization safe and secure. ISO 27001 has many requirements, and the implementation and effective maintenance of these requirements are highly dependent on the maturity of the enterprise. Enterprises can be ISO 27001-compliant and yet never have had a professional IT audit. This is an issue because IT audit is an essential component of IT governance. Without an independent, professional IT audit review, top management cannot be assured that information security-related risk is properly managed.

Many top managers do not differentiate information security and cybersecurity and therefore do not realize how to properly address both.

The FFIEC Cybersecurity Assessment Tool is another helpful tool. However, it was designed for the US market, so using the FFIEC Cybersecurity Assessment Tool in other jurisdictions without proper localization can provide incorrect results.

The NIST CSF is a powerful tool to organize and improve an organization's cybersecurity program. It is a set of guidelines and best practices to help organizations build and improve their cybersecurity postures. The framework provides a set of standards and recommendations that enable organizations to be better prepared to respond to cyberattacks.

COBIT is a comprehensive framework for enterprise governance of information and technology. In most cases, IT professionals use highly technical language, while top management tend to think about business issues. COBIT can help fill this gap between top management and IT professionals and guide them to communicate using the same language.

Cybersecurity vs. Information Security and Why It Matters

Different frameworks can be used to address information security and cybersecurity; however, many top managers do not differentiate information security and cybersecurity and therefore do not realize how to properly address both.

Although both cybersecurity and information security are based on the well-known confidentiality,

LOOKING FOR MORE?

- Read I*mplementing the NIST Cybersecurity Framework Using COBIT® 2019. www.isaca.org/implementing-nist-cybersecurity-framework-using-cobit-2019*
- *Learn more about*, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

integrity and availability (CIA) triad, the vast majority of professionals prefer to use the term cybersecurity even when referring to what is technically information security, believing it sounds more modern. However, cybersecurity refers to mitigating risk that threatens digital assets, including data, that spreads through digital channels (i.e., over the Internet), while information security refers to risk that threatens assets, including information that is not necessarily in a digital format. Cybercriminals can steal data that do not inherently possess a logical meaning. In other words, the data would not be considered information and, at first glance, would not be usable. However, from a cybersecurity point of view, the data could still be used for planning or execution of attacks.

The Changing Threat Landscape

Institutions of all kinds, but especially central banks, must maintain cyberrisk awareness 24/7. Modern organizations use various digital devices (e.g., computers, tablets, smartphones, smart devices and Internet of Things [IoT] devices) to receive or provide digital services.

The number of IoT devices worldwide is projected to exceed 15 billion by 2025 and 25 billion by 2030 (**figure 1**).[12] The digital world is far from perfect, and vulnerabilities appear and are discovered every day, even in devices and programs from reputable manufacturers and service providers. The complexity of the problem is obvious, and it does not have a simple solution.

The mass shift to remote working brought on by the COVID-19 pandemic in March 2020, exacerbated this complexity. Before COVID-19, organizations conducted business in their respective office buildings, where many hardware and software solutions were mostly protected from cybersecurity risk and attack prevention was mostly effective. But throughout the COVID-19 pandemic, employees have been able to work from virtually anywhere. Because many organizations lack sufficient resources to equip their employees, they allow them to work on their own devices without enforcing an effective bring-your-own-device (BYOD) policy or putting effective mechanisms in place to manage risk.

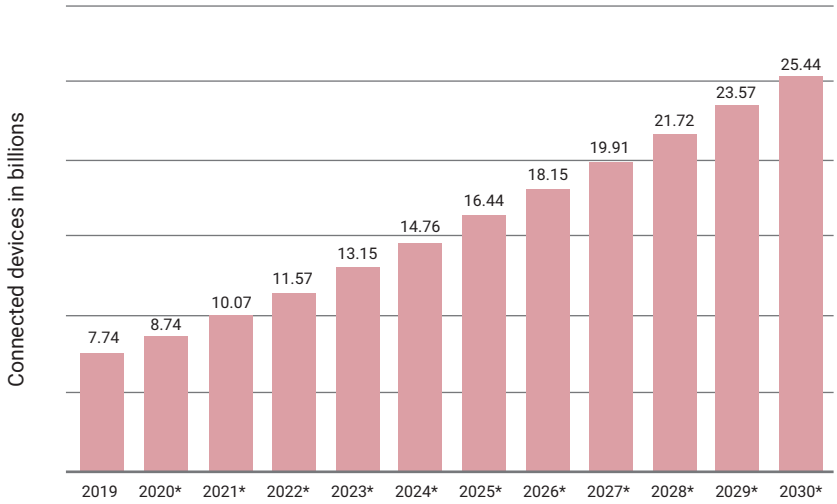
Remote working has completely changed the security paradigm. Enterprises must be able to ensure the security of employees working beyond the organization's field of view on their own devices and using various cloud solutions such as Zoom's videoconferencing service.

