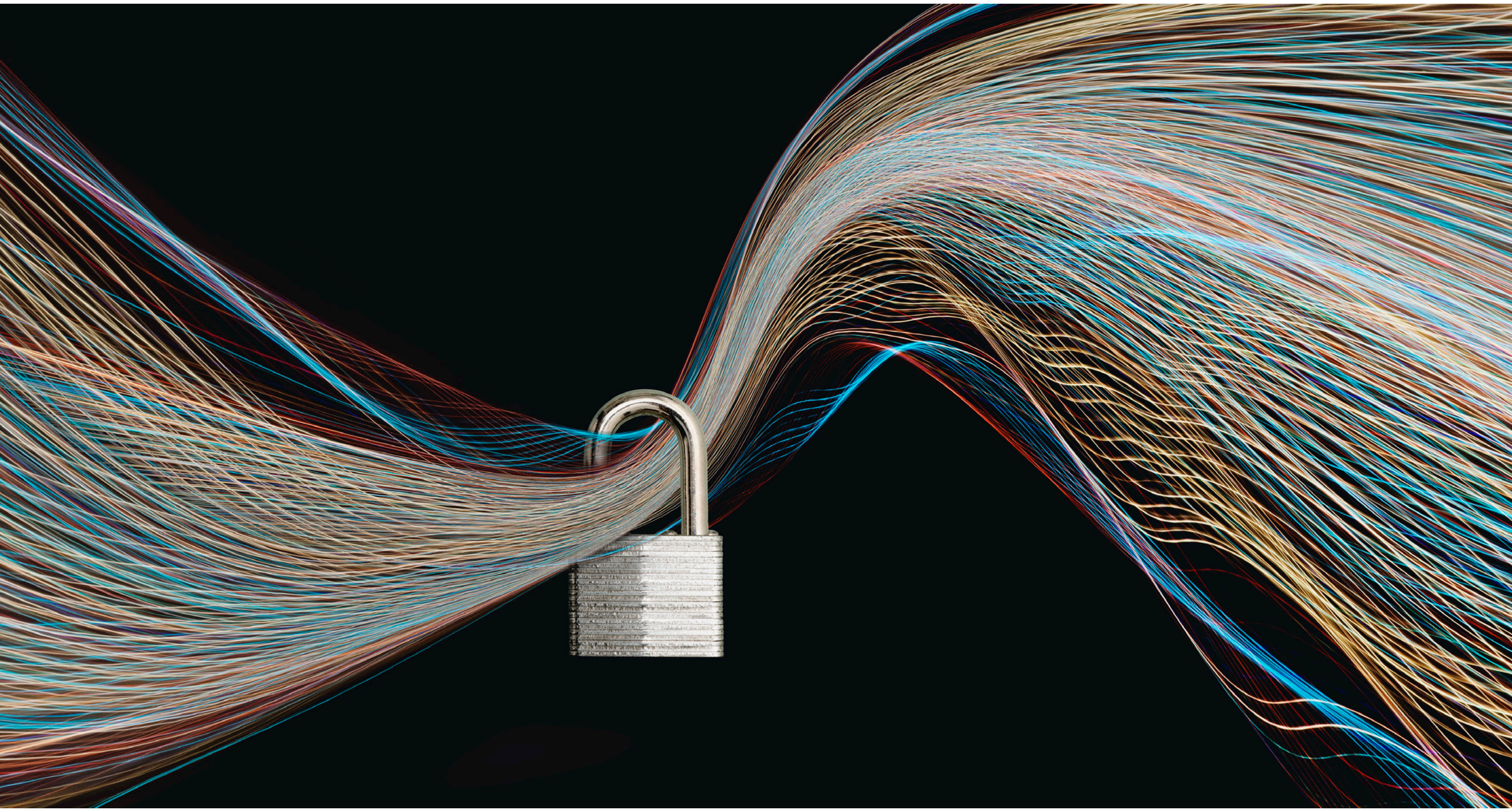
McKinsey
& Company

Risk & Resilience Practice

The unsolved opportunities for cybersecurity providers

With sophisticated cyberthreats on the rise, organizations must continue evolving by using novel strategies and technology. For cybersecurity providers, the challenges and opportunities are numerous.

