accenture

THE CYBER RESILIENT ENTERPRISE

Four questions every CEO must ask to build a cyber resilient business

NO CEO WANTS TO WAKE UP TO NEWS HEADLINES REVEALING A DISASTROUS CYBER ATTACK ON THE COMPANY.

But they need a winning cyber-security strategy for reasons that go far beyond avoiding this worst-case scenario.

A STRONG FOUNDATION

Cybersecurity is not a matter of spending more and more on defense, only to see attackers continue to breach barriers and systems. It has become clear that the stakes are even higher than that: Cybersecurity is the bedrock of tomorrow's intelligent business. If companies are to succeed through the use of digital capabilities, to develop superior customer knowledge, unique insights and proprietary intellectual property—the hallmarks of an intelligent business—they will need a robust cybersecurity strategy to underpin it all.

Although companies have been improving capabilities in the past year, few have the strong foundation they need. Many are unprepared for the growing threats from increasingly sophisticated attackers that this new dependence on digital capabilities creates.

For companies that move quickly, this presents an opportunity. To seize it, business leaders must accelerate the development of a new set of capabilities needed to thrive in this digital era. It's about establishing leadership and governance for these capabilities. They need metrics that put the focus on the business context rather than technology-driven rules and regulations. And they should fund these activities appropriately, to ensure the delivery of these capabilities in a timely way. This all adds up to the creation of a "security first" culture.

Cybersecurity is more than a matter of guarding against a costly attack, important as that is. Effective cybersecurity is what gives the business the stability needed for everything it does—how it connects with customers, enters new markets, operates within its ecosystem. It enables leaders to embrace disruption and to proceed with confidence as they scale new businesses.

Getting it right is *essential*.

THAT INSECURE FEELING

Security professionals recognize the need for improvement on the path to business resilience. When we asked them to assess their companies on 33 critical cybersecurity capabilities, they rated themselves highly competent in only 19, on average—a significant improvement from the previous year when they rated themselves highly competent in 11 capabilities.[1] Still, there is plenty of room for improvement.

One challenge is that a heavy focus on security compliance drains organizational attention from developing more business-relevant capabilities. Companies invest in the technologies and resources they need to ensure this compliance, but the relative business value is limited. Almost every major retailer that has suffered a data breach has complied with payment card industry standards—and yet the breaches have happened and continue to happen.[2]

Another challenge is the question of who is responsible for cybersecurity. Typically, that role is filled by the chief information security officer (CISO). But many CISOs have visibility only into a limited aspect of the enterprise. Most focus on the corporate level and do not have oversight of research labs, joint ventures, subsidiaries, or manufacturing plants. Ideally, the CISO should work more closely with the CEO and board to help answer strategic questions such as: Is the business ready for what comes next? And can we build on our security to grow the business with confidence?

In many companies, the board needs to be more engaged. Currently, 32 percent of security budgets are approved by the CEO and 27 percent are board-authorized—a big leap from the 22 percent and 11 percent figures, respectively, of the previous year.[3] But that rapid upward trend must continue. Board-level knowledge of cybersecurity risks is critical, and overseeing budgets ensures that directors are carefully scrutinizing the issue.

Technology can help close the capability gap, but there are no quick or easy fixes. A typical organization is managing more than 55 security tools and can knock on the doors of at least 1,600 vendors in the cyber-tech sector for help. Some organizations have hundreds of security tools. In short, there is a tremendous amount of technological complexity for companies to sift through, and yet the hacks, breaches, and attacks continue to grow.

These issues—lack of deep capabilities, the compliance mind-set, the need for a stronger CEO–CISO relationship, gaps of knowledge on the board, and huge technological complexity—are holding companies back. They are preventing organizations from attaining the competitive agility they need and from innovating at speed and at scale.

How can companies accelerate the development of their cybersecurity and business resilience capabilities?

