Risk in the Digital Era and the Skills Required for a New Environment

The COVID-19 pandemic led to a whirlwind of changes in the digital ecosystem, which gave rise to new risk factors linked to the use of technology and data. Organizations with the ability to detect possible blind spots or latent threats in day-to-day operations can take preventive measures to manage them.

However, as the COVID-19 pandemic demonstrated, sometimes identifying risk and having action plans are not enough. When a black swan event (i.e., an unimaginable event that comes out of nowhere) affects humanity worldwide, both people and enterprises must be resilient and adaptable if they hope to survive.

During the COVID-19 pandemic, people experienced changes that affected them professionally, socially, technologically, psychologically and medically. The COVID-19 pandemic marked a before and after in terms of how people view risk. Today's new normal requires a change in habits created over many years. For enterprises, this means establishing the habits of identifying, protecting, detecting, responding to and recovering from any risk event that arises.[1]

The COVID-19 pandemic increased the digitalization of customer interactions threefold, as organizations accelerated the use or adoption of technology to continue operations.[2] The World Economic Forum identified 10 potential economic, environmental, geopolitical, social or technological threats, ranking cybersecurity failures number one and digital inequality number two.[3] These two threats can affect humanity on both personal and organizational levels.

There is a gap between the risk that is likely to impact organizations and the development of plans to treat the risk.

The development of big projects often requires specialized roles in cybersecurity, IT risk and IT internal control. Without these specialized roles, organizations may spend unnecessary time, effort and money to avoid or mitigate risk. However, if these kinds of roles were added at the beginning of projects, it would help organizations gain a realistic understanding of the IT environment and determine design plans to effectively mitigate IT risk.

The Three Dimensions of Technology and Cybersecurity

It is impossible to discuss technology and new skills without talking about the risk associated with their use, and that leads to the topic of cybersecurity. Cybersecurity is about much more than cyberattacks; it is about data protection, digital identity, data privacy, regulatory compliance, digital channels, third parties and the digital ecosystem, business continuity, fraud, and other IT topics. Cybersecurity

PIERINA GUIZADO | CISA, CISM, CDPSE, CSX-P, COBIT FOUNDATION, ISO 31000 SENIOR LEAD RISK MANAGEMENT, ITIL V3

Is head of data security and business continuity at BBVA Peru. She is also a lecturer of cybersecurity and the marketing director of the ISACA® Lima (Peru) Chapter. She participates in financial sector events through the Asociación de Bancos (ASBANC) and the ISACA Lima (Peru) Chapter. She specializes in nonfinancial risk management, the US Sarbanes Oxley Act (SOX), business continuity management (BCM), project management, information security, technological risk, cybersecurity, and process and data privacy management.

must be oriented to the present digital environment and its risk level through digital interaction.

To implement effective IT controls and cybersecurity strategies in this new environment, enterprises need specific skills. These might be completely new skills or skills that people already have, and which may need to be sharpened.

The starting point is to examine skills development in three dimensions:

1. **Personal**—The individual's role in daily life, such as the relationship with family or surroundings
2. **Organizational**—The individual's role as a member of an agency or enterprise
3. **Digital**—The individual's role as a member of a digital ecosystem

Each dimension offers opportunities to develop new skills to enable security in the digital ecosystem.

Personal

According to the World Economic Forum, the skills needed today have changed due to the digital divide resulting from technology.[4]

In today's environment, there are numerous challenges related to geography, such as having the necessary infrastructure to connect to the Internet in every town and city, particularly in developing countries. Technology and digital connectivity need to be available to everyone. Regardless of geographic location, people's technology skills should be cultivated from an early age, educating them on the proper use of technology and enabling them to see technology as a tool that can help them potentiate their plans and achieve their goals.

There are essential skills required for people to protect themselves from the external threats present in the virtual world of social interaction, including:

- The secure use of online and social interaction services and the configuration of privacy options
- The protection of digital identity and the use of services or applications
- The ability to interact with digital services
- The analysis of reliable sources of information or intensive data analysis
- The ability to build web portals or online services
- Knowledge of programming logic and algorithms to enable problem solving by analyzing component parts
- The use of software tools for presentations and videos

These skills are not necessarily part of every country's educational curriculum. Many countries have a long way to go before technology and cybersecurity courses are taught in school.