by Bharath Aiyer, Jeffrey Caso, and Marc Sorel



© John M Lund Photography Inc/Getty Images

January 2022

The COVID-19 pandemic has forced rapid changes on corporate cybersecurity functions. Chief information-security officers (CISOs) have had to adjust their strategies to account for remote working, pivoting from working on routine tasks to working on long-term goals of establishing secure connections for remote situations. Managing business continuity has been the goal, with the patching of remote systems over virtual private networks, handling of those systems' increased workloads, and monitoring of spiking cyberthreat levels and cyberattackers targeting at-home workers with an array of threats. In fact, a McKinsey survey of cybersecurity providers found a near-sevenfold increase in spear-phishing attacks since the pandemic began.[1]

The challenges that face organizations are also forcing cybersecurity providers to pivot, adjusting their strategies and their product and service offerings to meet postpandemic objectives. That must be done in a manner that accommodates the new security landscape but continues to monitor customers' needs while adjusting sales, service, and training accordingly. The elements that enterprises must secure (data, devices, people, networks, machines, and applications), how they must secure them (prevention, detection, response, and remediation), and why it's important to secure them (to mitigate loss of lives and livelihoods) continue to evolve, and cybersecurity providers have yet to solve several crucial customer challenges. The stakes have never been higher.

Insights from the results of the cybersecurity-provider survey revealed that CISOs and cybersecurity-operations teams will continue to invest niche spending in the areas of perimeter security, next-generation identity and access controls, remote access, security automation, and security training. With a vast ecosystem of technology platforms and partners, cybersecurity providers will need to differentiate themselves. The research suggests that there remain four unsolved challenges: the visibility gap, fragmentation of technology, the talent gap, and the measurement of ROI. Addressing even one of these challenges can help providers gain a sustainable edge in an ever-evolving, fragmented, and competitive market.

Visibility gap

Without visibility into digital infrastructure, it will be difficult for companies to recognize when, where, or why there is a problem. According to a recent McKinsey survey of approximately 200 buyers of security-operations applications (such as security-information and -event management and security-orchestration, -automation, and -response tools) in the enterprise market (companies with more than 1,000 employees or topline revenue more than $1 billion), around 60 percent of buyers analyze and triage less than 40 percent of their enterprises' log data. Worse, that figure may be understated: third-party and software-as-a-service log data are often excluded, since they are not prioritized for collection and analysis in many enterprise environments.

Today's typical enterprise environment, though, can make that necessary visibility difficult (see sidebar "Case example: Cybersecurity visibility"). Chief information officers and CISOs also need to rethink their analytics strategies, with an eye on deploying analytics designed for the volume and nature of today's data, both structured and especially unstructured.

Case example: Cybersecurity visibility

McKinsey worked with a large, multinational pharmaceutical company that had a security-visibility problem made worse by its ongoing move to the cloud. One-fourth of its public-cloud workloads were not connecting to its system for security-information and -event management. A forensics analysis discovered the issue when responding to an active cyberthreat.

[1] Venky Anant, Jeffrey Caso, and Andreas Schwarz, "COVID-19 crisis shifts cybersecurity priorities and budgets," McKinsey, July 21, 2020.

The best way to begin any compliance or security program is to assure telemetry at the endpoint, thus helping ensure that automated communication processes from multiple data sources are normalized and standardized for faster and more consistent analysis. That element alone can contribute to better customer experience, application health, quality, and performance, in addition to more scrutiny from a security standpoint. The sad truth is that few, if any, enterprises are confident that they have accurate and comprehensive telemetry to detect an intrusion in their environment. In solving the telemetry and visibility gap, cybersecurity providers should perform the following actions:

- *Rethink the 'pay by the drink' approach (such as pay per log) to volume-based pricing models.* Such payment mechanisms are unsustainable at scale for enterprises, particularly when considering an enterprise's consumption models for cloud architecture and infrastructure. Offerings should be adjusted to solve rate limits of mass data processing at the peta- or terabyte level.