NEW CAPABILITIES FOR THE CYBER-RESILIENT ENTERPRISE

To accelerate the development of security capabilities, leaders must develop a healthy paranoia. Like business competitors, cyber criminals and more advanced adversaries are innovating continuously. To bring about the cyber-resilient enterprise, we believe changes are necessary in four areas: in leadership and governance, in the organizational culture, in debates about funding and in the way security is measured and monitored.

LEADERSHIP AND GOVERNANCE

Do you really understand what is at stake for the business?

CEOs and boards are ramping up their engagement in cybersecurity—to a point where they are assuming accountability for the cyber risks facing the company. But, with security programs only covering 67 percent of the organization on average,[4] most have much more to do, and their relationship with the CISO is a critical component of the right kind of engagement.

A series of questions can help you determine whether you are fully engaged in taking on the challenge of cyber risk; here are a few of the most important:

- Does the CISO have oversight of more than just the corporate office—of functions, subsidiaries, joint ventures, labs? Put another way, over which areas of the business does the CISO *not* have oversight?
- For new business initiatives that will increase cyber-risk, have you involved the CISO in discussions to advise, coach and address the risk?

- When considering the adoption of new technologies, have you consulted the CISO to identify and develop solutions for security concerns?
- In discussions with your CISO, do you feel you are speaking the same language? Does the CISO understand where you are taking the business?
- Do your business leaders hold regular discussions with the CISO?
- What is the nature of discussions between the CISO and business leaders—do they focus on technical and compliance issues or on the risk implications for business success?
- Have you observed changes in behaviors, program design and business decisions as a result of those interactions?

The bottom line is that the CISO must become a business advisor to leadership. CISOs must prepare business leaders to think differently about security, because they set the tone for the whole company. Only top leaders can ask the hard questions, understand that end-customer expectations are way ahead of security-industry norms, and put across the idea that “good” is not good enough.

CULTURE

Do you put security first?

In other words, are you paying lip service to security or is it really at the front and center of our strategy?

Many companies believe that their cultures already "get it" when it comes to security. For example, 83 percent of survey respondents said they have "completely embedded cybersecurity into their cultures." And yet, 71 percent report that cyber attacks remain "a bit of a black box." They do not know how or when they will affect the organization.[5]

A big part of a security-first culture is having the right mind-set. At the C-suite and board level, cyber resilience should be in the same "box" as operational performance management. Just like measuring the profitability of the business units, security must be a strategic priority tracked and reacted to as part of the tempo of normal business management. It is a new competence that needs to be built, just like manufacturing excellence or personalization in digital marketing.

This mind-set needs to spread throughout the organization and serve as a spur to the proper actions. Line management must understand that they have a primary objective: Data protection for the customer and the company's digital assets and operations. Fail at these and all else is irrelevant. The same is true for the front lines—but only 13 percent said that investing more in cybersecurity training was a top priority.[6] Cultural change must be backed by action and investment.

FUNDING

How much is the right amount?

Never an easy one to answer, the question of funding has two distinct aspects.

First, are you "brilliant at the basics"? That is, have you invested properly to resolve challenges of any magnitude—from intruders who want to target a particular customer, use our infrastructure, or even trumpet a cause, to attackers after our "crown jewels," the data that is most critical to our operations and our differentiation in the market.

Getting the basics right is not easy. Otherwise we would not see successful ransomware attacks such as WannaCry and Petya, the majority of which were avoidable with basic security hygiene like keeping your IT environment up to date. In fact, the official report following a major attack on a government agency noted that it "could have been prevented if 'basic IT security' precautions had been taken."

Companies must do more to understand and prepare for the many potential intentions of cyber attackers and also to "harden" their high-value assets. They must make it as difficult as possible for attackers and limit the damage when they do breach defenses.

The second question for funding is about innovation to improve your cybersecurity and data protection. With all the new technologies and new ways of getting in, the cyber attackers are finding it far too easy. Companies need to lower the cost (or at least slow down the increases) of cybersecurity while improving the overall capability. The only way to

do this is to innovate. When the attackers find a way into your company, you need to employ breakthrough innovations to prevent or disarm those schemes, including:

- Advanced cyber analytics and user behavior analytics to help identify unusual activity;
- AI and machine learning to capture expertise and spread it throughout the organization;
- Blockchain to shore up security in your supply chain by enabling you to monitor goods in transit and analyze suspicious transactions;
- Advanced identity and access management—think two-step authentication and biometrics—to make it harder for the attackers to impersonate authorized personnel.

