McKinsey
Digital

Transition to the next normal: Enhancing cybersecurity in the Iberian Peninsula

Remote work and more-sophisticated attackers are challenging cybersecurity for companies in Spain and Portugal. Here’s how they’re upgrading their defenses.

by Duarte Begonha, Joana Candina, Jesus Mathus, and Benjamim Vieira

© Getty Images

July 2020

The sudden need for large portions of the workforce to work remotely during the COVID-19 pandemic has forced chief information security officers (CISOs) and their teams to stitch together secure remote work arrangements on an unprecedented scale and at unprecedented speed. Making these fortifications even more secure is now an essential task in protecting enterprises from attack. The stakes are especially high in the Iberian Peninsula (Spain and Portugal), where it has long been hard to institute and maintain standard cybersecurity protocols.

Already, there have been significant failures in the region. Phishing attacks have penetrated government-entity perimeters; malware and ransomware have infected the internal network of one of Spain's largest telecommunications companies; a professional sports club fell victim to a large-scale data breach; and several financial institutions have suffered distributed-denial-of-service (DDoS) attacks, to name a few. These and other cyberincidents have hurt both the operations and public perception of Iberian organizations—damage that can translate into millions of dollars in cost.

The Iberian context

The pandemic has stressed the region's cybersecurity systems, making Iberian companies especially vulnerable to cyberattack. The statistics indicate that cybercriminals are taking full advantage. Since January, phishing, malicious websites, and threats targeted at remote users have increased by 85 percent, 25 percent, and 17 percent, respectively (Exhibit 1).

The Iberian Peninsula has three elements that make it uniquely vulnerable to cyberthreats:

1. Many Iberian workers see cyber-related controls as infringements on their free will and privacy and impediments to productivity. As a result, there is a widespread employee culture that takes pride in flouting the rules and finding ways to operate around controls. This culture has not been greatly challenged, given that Iberian companies have been primarily targeted by medium- to low-capability attackers, such as hacktivists, independent hackers, and insiders.

Exhibit 1

Bad actors in Iberia are doubling down on exploitation of the pandemic.

30,000%

Increase in COVID-19-themed phishing, malicious websites, and malware targeted at remote users since January

Phishing & spam			Malware & threats		
18M	**2%**	**85%**	**148%**	**25%**	**17%**
Global COVID-19 phishing emails blocked by Google in one week	All daily malicious spam using COVID-19 lures	Increase in phishing targeted at remote enterprise users	Increase in ransomware attacks from February to March	Increase in malicious websites and malware files	Increase in threats targeting remote enterprise users

But reining in the rule breakers may become increasingly important as the region begins to attract more nation-state actors and organized crime.

2. The Iberian market is a consumer society that accounted for about 10 percent of EU consumer spending as of December 2019, most of it at physical retail stores. COVID-19 has shifted much of that activity to online channels, exposing end users who are unfamiliar with cybersecurity to dramatically more-digital interactions. This gives attackers a larger pool of endpoint devices to compromise and use to bypass corporate firewalls.

3. Cyber maturity is lower in Iberia than in most of its European neighbors, such as France, Germany, and Italy, and Iberia particularly lags on the people dimension of cybersecurity.[1] The people dimension is critical, as security for remote working depends on building a "human firewall" of employees, each of whom does his or her part to keep the enterprise secure. But workers in Spain and Portugal have instead become threat vectors due to their poor adherence to security protocols; hence the spike in people-related cyberattacks.

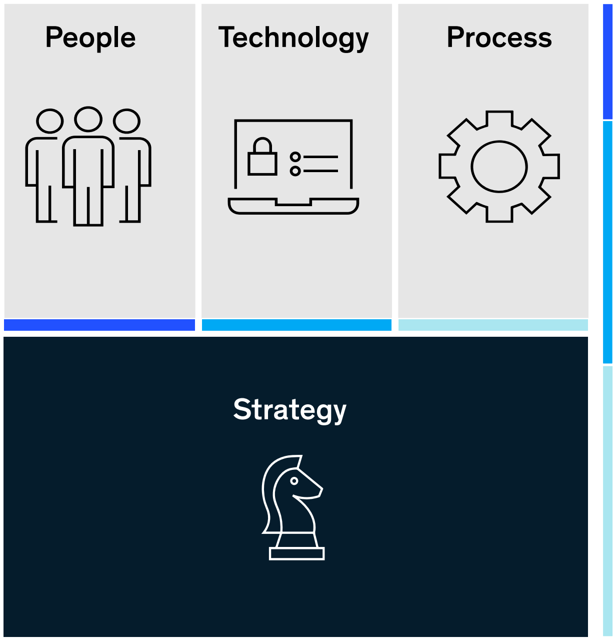
Four dimensions to strengthen security

In our work with cybersecurity teams in the Iberian Peninsula, we have developed a four-dimensional approach to increasing cyber defenses during this disruptive, high-risk period: people, technology, process, and strategy (Exhibit 2).