This new security paradigm causes difficulties for IT and cybersecurity specialists by presenting more opportunities for cybercriminals to attack. The number of phishing and spearphishing emails has increased by approximately 400 percent, according to the FBI.[13]

Another serious risk is ransomware. It is not a new threat; many cases of successful ransomware attacks have been recorded around the world

FIGURE 1

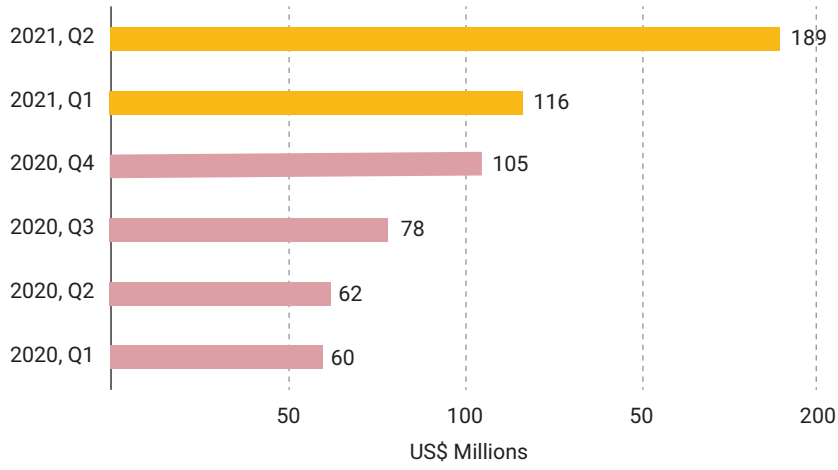
Number of IoT Connected Devices Worldwide



Source: Statista, "Number of Internet of Things (IoT) Connected Devices Worldwide From 2019 to 2030," *https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/*

FIGURE 2

Ransomware Growth by Quarter



(**figure 2**).[14] These successful attacks should be considered a call to action for any organization. For example, in May 2021, cybercriminals spread ransomware in the US Colonial Pipeline infrastructure, completely disrupted the organization's operations, and demanded US$4.4 million to release the encrypted information.[15] This is one of the most significant cases of disruption of critical infrastructure operations.

How to Address Cyberrisk

Assuming that ensuring the CIA triad is the goal for information security and cybersecurity, how do organizations achieve it? The people, process and technology (PPT) framework can be used (**figure 3**).

Many executives regard cybersecurity as merely a technical issue that can be easily solved with proper equipment and technology. There may be a belief that if an organization conducts a penetration (pen) test every year, there is nothing to worry about. But pen testing is just one piece of the cybersecurity puzzle.

The NIST CSF demonstrates the cybersecurity life cycle (**figure 4**), which begins with the identification/inventory of the organization's assets (identify). If this is not done correctly, it will be impossible to protect the assets (protect). The risk is then registered (detect) and the organization reacts (respond). If the risk violates the CIA of the organization's assets, then recovery must take place to ensure the continuity of the organization's business processes. Only by combining testing and continuous learning with these steps can an organization have a solid cybersecurity system. Therefore, if an organization relies simply on pen testing for cybersecurity, there is a significant chance it has already been hacked but has not discovered it or that it will be hacked in the near future.