Organizational

At the organizational level, there is growing interest in digital transformation and the intensive use of technology and initiatives to update business processes using technology. Of particular interest are projects to provide online services with a unique customer experience.

Typically, the skills of the people who make up an enterprise are limited to their specific areas of specialization. This means that employees do not necessarily have all the knowledge they may need in this new IT environment. Enterprises can benefit from more people with skills in technology, data, analytics, and cybersecurity, who hold degrees in science, technology, engineering and math (STEM). In addition to highly specialized technological knowledge, soft skills and the ability to build software solutions and manage projects are important. Expanding employees' skills to address this gap requires more than an employee training plan. Employees must be willing to put in effort to learn the relevant skills to be successful in this new environment and understand that it is a prerequisite to developing their specialized roles.

Also, requirements for each role must be redefined. Security skills cannot be limited to the role of chief information security officer (CISO). They should permeate each area, process, technology, activity or outsourced role in the enterprise. There should be different levels of maturity and, above all, a higher level of expertise in cybersecurity skills in technology-related areas, but not to the exclusion of the rest of the enterprise.

According to the ISACA® *State of Cybersecurity 2022* report, recruiters in the cybersecurity sector found that enterprises around the world are demanding technology and security specialist personnel.[5] When hiring such personnel, enterprises want to know whether a candidate is well qualified for the

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

position, and they base this determination first on an applicant's soft skills rather than technical skills. The report found that experience is the number one factor in determining whether a candidate is qualified with 95 percent of respondents ranking experience as somewhat or very important. This is followed by credentials or certifications that prove technological or security know-how, practical experience applicable to the enterprise, employer recommendations and a relevant university degree.[6]

This indicates not only an unmet demand, but also opportunities for professionals willing to expand their knowledge bases.

Digital Ecosystem

Important parts of the digital ecosystem are digital interactions between stakeholders, which are becoming more common. Two years ago, Peru enacted a new regulation for the financial sector (i.e., banking, insurance, pension funds).[7] This regulation covers:

- Organizational governance
- Use of technologies
- Control over different technological processes
- Data security at the business level
- Authentication processes
- Enrollment and security measures in digital channels

It also requires financial enterprises to have employees with information security, cybersecurity and fraud prevention skills. In Peru and Latin America, enterprises in the financial sector that make up this digital ecosystem are exposed to IT risk, attacks and failure of controls. Certain skills were required to design plans to mitigate the negative effects and provide reliable services to customers, such as:

- Regulatory and legal compliance expertise
- Internal control of technology management
- Data governance capabilities specializing in privacy, security and data integrity
- Nontechnological skills

When these skills are possessed by employees throughout an enterprise, the level of security improves, as does the ability to provide services and communicate between enterprises. Above all, these skills are necessary for enterprises that adjust their focus to become more technological.

In the virtual world, the interconnection of services and enterprises should have a standard level of security that guarantees reliability and trust.

In the virtual world, the interconnection of services and enterprises should have a standard level of security that guarantees reliability and trust. And a more secure digital ecosystem will be achieved only if every interaction between enterprises and third parties meets that level of security.

Required Skills vs. Available Talent

The ISACA *State of Cybersecurity 2022* report is based on a survey of more than 2,000 professionals who hold the ISACA® Certified Information Security Manager (CISM®) certification or who were in positions related to information security in a variety of industries linked to technological services, including financial and insurance, government and healthcare. The report identifies some important skills required and the gap between the talent needed and the talent that is available.[8]

The respondents were asked which particular skills are missing in today's cybersecurity professionals. The largest skills gap was soft skills (54 percent) followed by cloud computing skills (52 percent). Although rated less highly, the report suggests that data-related topics, pattern analysis and system hardening will be increasingly important in the post-COVID-19 environment (**figure 1**).[9]

After three years of COVID-19 pandemic-related isolation, enterprises need to reconnect with their customers, which requires more talent in the areas of data analysis, cloud security, pattern analysis and, above all, human interaction skills. For example, soft skills linked to communication, teamwork, attention to detail, leadership and conflict resolution are needed (**figure 2**).[10] Employing specialists trained in these areas enables managers to focus on the business. It is also worth mentioning that because of the COVID-19 pandemic, enterprise digital transformation was accelerated. What previously was thought of as a gradual incorporation of technology turned into a whirlwind when digitalization became necessary for survival.

