accenture

BUILD PERVASIVE CYBER RESILIENCE NOW

Securing the Future Enterprise Today – 2018

Contents

COMPANIES ARE RACING INTO THE DIGITAL FUTURE—ADOPTING TECHNOLOGY-ENABLED OPERATING AND BUSINESS MODELS THAT DRIVE BOTTOM- AND TOP-LINE GROWTH.

They are not prepared for the new cyber risks that come with the connected, data-driven future enterprise. To be cyber resilient, organizations need to infuse security into everything they do—and every new thing they are preparing to do.

When everything is digital, everything is at risk

Companies everywhere are betting on a wholesale shift to tech-enabled business and operating models that promise to deliver bottom-line savings and top-line growth. They are building an enterprise that is faster, smarter, leaner, and more responsive—what Accenture calls "rotating to the new." This future business relies upon constant, intimate digital connections with suppliers, partners, and customers to stay relevant and competitive. It uses intelligent technologies and big data in all facets of business operations—from C-suite decision making to crafting custom offers for Internet shoppers in pursuit of profitable growth. It deploys autonomous machines and automated processes to simultaneously augment the workforce, raise productivity and decrease cost.

The connected, intelligent, and autonomous enterprise comes with additional cyber risk. All that sensitive data, connectivity, and automation multiplies the opportunities for hackers by expanding the "surface area" exposed to cyber attack. And, because digital systems are so embedded in daily operations, the potential damage from even a single security incident is magnified.

The future is arriving now, along with more cyber risk

Virtually everything that makes the future business more efficient, fast-moving, and competitive involves some type

of digital system or network connection that is open to the introduction of corruptive elements and vulnerable to incidents. Both the data and the programs that provide intelligence, for example, can be hacked.

A subtle change in an AI algorithm or the data used by a machine learning system—to evaluate loan applications, for example—might go undetected, leaving the company to take actions based upon tainted output. Nefarious interference in a robot or an autonomous vehicle system could be life-threatening. As many companies have learned the hard way, breaches of customers' sensitive and personally identifiable information can not only disrupt business, but also destroy the trust needed to retain customers (both B2B and consumer) in the new world of digital business.

CONNECTED
ALWAYS ON, ALWAYS VULNERABLE

The future business relies on 24/7 connectivity to carry out internal processes, work with partners, and reach customers. Companies are linked electronically across value chains and supply chains with a growing universe of suppliers, partners, distributors, customers, and other external parties—increasingly over wireless networks and over long distances. In addition, with the rise of the Internet of Things (IoT), companies are also using digital connections to retrieve data and manage equipment in the physical world.

In a recent Accenture survey of more than 1,400 C-suite executives, including Chief Information Security Officers

(CISOs), respondents cited several types of technology-related connections that they believe will raise cyber risk as they are more widely adopted. Topping the list is IoT technology, which 77 percent of respondents said will increase cyber risk moderately or significantly. Companies are installing IoT technology to control factory machines and manage physical environments—turning off the lights and heat in a meeting room when sensors detect that it is unoccupied, for example. IoT is also being used extensively in supply chains to increase operational efficiencies, manage and track assets and monitor vital processes; IoT also helps companies get a better grasp on quality control, on-time deliveries, and product forecasting. Cloud computing—using remote computing and storage facilities and services—was cited by 74 percent of respondents as posing a growing risk. Increasingly, companies rely on cloud setups to gain greater flexibility in IT operations and to access specialized services, such as AI analysis. Cloud computing is also used behind the scenes in many smartphone apps to do the data crunching that a phone can't, creating another potential vulnerability in the Bring Your Own Device (BYOD)/ virtual work environment.

Top executives are also highly concerned about the potential dangers of sharing data with third parties. In our survey, more than 70 percent of respondents said they expect data exchanges with strategic partners and other third parties to raise cyber risk, and 80 percent of C-suite leaders anticipate that the number of third parties and strategic partners in their ecosystems will increase in the next three years.

Companies also expect to make and sell many more connected consumer devices—everything from connected cars and "smart"

appliances to wearable health monitors and even Internet-enabled pacemakers. These products introduce potential catastrophic cyber risks—expanding the risk from monetary and reputational loss to potential loss of life and physical disruptions.