[1] McKinsey Digital Resilience Assessment measuring the level of cyber maturity of cyber companies from 0 to 4 (0 = inexistent, 1 = ad hoc, 2 = basic, 3 = mature, and 4 = leader).

Exhibit 2

Our approach to assess cybersecurity postures in organizations is focused on four main dimensions.



1. Continuous cybersecurity communication
2. Focus on "what to do," not "what you cannot do"
3. Increase awareness of social engineering
4. Identify and monitor high-risk user groups
5. Patch and configuration management for relevant systems
6. Multifactor authentication and privileged access management
7. On-premise application security for remote access
8. Device virtualization
9. Device, software, and communication security
10. Monitoring capacity and scope
11. Web-facing threat-intelligence monitoring
12. Capacity management
13. Remote-working support for end users
14. Incident-response and business-continuity capabilities
15. Contractors, off-site vendors, and third-party management
16. Hard-copy document security
17. Shadow IT management
18. Threat monitoring
19. Fraud prevention
20. Security-cost management
21. Customer support

1. People: Understand employee behavior to detect emerging threats and vulnerabilities

The Iberian market has less effective cybersecurity than its immediate neighbors, especially in terms of employee adherence to security protocols. It can turn these weaknesses into an opportunity by using behavior analytics.

Use employee communication for early threat detection. As employees set up their remote workstations, many inadvertently introduce technologies and practices that have the potential to weaken cybersecurity. For example, parents working from home are more likely to share corporate devices with kids, perhaps adding an easier password for their use or making other changes that generally weaken security. Companies can address these threats quickly by setting up two-way communication channels. These can enable collaboration but also act as forums for communicating cyber standards and for running awareness campaigns that teach employees how to identify phishing emails, use firm-approved applications, and handle critical data. One large telecommunications firm has organized regular pulse checks with frontline employees to learn how their working habits are evolving as they work from home.

Visibility through user-behavior analytics. Awareness campaigns, though useful, do not easily identify high-risk users. For that, companies can apply user-behavior analytics (UBA). Using user-behavior profiles to detect anomalous behavior, organizations have been able to recognize and deal with live threats before damage is done. Companies in the region must comply with regulations such as the Spanish Data Protection Act and Portuguese Data Protection Law, which restrict the collection of employee data, define baseline privacy guarantees on corporate devices, and sometimes require that companies establish clear rules for employees' data-collection activities, with input from workers' representatives. Collecting data outside of working hours, for example, is forbidden.

2. Technology: Apply critical technology controls, and make sure they work

As work and commerce move online, customers and employees are exposed to a higher volume of digital interactions, increasing the cumulative level of cyberrisk. Companies can use technology to reduce and control this risk. The first steps are to ensure that existing technology is being used to maximum effectiveness and then to address areas with the most serious security gaps, such as device virtualization.

Extract maximum value from existing technology. The shift to working remotely has exposed serious cybersecurity gaps at many organizations. Addressing them with new technologies, however, usually involves high costs and long implementation times. To provide security now, when it is urgently needed, organizations should instead focus on ways to strengthen existing technology. Instead of adding new tools, one large telecommunications firm was able to improve its security by building out additional security, information, and event-management (SIEM) use cases and fine-tuning its cloud data-loss prevention (DLP) policies.

Use device virtualization as an opportunity to complement remote security capabilities. The large-scale shift to remote work brought on by COVID-19 has exposed serious security gaps in device virtualization at organizations in Spain and Portugal. Most companies are choosing to address these gaps with advanced monitoring using machine learning. But once those systems are up to speed, organizations can take other steps to protect against medium- to low-capability attacks. Limiting lateral movement within the network through microsegmentation is one. Protecting corporate data through operating-system (OS) virtualization is another. One financial-services firm quickly segmented users in its networks specifically to improve the security of its device virtualization as its workforce moved en masse from the office to working from home. However, organizations must be careful that these short-term solutions don't impede the investment of time and funds necessary to implement long-term cybersecurity goals.

3. Process: Learn to continuously adapt to disruption and stay ahead of emerging risks

The absence of serious cyberattacks in the Iberian Peninsula does not imply highly effective cybersecurity programs but rather a preponderance of low-level attacks. In the future, companies may be targeted by more-advanced attackers. Companies in Spain and Portugal cannot be complacent. They need to continuously adapt to the dynamic work-from-home environment and anticipate emerging cyberrisks, especially from high-capability attackers who may target the region in the future.

Transition to remote working is a continuous process. Ensuring that employees use existing controls correctly and that they understand the importance of cybersecurity is critical. However, it is not enough. Cyberrisks continue to evolve and can impact an organization in ways existing controls cannot stop. To address this challenge, organizations need to adopt a mindset of continuous transition, remaining ever vigilant for evolving vulnerabilities and threats. One financial-services company in the region has actively adapted its cybersecurity practices throughout the COVID-19 pandemic by beefing up communications to frontline employees and strengthening incident response plans. It now plans to make continuous vigilance a permanent part of its cyber activities.

