Cybersecurity: how to make it pay

How to build a cybersecurity strategy that will both reduce risk and yield a return on investment

BinaryCore | KEARNEY | in collaboration with aws

Executive summary

With cyber risks proliferating, it is hard to know how much to spend on cybersecurity and how to get the most bang for your buck. While many vendors promote sophisticated security tools and systems, most enterprises still need to get the basics right: you need to build a culture of security before evaluating and employing security excellence. The first step is to develop a strategic and tactical cybersecurity plan aligned with your business objectives, risk tolerance, and unique operating situation. While most enterprises will have already suffered a security breach, many have yet to identify what business impact they can tolerate and the critical assets that, if compromised, could result in a disastrous impact. Until you do, optimizing your investments in cyber risk mitigation is almost impossible.

As explained in our recent article, being proactive is key and each organization should conduct a probability and impact analysis of the risk against their critical assets and a corresponding capability analysis to identify the highest-priority risks. A failure to protect assets adequately can result in a business disruption or sensitive information being corrupted, stolen, and even sold, resulting in a major public embarrassment and loss of share price.

After protecting the most critical assets, the next step is to work on the capability to respond and recover rapidly from an attack. This is not accomplished by a cybersecurity tabletop exercise twice a year and reliance on a team with little cyber experience; rather, it demands the development of an incident preparedness and response playbook that assumes a cyber compromise will occur and could lead to an operational failure. It's now a question of "when" rather than "if."

In recent interviews with Kearney, enterprises with significant operational technology (OT) investments consistently highlighted OT risk as an active or looming concern, driven by the growing convergence of IT and OT and a significant reliance on digital systems. Enterprises with "critical infrastructure," such as utilities, healthcare providers, and defense manufacturing, are at the most significant risk, followed by those that rely heavily on machinery and automation. Critical infrastructure is now a strategic target of very sophisticated nation state actors, as well as cybercriminals.

> Most enterprises still need to get the basics right: you need to build a culture of security before evaluating and employing security excellence.

Hackers are here to stay

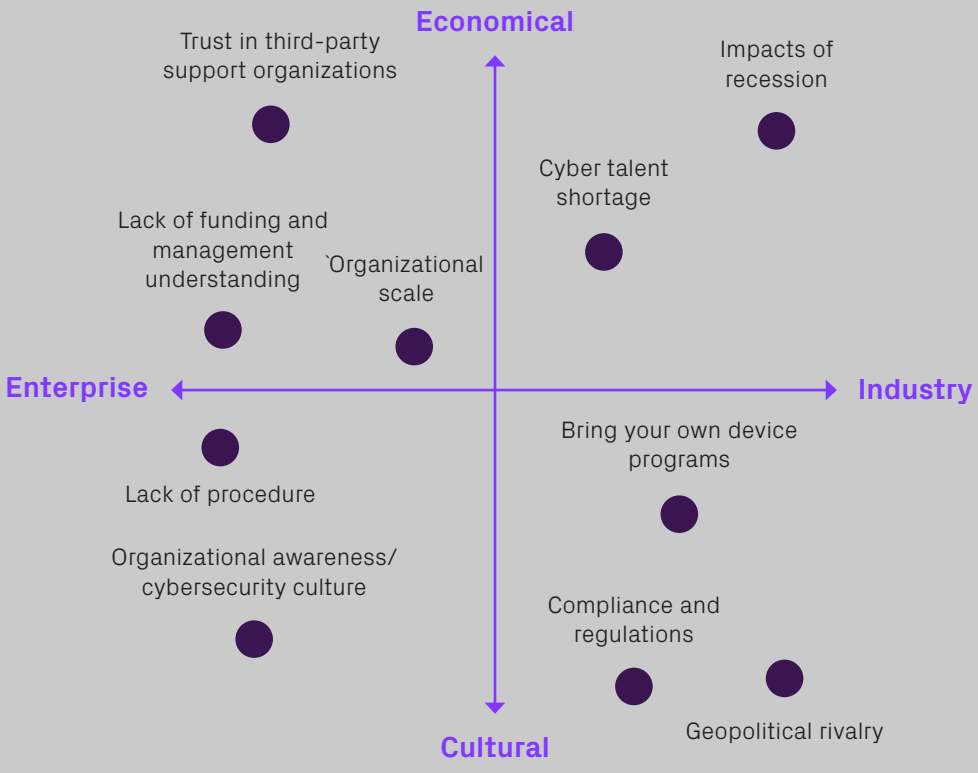
Enterprises' operational technology (OT) is increasingly exposed as it moves online and becomes interconnected. With automated systems now employing application programming interfaces (APIs) to exchange real-time information across networks, the risk of data breaches (via software updates and unauthorized access) is rising. Those were two key takeaways from Kearney's recent interviews with leading cybersecurity practitioners.