- *Identify the missing puzzle pieces to building a 360° view.* The security-telemetry implication is often the tip of the iceberg. In many companies, the broader ecosystems for IT- and data-asset management have not matured to keep up with the security approaches. Leading providers will build tooling that can construct an outside-in view of the puzzle and identify the critical missing pieces. Such business-aware, intelligent tooling provides substantial value to a cybersecurity-function because it shifts the conversation with business leaders away from numbers to the value chain and revenue streams of the business. Educating customers on how to plan for cost reduction and be purposeful about which logs they select to ingest, as well as building low-cost data lakes that can affordably collect all logs for pretriage to feed into the system of choice for security-information and -event management, can bridge the gap in the interim. That means that sales engineers, architects, analysts, and other personnel are critical in identifying puzzle pieces that are missing (or redundant) as part of the presales process to demonstrate to security buyers how a technology will close visibility gaps.

- *Reduce false positives, forcing the organization to approach cyberthreats proactively, not reactively.* The improved use of AI and machine learning provides a holistic view of an entire security program, including on-premises, in the cloud, across geographies, within business units, and from remote networks. Transparency here allows an organization to prioritize potential threats. By reducing false positives, it has a clearer picture of cyberthreats such as vulnerabilities, unpatched systems, and misconfigurations.

Technology-fragmentation challenge

Part of a CISO's job has an impossibility element. Their teams are supposed to protect against future cyberattacks, with the nature, method, timing, scale, and identity of those attackers unknown. Those frightening unknowns fuel a fear of reducing the number of security applications, even seemingly redundant ones (perhaps obtained through an acquisition), because it's possible that the targeted app might be the one to save the enterprise.

Enterprises grapple with the timeliness challenge of technology decisions (where and how to balance agile-best integrated options with fragile, fragmented, best-of-breed options), since different technology, applications, and providers are used across an organization. Often, a company may have more than 100 third-party security tools in use. In many cases, that number is driven by the CISO's expanding mandate—and desire not to be the one who cancels the tool that might prevent the next big breach. There are several key drivers of this security complexity.

The enterprise perimeter has changed in recent years as the paths to access data assets has soared, with no single perimeter existing. The influx of IT functions hosting on-premises, private- and public-cloud environments is upon us. As a result, multi- and hybrid-cloud security will continue to be critical, and CISOs will be willing to pay for increasingly hard-to-find skills (such as mainframe security) from a service provider.

With many industries, the first challenge of operational-technology (OT) security is identifying who “owns” it. Once resolved, the logical next questions follow: Who funds it, who operates it, and what are the intersection points between IT and OT security? A duplication of security controls, policies, frameworks, and vendors across both IT and OT only drives complexity further.

The interlinkages among data governance, data privacy, and cybersecurity have precariously positioned the CISO as the only first-line enforcer amid a second-line function. With the continued expansion of data regulations, data-sovereignty laws, and customer interest in data privacy, the CISO is increasingly asked to add tooling, process, and prioritization to retrofit privacy into security. In many cases, that has led to a proliferation of tooling, such as data classification, data tagging, data-access governance, and privacy management, where the operating model between information security and privacy (compliance concerns) can get blurry.

While CISOs report varying degrees to which they have a seat at the table during M&A, one thing is for sure: after M&A, they will have plenty of cleanup to do. Companies are vulnerable to cyberattacks during acquisitions, which means that the last thing a CISO wants to do is rip and replace the tooling, leaving unknown vulnerabilities exposed. To understand capabilities, cyberthreats, and critical data, integration teams can prioritize a target’s function-specific technology applications by categorizing each. Here lies an opportunity for cybersecurity providers to offer material value.

To help CISOs extract themselves from the “one-way ratchet” that is enterprise cybersecurity tooling today, cybersecurity providers need to perform the following actions:

— *Produce offerings that allow for seamless simplification of sprawl.* Deploy a product that takes over incumbent functionality, generates data to show the efficacy of the new layer offering (such as recurring money and time saved by rationalizing tooling), and enables the sunsetting of old, legacy approaches.

— *Use cloud and software-as-a-service adoption or updates as an opportunity for tool rationalization.* Providers must maintain relationships with major cloud platforms, emphasizing native integration with software and platform leaders, as hybrid scenarios with on-premises, public- and private-cloud expand. Many major platform players have invested significantly in managing their relationships with cloud service providers.

— *Engage all stakeholders, make business-based simplification decisions, and don’t put all the cybersecurity burden on the CISO.* Organizations should empower their CISOs to make risk-based simplification decisions, gaining cross-functional support for key simplification decisions so the burden (and after any incident, the blame) do not rest solely on the CISO.