INTELLIGENT
MORE DATA BRINGS MORE RISK TO PRIVACY AND IP

Intelligent systems use a combination of advanced technologies, such as AI, and large data sets to take on tasks once performed by humans, and to do things that humans cannot easily do—like finding hidden patterns in massive files of social media data that point to changes in consumer preferences. Today, intelligent systems enable any business to acquire the analytical sophistication that was once reserved for the few large organizations that could hire ranks of data scientists. Using machine learning, for example, a visual processing program can teach itself how to sort parts on an assembly line or "listen" to a caller and answer a simple service question. In management, intelligent systems are helping companies make data-driven decisions.

An increasingly important application of intelligent technologies is to drive sales by making the company "hyper-relevant" to customers. Gathering data from digital "touchpoints" (such as online stores), social media, and other online activity, companies can compile sophisticated profiles of individual consumers and detect emerging market trends. Using AI and machine learning, companies can extract ideas for new ways to boost sales—a tweak in pricing, a design refresh, or a custom offer

for specific shoppers. Behind the scenes, intelligent systems enable continuous improvement in operations—optimizing how production machinery is used or raising customer satisfaction in the call center by analyzing performance data, for example.

Companies represented in our survey are well aware of the risks that they are assuming with the wider use of intelligent technologies. Three-quarters of executives said AI would raise cybersecurity risks moderately or significantly. For example, the same AI technology that enables banks to create sophisticated profiles of individual consumers to customize loan offers can also be used by hackers to track consumers' online activity to steal account passwords.

Given the intersection of AI, machine learning and big data within businesses, both security and privacy protection will become stretched as risk increases. Protecting larger amounts and new kinds of sensitive data is a major concern for executives. Three-quarters of respondents said they believe that storing business-critical information, such as corporate strategy, trade secrets, and intellectual property (IP) on their systems will increase cyber risk; 72 percent have similar concerns about the risks they face in trying to protect sensitive customer data. Companies collect more information about consumers and in many more categories than ever—demographics, finances, buying histories, and lifestyles—to craft the customized offers and better customer experiences that can stimulate incremental sales and build loyalty. If such data is stolen or abused, companies know that they could suffer severe damage to their business, including financial loss, fines, and reputational loss.

Given the intersection of AI, machine learning and big data within businesses, both security and privacy protection will become stretched as risk increases.

AUTONOMOUS
SELF-DIRECTING SYSTEMS NEED PROTECTION

In the future business, a good deal of work is done autonomously—from robots and self-driving vehicles, to algorithms that enable companies to interact with intelligent systems without human intervention. The most obvious form of autonomous production is robotics—the cognitive system used to perform difficult, repetitive, or dangerous tasks in production processes. More than 60 percent of respondents say robotics will be a growing source of cyber risk. As was the case with IT systems, security was an afterthought in the creation of robots. Unlike IT systems, the danger is higher, as many robots are self-directed.

Autonomous machines are spreading rapidly beyond the factory. Flying drones are being dispatched to inspect power lines and refinery pipes. In warehouses, autonomous machines are moving pallets and roaming the aisles, counting inventory.

In the back office, autonomous systems are multiplying as robotic process automation is introduced to save time and cost and improve quality by standardizing and streamlining a wide range of business processes. Often, this involves autonomous machine-to-machine communication, such as

automatically generating an order in a supplier's computer when the procurement system signals that inventory is running low. Businesses also rely on application programming interfaces (APIs), which two-thirds of respondents say will increase cyber risk. Open APIs used in platform-based business models, such as the Apple app store or the Alibaba eCommerce platform, enable third-party developers to interact with the company's systems and data to design their own applications—such as iPhone games or AliExpress shopping apps.

A less obvious form of autonomy involves employee activity. Increasingly, companies are using virtual work arrangements for contractors or employees who work remotely, often using their own devices. These "mobile workers" interact with company systems and data over public networks, raising cyber risk. More than two-thirds of respondents cited the virtual work environment and the mobile workforce practices as a source of greater cyber risk.

Today's security strategies are winning—the *last* war

Companies are making gains against cyber crime. According to the latest Accenture State of Cyber Resilience Report, companies reported that only one in eight focused attacks got through in 2018, compared with the one in three that caused considerable disruption to organizations just over a year ago.[1] As impressive as this progress seems, most of the victories are related to known threats on existing systems. Meanwhile, the future is arriving before companies have developed a broad perspective on the cyber risks, responses, and remediation plans that are required in the new business environment. In short, we are winning yesterday's war, but we are not building adequate protection against the risks created by the connected, intelligent, and autonomous systems of the future business.