At the same time, new technologies, such as crypto attack tools and ransomware-as-a-service, are now readily available on the dark web, making it easier to launch an attack. Concurrently, bad actors are getting better at disguising their activity and intentions. Indeed, organizations, rather than individuals, are increasingly drawing on their R&D capabilities to carry out sophisticated attacks employing more automation and greater stealth.

The risks arising from these technological shifts are being exacerbated by socioeconomic shifts, such as the rise of working from home, a cost-of-living crisis, and greater geopolitical tensions, as nation states now see cyber weapons as one of the most cost-effective means of waging war (see figure 1).

As policymakers grasp the dangers, governments are increasing regulatory requirements and oversight on businesses, particularly those designated as critical infrastructure, with greater financial liability for cyber negligence and non-compliance.

Figure 1
A number of key factors impact cybersecurity



Source: Kearney Analysis

The C-suite now needs to switch on

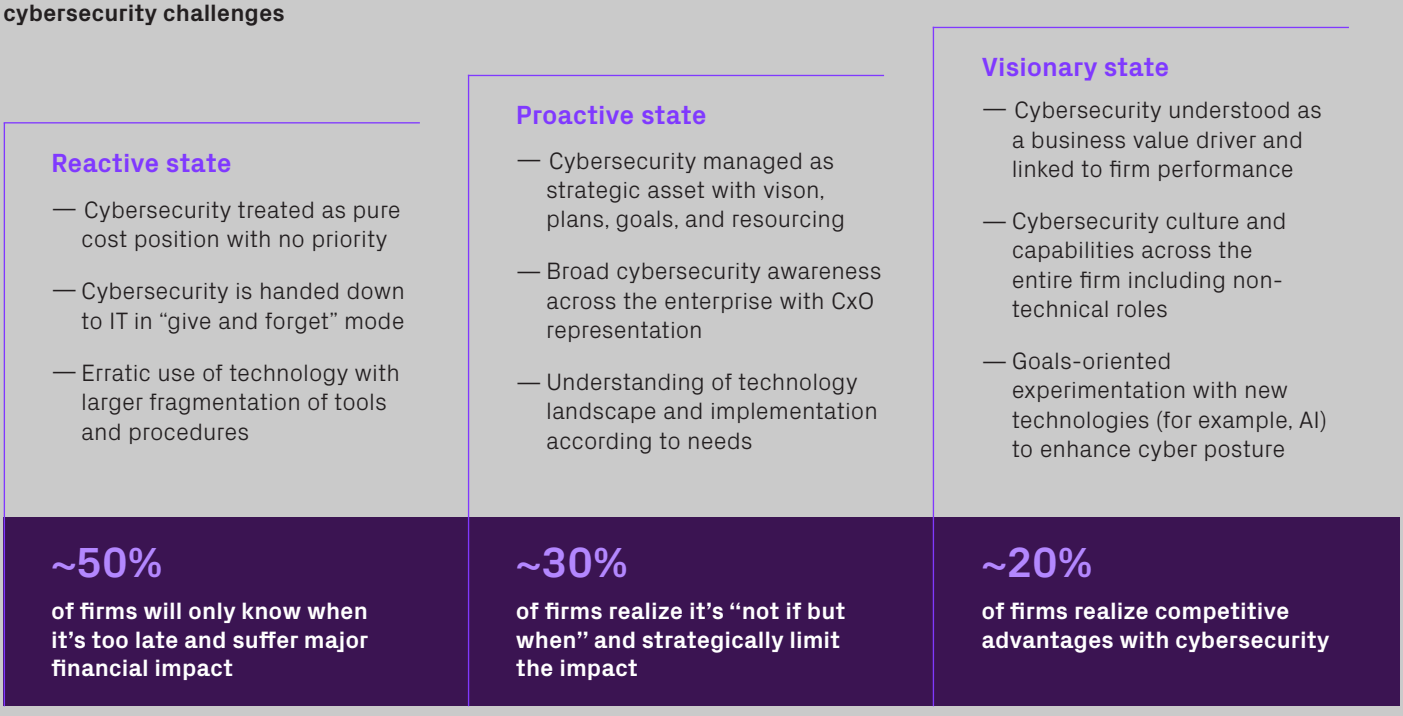
Today, cybersecurity is often bedeviled by cultural, talent, and communication challenges, particularly between the C-suite and the IT professionals. All too often, IT and cyber metrics fail to align with operational or financial outcomes, meaning business leaders don't give them enough attention.

As a result, cybersecurity is still largely reactive and tactical, rather than proactive and strategic, leaving enterprises overexposed. A lack of management support and understanding of the nature of their cyber risks, together with the recession and talent shortages, means expenditure is not being optimized for maximum impact on the situational cyber risk of the enterprise.