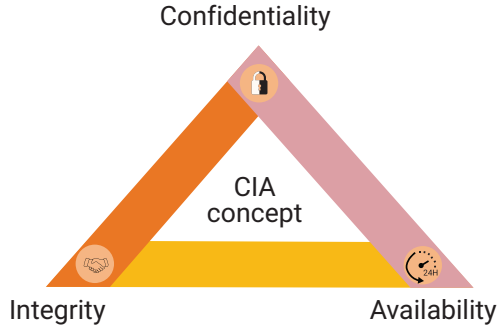
As for the financial sector, the effectiveness of cyberpreparedness is highly dependent on a central bank's leadership.

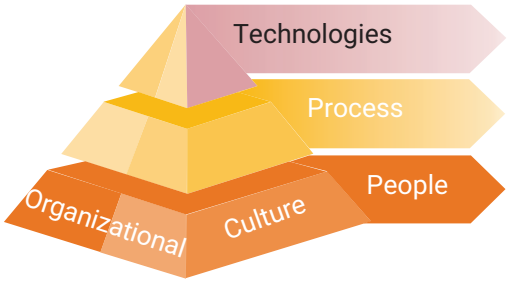
Effective cybersecurity depends on an organization's leadership. The effectiveness of cybersecurity is also greatly conditioned by organizational culture and the leadership skills of senior management. As for the financial sector, the effectiveness of cyberpreparedness is highly dependent on a central bank's leadership. If leaders accept that cyberthreats pose significant financial stability risk, they may be more inclined to pay proper attention to cybersecurity regulation and supervision.

By inverting the illustrated PPT model so that the people component is moved to the top, the stability of the pyramid becomes dependent on the behavior of people (**figure 5**). Just one careless step by an employee can entirely undermine the stability of the pyramid. The creation and preservation of an organization's cyberresilience culture is not a mere technical problem to be solved. It requires effective leadership to guide employees into making cyberconscious decisions. Deceiving employees with phishing emails is much easier for cybercriminals than bypassing complex hardware

FIGURE 3

The CIA Triad and the PPT Framework





and software security solutions. Any organization can become a victim of cybercriminal activity in this manner, so it is essential to be prepared to adequately restore the organization's business processes with minimal loss.

The concept that security is everyone's responsibility can be one of the best mitigation strategies for organizations that do not have the resources or budget for dedicated cyberteams.

For an organization to become cyberresilient, it must adopt the attitude that cybersecurity is everyone's responsibility. An organization can implement sufficient hardware and software cybersecurity risk management solutions, but the degree of its cybersecurity protection ultimately depends on the consciousness, vigilance and behaviors of each employee. In this case, continuously training employees in cybersecurity risk, noticing risk in a timely manner, and regularly testing employees' specialized knowledge is essential. Organizations that have ISO 27001 certification provide security awareness training to their employees because it is required, but what about fintech organizations that do not have any requirement to provide security awareness training? These organizations must realize the importance of effective training and prioritize it.

Conclusion

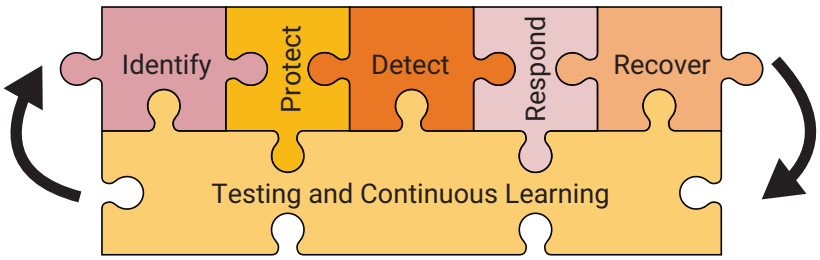
Cybersecurity is a journey rather than a destination. It has a beginning, but there is no end. The point at which an organization decides to protect its assets from cyberthreats is the beginning, and because technologies, processes and people are everchanging, the journey is endless.

Unfortunately, not every fintech organization has a dedicated team for cybersecurity. The concept that security is everyone's responsibility can be one of the best mitigation strategies for organizations that do not have the resources or budget for dedicated cyberteams. To implement this strategy, organizations can use cybersecurity frameworks and best practices.