Breakthrough innovations result from sound ecosystems. Think of the startup community as your route to innovation and experimentation. Once you find the partners that will drive the most value in your security mission, you need to be able to scale rapidly across the organization.

To put it in financial terms, the right level of funding for cybersecurity understands the critical importance of the brilliant basics and the need for cutting-edge innovation. Both sides of the equation are “must haves.”

METRICS AND MONITORING

Are you measuring your security efforts for business relevance?

The metrics used in the past will not help in the future. Whether you are "low, medium, or high" on compliance scores does not tell you enough about the risk to the business. A senior security executive for a bank told us what is needed instead: "We do not present the board project plans on encryption. We present the board with metrics on data protection for the customer. And we don't have metrics around patching. We have metrics around maintaining the integrity of our production environments."

In other words, companies need a business-relevant scorecard on security. And the explanation of the metrics must address business-critical questions, such as:

- Can the business protect online customers so they continue to buy?
- Can we protect our most important assets—contracts, pricing sheets, M&A data?
- Can we prevent employees from stealing from the company?
- Can we protect our intellectual property?

In addition to creating the right scorecard, business leaders need to improve their monitoring of cyber threats. They need to develop "muscle memory" by taking part in crisis drills and working through attack scenarios. Such practice helps senior leaders to track improvements and lessons learned, and be prepared, when a threat

hits, to respond immediately. Only 56 percent of companies say they are competent at practising how to respond to cyber attack scenarios.[7] And while most security teams run crisis drills for themselves, few engage the top level of their companies.

This is a recipe for trouble. As that same bank's security executive told us: "Generally what happens during a crisis is chaos, unless people have gone to practice enough times" so that they know how to act. The executive created "playbooks" that cover everything from who needs to be contacted, who initiates crisis management calls, the agenda of those calls, and the desired outcomes—and led people in senior positions through the experience of using the playbooks.

For companies that are serious about building a cyber resilient business, rethinking metrics and stepping up monitoring capabilities are critical activities.

THE PATH TO BUSINESS RESILIENCE

We have covered four areas of "necessary change" for the creation of the cyber-resilient business. Clearly, they are closely interrelated.

As always, resolving the challenges starts with leadership—in this case, the web of relationships between the CEO, the board, and the CISO. Everyone must be speaking the same language. When leadership is on the same page, it becomes much easier to see where funding is needed, and at what levels. Bring together sound leadership and the right resources, and the organization's culture begins to change. A security-first culture will constantly monitor and measure the right elements—the most business-relevant things—to help the business embrace disruption, safely.

The CEOs of big organizations are leading a wise pivot to the new—an essential pivot for long-term survival. But this pivot brings risks and an increased "attack surface" that could harm the critical digital assets and operations of the business. Business leaders see the challenge; they must now engage more directly to own it. In the future, the only truly resilient business will be one that is cyber resilient.

ENDNOTES

1: 2018 State of Cyber Resilience Executive Summary
2: Achieving Data-Centric Security
3: 2018 State of Cyber Resilience Executive Summary
4: Ibid.
5: Ibid.
6: Ibid.
7: Ibid.

CONTACT US

Omar Abbosh
Chief Strategy Officer
Accenture

Kelly Bissell
Senior Managing Director
Accenture Security

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown.

ABOUT ACCENTURE RESEARCH

Accenture Research is a global team of industry and digital analysts who create data-driven insights to identify disruptors, opportunities and risks for Accenture and its clients. Using innovative business research techniques such as economic value modelling, analytics, crowdsourcing, expert networks, surveys, data visualization and research with academic and business partners they create hundreds of points of views published by Accenture every year. Visit **www.accenture.com/research.**