In many cases, an undeserved assumption and assignment of trust to products and services is introducing a significant form of cybersecurity risk. Lax practices associated with "bring your own device" programs have opened the door to corporate systems. Third-party support organizations are also often granted an unwarranted level of trust and excessive privileged access to key IT and OT systems. This large and unnecessary risk can be greatly reduced with nominal investment. Right-sizing privileged access should be an early priority.

To address these challenges, enterprises need to work their way through a three-stage process (see figure 2). The first stage is to implement key foundational concepts and controls that enable you to reduce your risk surface area and to firefight effectively. The second stage involves developing cybersecurity as an integral part of the culture and assignment of resources to address risk and to become a driver of business value. In the final stage, you are ready to judiciously select the emerging advanced technologies and techniques that promise cybersecurity excellence and focus more on superior operational integrity and the delivery of top- and bottom-line financial impact. In our interviews with expert practitioners, it was clear that very few businesses have made it to this third stage.

Figure 2
A three-step process helps address cybersecurity challenges



Source: Kearney Analysis

Stage 1: Getting the basics right
Begin by generating a full picture of the status quo: consider exactly who has access to organizational systems, infrastructure, and data and on what basis by identifying and challenging all areas of "assumed trust." Revisit your outsourcing arrangements to identify potential vulnerabilities. At the same time, the business should identify its critical assets (which are increasingly likely to be data and information), the threat to operational technology, and how much risk it can tolerate. For those critical information assets, consider the risks across the entire data life cycle: data can be compromised when it is created, transported, stored, consumed, and disposed.

Once you have a full picture, you can begin to prioritize your efforts and isolate functional system environments wherever possible, eliminating all unnecessary privileged accounts from production. Compartmentalize sensitive data and minimize copying or even access. It is also important to build awareness across the organization, while developing an incident preparedness and response playbook, which outlines how to explore and respond to a disruptive incident on the basis that it is likely to be cyber compromise.

These measures are the foundations of a modern cybersecurity strategy—if they are not in place, they should be given greater executive and management focus and effort and developed as a priority.

Stage 2: Build a cybersecurity culture to be proactive
Operational resources and capital investments are crucial to effectively counter cyber risks. But not all CEOs and CFOs recognize that cyber investments can significantly move the needle and generate an attractive return. Developing a business-led cybersecurity strategy framework will help to build that understanding.[1] This framework should clearly link the cybersecurity business case (based on a reduction in attacks and breaches) with the value assigned to the risk. Note, investment in cybersecurity should be dictated by risk, rather than compliance.

Cybersecurity metrics need to show both the impact of the cyber threat on core business functions and the impact of threat mitigation efforts over time. For example, the business needs to track the number of incidents where precautions failed to preclude realization of the threat, the time to contain and recover from each incident, and the business impact of the incident. Our research showed that the more mature cyber organizations had business-aligned metrics reviewed with the board and senior management.

The overarching goal at this stage is to build a security culture fully integrated with the business functions, and led from the top of the organization and practiced to the bottom. That will require security to be embedded in IT and development practices, together with the recruitment of appropriate talent and the upskilling of the existing workforce. Robust authentication, authorization, and "need to know access" processes are key to creating the necessary zero-trust capabilities. For more on this topic, see: Transformative technologies: zero trust—the new touchstone in cybersecurity.

During this stage, expertise in cybersecurity becomes a clear source of competitive advantage. It is now very apparent that cybersecurity capabilities are essential to maintaining the company's market position. As past investment decisions have yielded positive top- or bottom-line results, the business leadership recognizes that investment in cybersecurity will enhance overall operational integrity and improve historic performance by avoiding lost productivity.

Stage 3: Cybersecurity excellence: evaluating advanced technologies and techniques
In the third stage, the business will be employing advanced cybersecurity technologies and techniques, such as behavioral AI-enabled mechanics (rather than signature-based detection solutions) for advanced authentication and authorization. Using the power of data generated by users (within the boundaries of ethics and privacy), as well as third-party data, leads to greater accuracy, personalization, and more context for cybersecurity measures.

[1] Can be based on NIST or similar, but ideally is strongly linked to other more business-led frameworks, such as COBIT

Next steps—ask yourself some hard questions

Before you can build the kind of value-accretive cybersecurity strategy outlined in this article, you need to honestly answer some tough questions that will help you determine which stage you are in and what you should do next:

— Are you in denial? Does the leadership believe that the threat isn't significant, that the business isn't a target, or that existing defenses are adequate?

— Has the organization passed the buck to a third party? Have you effectively outsourced responsibility to cybersecurity to vendors, in the mistaken belief that it isn't strategic?