Financial regulatory authorities should also be proactive in ensuring that minimum cyberhygiene exists at any organization that provides financial services.

FIGURE 4

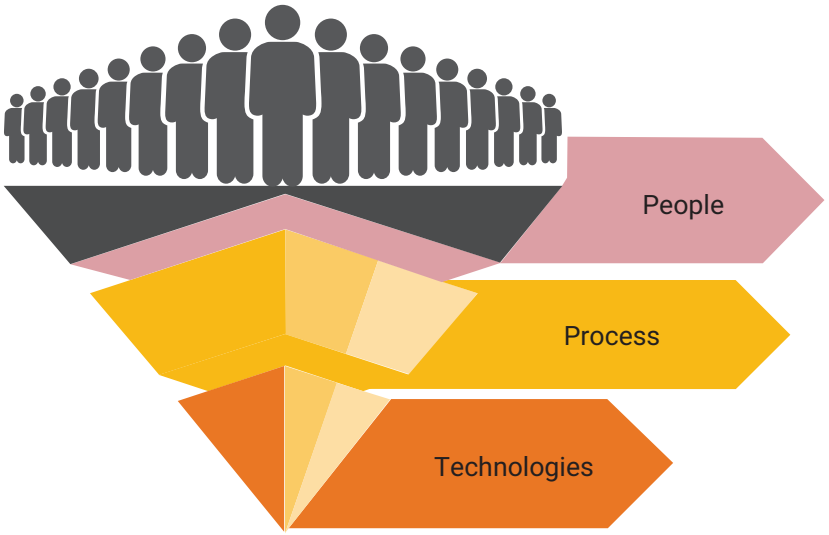
Cybersecurity Life Cycle



Source: Adapted from US National Institute of Standards and Technology (NIST), Cybersecurity Framework, USA, *https://www.nist.gov/cyberframework*

FIGURE 5

Importance of Cyberculture



Endnotes

1 Mueller, R. S.; "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies," US Federal Bureau of Investigation (FBI), 1 March 2012, *https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies*

2 IBM, *Cost of a Data Breach Report 2021*, USA, 2021, *https://www.ibm.com/security/data-breach*
3 *Ibid*.
4 Schwartz, M. J.; "Bangladesh Bank Hackers Steal $100 Million," Data Breach Today, 10 March 2016, *https://www.databreachtoday.com/bangladesh-bank-hackers-steal-100-million-a-8958*
5 World Informatix Cyber Security, *The Bangladesh Cyber Heist: 5 Years Later*, 2021, *https://worldinformatixcs.com/2016_bangladesh_cyber_heist/*
6 *Ibid*.
7 Arner, D. W.; J. Barberis; R. P. Buckley; "FinTech and RegTech in a Nutshell, and the Future in a Sandbox," CFA Institute Research Foundation, July 2017, *https://www.cfainstitute.org/en/research/foundation/2017/fintech-and-regtech-in-a-nutshell-and-the-future-in-a-sandbox*
8 National Institute of Standards and Technology (NIST), Cybersecurity Framework, USA, *https://www.nist.gov/cyberframework*
9 Federal Financial Institutions Examination Council, "Cybersecurity Assessment Tool," USA, *https://www.ffiec.gov/cyberassessmenttool.htm*
10 International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27001 *Information Security Management*, Switzerland, *https://www.iso.org/isoiec-27001-information-security.html*
11 ISACA®, *COBIT® Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*
12 Statista, "Number of Internet of Things (IoT) Connected Devices Worldwide From 2019 to 2030," *https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/*
13 Kass, D. H.; "FBI: COVID-19 Cyberattacks Spike 400% in Pandemic," MSSP Alert, 19 April 2020, *https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/*
14 SonicWall, *2022 SonicWall Cyber Threat Report*, USA, 2022, *https://www.sonicwall.com/2022-cyber-threat-report/?elqCampaignId=14431&sfc=7013h000000Mm0SAAS*
15 Reuters, "Colonial Pipeline Halts all Pipeline Operations After Cybersecurity Attack," 7 May 2021, *https://www.reuters.com/article/usa-products-colonial-pipeline-idAFL1N2MV01W*