Cybersecurity-talent gap

With more than 3.12 million jobs in cybersecurity estimated to be unfilled in 2021,[2] the talent shortage is a massive problem, and it’s affecting both clients and providers. The use of technology—primarily AI and its machine-learning offspring—has helped slightly, especially in a security-operations center dealing with an active cyberattack. But the technology is primarily supplementing security analysts, allowing human capacity to be more efficient and to focus more on tasks where their experience and creativity are essential. Addressing the talent gap takes innovation and persistence:

[2] “Cybersecurity workforce demand,” US National Initiative for Cybersecurity Education, 2021.

— *Recruiting realities.* To manage the skill gap, cybersecurity providers may want to focus on offerings that are not as people intensive to deploy and manage or maintain. To remain talent competitive, providers should get creative when it comes to recruiting, training, and retaining talent, such as looking beyond traditional places, finding individuals with similar skills sets that can be trained, looking beyond formal education, and so on.

— *More one-shop and full-stack-service providers (such as 'infra in a box').* Companies are moving away from the approach of product-delivery deployment and moving toward annual subscription models that include service delivery.

— *Impact of delivery preferences on customers' key buying factors.* Delivery preferences are critical. For example, the rate of false positives has historically been a top buying factor in several security-product markets, for a logical reason: the more false positives, the more frustration and manual effort for security-operations teams to trudge through every day. However, as the delivery of those products has shifted to a service-driven approach, buyers care less about false positives because they no longer see level-one and -two data. Instead, the triage stage is outsourced almost entirely by the product provider's service team. Buying preference moves farther right along the value chain to the value and actionability of the intelligence, response time, and so on.

Cybersecurity's ROI

The most successful cybersecurity program is one that no one notices and that enables the underlying business to function unhindered. Organizations today struggle with understanding how to measure the return or value of a dollar spent on cybersecurity, as well as how to communicate its value to internal stakeholders, such as C-suite and board members. Providers should structure their output, reporting, and dashboards to speak to business audiences, as well as technical audiences. Provider solutions should take credit for all their accomplishments.

If an industry is not implementing the right cybersecurity programs and therefore spending less than their needs demand, there is no comfort in looking at its neighbors from a comparison standpoint. Maturity in no way guarantees resilience, but it does help define and measure ROI appropriately. To have a true security proposition, there are at least three dimensions that the cybersecurity provider community should consider:

— *Business value.* Do the organization's security offerings reflect the priorities of its customers' businesses today? When those business priorities change, can its security program adjust its priorities effectively? When there's a crisis, can it quickly map online services to business processes?

— *Customer value.* Does the customer see the organization's security capabilities as a differentiator? Do they know it is managing top risks?

— *Market value.* Do external stakeholders, including investors, vendors, and third-party supply chains, understand the organization's security journey and the impact of the security team over time? Are security capabilities included as part of the company's valuation? How does the organization talk about security to "the Street"?

Continuing to evolve

For cybersecurity providers, the ability to offer customers real-time technology and services that speak to the business, not only the CISO, is crucial. They also need to demonstrate the right value and key performance indicators to measure outcomes, which is the first step on the journey to helping its customers differentiate as security-minded businesses.

The four challenges detailed in this article can be solved, and a wait-and-see approach is not advised. It is important to realize that the challenges are fundamental to the industry and to define the constraints within which the industry operates. Executives must be cognizant of such issues, as well as try to solve them. But most importantly, cybersecurity professionals need to be open and transparent about them with internal stakeholders, working in collaboration to solve each challenge (see sidebar “Case example: Cybersecurity trust”).

From a go-to-market perspective, cybersecurity vendors that can appeal to business, functional, and technology executives alike will have more success in becoming household names.

Case example: Cybersecurity trust

Following a series of public breaches, a global software provider created the position of chief trust officer. It empowered that leader to be the company’s external-facing cybersecurity ambassador to the market. The role serves as a bridge between customer-account teams and technical information security, as well as a convener role (for example, promoting industry-wide collaboration on cybersecurity and establishing a regular cadence of cybersecurity discussions with key customer accounts).

Bharath Aiyer is an associate partner in McKinsey’s Bay Area office; **Jeffrey Caso** is an associate partner in the Washington, DC, office; and **Marc Sorel** is a partner in the Boston office.

Designed by McKinsey Global Publishing