If you have answered "yes" to either of these questions, then you need to focus on getting the basics right. If not, consider the following:

— Do you know how much to spend on cybersecurity? What is the dollar value on your risk appetite, and can you weigh it against your investments in cyber?

— Do you consider security to be an intrinsic part of your business value?

If you have answered "yes" to these questions, then you may have successfully created a cybersecurity culture and are ready to explore advanced technologies and techniques (stage three).

Figure 3 summarizes the key actions you need to take to become a leader in cybersecurity.

As Steve Schuster, director for AWS security response and engineering, noted in an interview with Kearney, every organization will face a security issue at some point in time. But he stressed that "you can choose how to limit its effect." If you prepare well, you can minimize the impact on the company's reputation.

Figure 3
Several actions can help you become a leader in cybersecurity

Reactive state

1. Classify assets: identify critical assets to focus security investments.
2. Institute a privileged access policy and process for trusted partners.
3. Manage BYOD policies and monitor shadow IT.
4. Ensure malware protection on your devices.
5. Keep systems patched and up to date.
6. Back up systems and data and practice restoring.

Proactive state

1. Link cybersecurity risk to overall risk framework.
2. Involve senior management in review of cyber risks.
3. Gamify the culture: recognize positive security actions.
4. Create career paths that include roles in cybersecurity.
5. Conduct cybersecurity awareness training.
6. Go beyond: support development of cybersecurity skills and certifications.

Visionary state

1. Migrate from signature-based threat detection to behavioral-based, AI-enabled threat detection and response.
2. Implement software bill of material verification.
3. Adopt zero-trust principles throughout organization.
4. Apply behavioral and biometric authentication.
5. Use authorization policies based on trust scoring.
6. Establish policies of security orchestration, automation, and response.

Source: Kearney Analysis

How we can help

With the threat posed by cyberattacks increasing daily, and attacks growing both in volume and sophistication, executives must deploy the right resources from the outset to ensure their organization has the right frameworks in place to resist these threats successfully. That means taking proactive steps to develop a robust strategy that deeply engrains cybersecurity concerns within a firm's business processes—and, perhaps more fundamentally, within its entire culture.

Kearney and BinaryCore, Kearney's deep-tech solutions business, are supporting organizations with these challenges all around the world. Our global teams work to evaluate enterprises' existing cybersecurity capabilities and highlight where improvements can be made. By identifying vital assets, establishing companies' risk tolerance, conducting risk and impact assessments of key infrastructure, assessing supply chain cyber service level agreements, reviewing investment in cybersecurity, and evaluating existing governance procedures, BinaryCore can quantify a firm's exposure to the threats. With this information, we are working with organizations across the globe to co-develop and implement an appropriate cybersecurity strategy that contributes to greater organizational resilience. In so doing, we are helping leaders protect their companies' vital assets from the increasing number of bad actors who have the potential to inflict serious damage.

To discuss any of the themes outlined in this article, email us.

> Executives must deploy the right resources from the outset to ensure their organization has the right frameworks in place to resist cyber threats successfully.

Co-brand Authors

Dieter Gerdemann

Partner, Kearney, and
Co-Founder, BinaryCore, Munich
dieter.gerdemann@kearney.com

Michael Roemer

Partner, Kearney, and
Co-Founder, BinaryCore, Munich
michael.roemer@kearney.com

Clif Triplett

Executive Director, Washington, D.C.
clif.triplett@kearney.com

Guy Ngambeket

Consultant, Doha
guy.ngambeket@kearney.com

Steve Schuster

Director, Security Engineering and
Operations, Amazon Web Services
stschust@amazon.com

About BinaryCore

BinaryCore was born from a need to tackle complex technology challenges businesses face in an era when realizing the full value potential of software engineering and cloud usage will clearly distinguish the leaders from the laggards. But addressing these challenges requires radical step change—a willingness to unlearn what went before, an openness to new possibilities and partnerships, and the confidence to make bold decisions and rewrite the rules.

With deep technology expertise, powerful proprietary software, a sharp focus on the numbers, and a clear set of rules, we'll guide you every step of the way to transform your technology and talent set and put in place the infrastructure and teams needed to set you up for long-term success.

binarycore.com

About Kearney

Kearney is a leading global management consulting firm. For nearly 100 years, we have been a trusted advisor to C-suites, government bodies, and nonprofit organizations. Our people make us who we are. Driven to be the difference between a big idea and making it happen, we help our clients break through.

kearney.com

About Amazon Web Services

For over 15 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud offering. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 81 Availability Zones within 25 geographic regions, with announced plans for 27 more Availability Zones and nine more AWS Regions in Australia, Canada, India, Indonesia, Israel, New Zealand, Spain, Switzerland, and the United Arab Emirates. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

aws.amazon.com