FIGURE 1

Qualified Skills Gaps

What are the biggest skill gaps you see in today's cybersecurity professionals?	
Soft skills (e.g., communication, flexibility, leadership)	54 percent
Cloud computing	52 percent
Security controls (e.g., endpoint, network, application, implementation)	34 percent
Coding skills	33 percent
Software development-related topics (e.g., languages, machine code, testing, deployment)	30 percent
Data-related topics (e.g., characteristics, classification, collections, processing, structure)	28 percent
Networking-related topics (e.g., architecture, addressing, networking components)	26 percent
Network operations (e.g., configuration, performance monitoring)	22 percent
Pattern analysis	22 percent
System hardening	22 percent
Computing devices (e.g., hardware, software, file systems)	11 percent

FIGURE 2

Top-Five Soft Skills

Select the five most important soft skills needed by security professionals today.	
Communication (e.g., listening/speaking skills)	57 percent
Critical thinking	56 percent
Problem solving	49 percent
Teamwork (e.g., collaboration, cooperation)	44 percent
Attention to detail	38 percent
Adaptability to change	32 percent
Decision-making	30 percent
Leadership qualities	29 percent
Time management	27 percent
Attitude	24 percent
Work ethic	23 percent
Writing skills	22 percent
Conflict resolution	22 percent
Honesty	16 percent
Empathy	13 percent

However, the need for additional skills does not change the core requirement: technological know-how in the field of specialized cybersecurity (**figure 3**).[11]

Creating a specialized safety and security culture is essential to protect customer data and develop plans to prevent and mitigate IT and cybersecurity risk.

Such knowledge must be incorporated into enterprises, either by hiring certified or experienced specialists in the field or by training existing personnel in these skills. The latter option is a good one in terms of talent development, and it takes advantage of employees' knowledge about the business. A third option is to hire third-party service providers for some functions.

Conclusion

In today's interconnected world, digital processes and data flows are highly dynamic, with an accelerated iterative process. Technology can enhance business models or help enterprises achieve their goals more quickly, become more efficient, and design a unique experience for the customer. But if security is not included in each part of the development process, the enterprise and client data can be exposed to risk.

It is important for people and enterprises to consider IT and security skills in all levels of the organization and across all processes related to technology, data and third-party business areas. Creating a specialized safety and security culture is essential to protect customer data and develop plans to prevent and mitigate IT and cybersecurity risk.

FIGURE 3

Top-Five Cybersecurity Skills

Select the five most important cybersecurity skills needed today.	
Cloud computing	52 percent
Data protection	47 percent
Identity and access management (IAM)	46 percent
Incident response	43 percent
DevSecOps	36 percent
Endpoint security (e.g., endpoint detection and response [EDR], extended detection and response [XDR])	32 percent
Data collection and correlation (e.g., security information and event management [SIEM]; security orchestration, automation and response [SOAR])	31 percent
Vulnerability scanning	30 percent
Threat detection technologies (e.g., intrusion detection system [IDS], intrusion prevention system [IPS], unified threat management [UTM])	29 percent
Threat hunting	28 percent
Penetration testing	27 percent
Vulnerability discovery	24 percent
Forensics	21 percent
Network segmentation	17 percent
Virtualization	11 percent

Endnotes

1 National Institute of Standards and Technology (NIST) Cyber Security Framework, USA, *https://www.nist.gov/cyberframework*

2 McKinsey, "How COVID-19 Has Pushed Companies Over the Technology Tipping Point—and Transformed Business Forever," 5 October 2020, *https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever*

3 World Economic Forum, *Global Risks Report 2022*, Switzerland, 2022, *https://www.weforum.org/reports/global-risks-report-2022*

4 *Ibid*.

5 ISACA®, *State of Cybersecurity 2022*: *Global Update on Workforce Efforts, Resources and Cyberoperations,* USA, 2022, *https://www.isaca.org/go/state-of-cybersecurity-2022*

6 *Ibid*.

7 *Diario Oficial El Peruano*, "Regulation for the Management of Information Security and Cybersecurity," Peru, 19 February 2021, *https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/*

8 *Op cit* ISACA

9 *Ibid*.

10 *Ibid*.

11 *Ibid*.