Improve threat detection as cyberrisks evolve. Malicious actors are increasing the volume of cyberattacks in the Iberian Peninsula that seek to take advantage of the ongoing disruption that has preoccupied cyber teams—phishing is up 85 percent, and ransomware attacks 148 percent. Companies need to build active defenses to identify incidents early and protect their most critical assets, using predeveloped plans that allow them to recover with minimal impact to business operations. For example, using multiple threat-intelligence services can help ensure that cyber teams learn of novel threats as early as possible, allowing them to better predict, prevent, detect, and identify attacks. Many companies in the region have already derisked their remote environment by implementing or expanding multifactor authentication (MFA) and enhancing monitoring capabilities to shorten risk response times.

4. Strategy: Convert cyber into a long-term competitive advantage

Given the reluctance of employees to embrace security controls, it is essential that top executives, starting with the CEO, spread the message that cybersecurity is not only critical to the company's ability to do business but also a powerful business enabler. This will require cyber and business leaders to adjust how cybersecurity ties into their overall business strategy. By doing so, organizations can better align short-term actions with long-term goals, add value to existing business offerings using cyber as a differentiator, better align business risk priorities with cyber priorities, and leverage leadership as a key to building a positive cyber culture.

Short-term actions should align with long-term goals. CISOs and CIOs have had to move fast to address the disruption caused by the COVID-19 pandemic, leading them to prioritize short-term efforts to "put out the fire." In many cases, this has caused them to lose sight of long-term objectives. They need to refocus now to make sure their efforts to address COVID-19 do not compromise their long-term cyber strategy. One financial-services company in Iberia was in the process of choosing a partner to address short-term cloud-security concerns, which had increased in the context of COVID-19. After performing a high-level threat-modeling exercise, it became clear that cloud misconfigurations were actually a long-term vulnerability and needed to be a higher priority. This led the company to modify its criteria by including cloud-security-posture capabilities as a key factor in choosing a partner.

Use cyber as a differentiator that adds value to existing offerings. In the past, the cybersecurity function has been perceived as of low value because its benefits are largely intangible. When it works well, it staves off threats and security breaches don't happen, making it hard for people outside the security function to perceive its value. This is especially true in Iberia, where many organizations perceive cyber as a necessary evil, one that provides important protection for products and services but also acts as a roadblock to progress and agility. However, the work-from-home model changes that. Company leaders realize that, in an era of remote working, providing customers with assurances of robust security adds value to existing business offerings and can be a valuable differentiator in the minds of potential customers. For example, a large financial-services company extended its rollout of MFA from all critical systems to less-critical systems to safeguard more of its technical entry points for end users.

Business risk priorities should be aligned with cyber priorities. Business leaders in Spain and Portugal often decouple cyberrisks from business risks because cyber is perceived to be an IT issue. However, with increased reliance on cyber in the remote-work environment, it has become more important for business and cyber leaders to align against both types of risk. With a universal understanding of risks, the business function and the cyber function can tie relevant risks together, align on a shared strategy, and develop a road map that promotes business growth as well as cyber resiliency. For example, a large telecommunications firm has leveraged the expertise of business information-security officers (BISOs) to communicate risk in a universal language to both cyber and business stakeholders, enabling cross-functional alignment.

Build cybersecurity into every business process. Frontline employees are dealing with the challenges associated with remote working and have limited bandwidth to apply and uphold new security demands. To make sure security is upheld by the organization, cyber teams should focus on integrating cybersecurity into organizational processes and reaffirming its value to frontline employees. For example, cybersecurity should be explicit in senior-leadership priorities. It should also be built into the software-development life cycle and business-impact analyses (BIA), to name a few. When cybersecurity is integrated across organizational processes, it can be promoted within the organization as a competitive advantage that improves the quality of products and services, changing the perception of cybersecurity from an obstacle to be overcome to a business-enabling necessity.

Securing remote-working arrangements while protecting the integrity of networks is essential to ensure the continuity of operations during this disruptive time. The dimensions we describe in this article, while not comprehensive, are helping multiple organizations in Spain and Portugal improve security for their organizations, their customers, and other stakeholders. The coming weeks and months are likely to bring more uncertainty. As new dimensions for upholding security standards emerge in the transition to the next normal, we will continue to learn from the experience of companies across the Iberian Peninsula.

Duarte Begonha is a partner in McKinsey's Lisbon office; **Joana Candina** is a consultant in the Madrid office, where **Benjamim Vieira** is a partner; and **Jesus Mathus** is a consultant in the New York office.

The authors wish to thank Jim Boehm and Wolf Richter for their contributions to this article.