Today's security approach will not be enough to win tomorrow's battles. For a start, in most companies, security remains a separate function—one that is dedicated to shielding core IT systems and sensitive data. Also, standard security strategies focus on detecting threats and minimizing damage, rather than making digital products and processes safer by design. The connected, intelligent, autonomous business needs pervasive cyber resilience—with proven methods for keeping cyber attacks from crippling the business and security baked into everything the organization does. Security expertise must be dispatched to the front lines and security must be embedded not only in IT, but in product design, business processes, and the daily work of employees as well.

We are winning yesterday's war, but we are not building adequate protection against the risks created by the connected, intelligent, and autonomous systems of the future business.

Closing the gap between risk and protection

There is a growing gap between the risks that companies are assuming and their cybersecurity posture. Companies are not hesitating to race ahead with investments in new tech-enabled ways of doing business, often in response to competitors and "disruptors" in their markets. As noted, they have a strong sense that the future business has far greater cyber risks. But there is a disparity between what C-suite executives say are the emerging areas of concern and the cybersecurity strategies employed to enable protection. For example, while companies say that the growing volume of data exchanged with third parties is a risk, few companies attempt to ensure data integrity beyond their own operations: 45 percent of companies rely on the protocols of the third parties or simply trust third parties to protect information that they share.

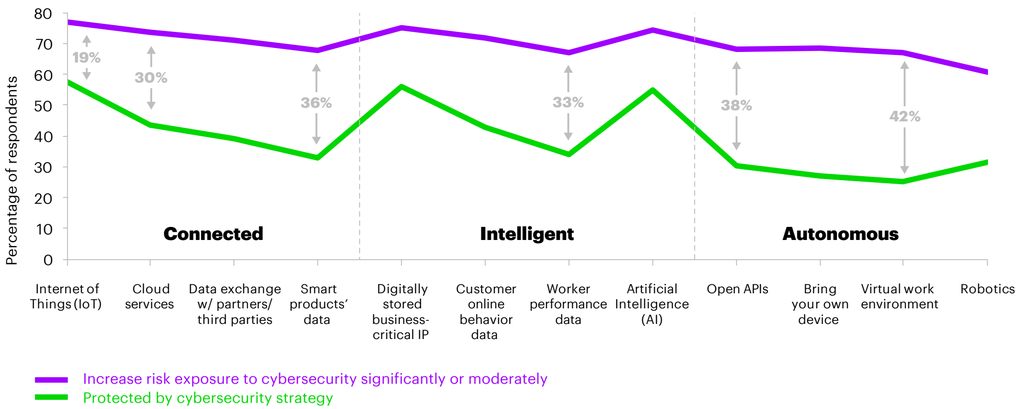
As Figure 1 illustrates, our survey data exposes a consistent pattern of gaps between awareness of growing risks and the protection afforded by current cybersecurity strategies. For example, 74 percent of respondents said cloud services will raise cyber risk, but only 44 percent said that cloud technology is protected by their cybersecurity strategy—indicating a wide gap of 30 percent, which is also the approximate gap,

on average, for all new technologies and business initiatives surveyed. The largest gaps are found in smart products, open APIs, protecting employee performance data, and risks associated with virtual work arrangements.

FIGURE 1

Gap between increased risk and cybersecurity protection

Where current cybersecurity strategy is not keeping up with emerging risks



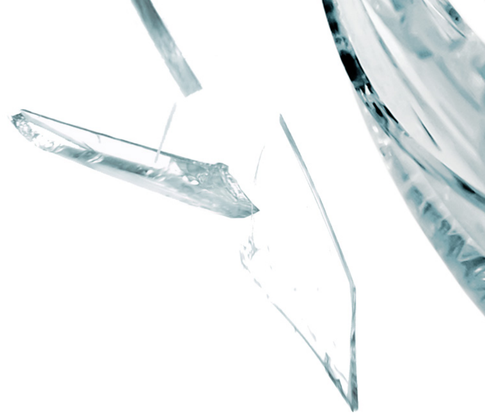
Source: Accenture Survey 2018, see "About the research"

To close the gap between current capabilities and future cyber resilience needs, companies must update the way they plan and execute cybersecurity. Companies today are waging war with outdated, backward-looking battle plans. For example, more than half of companies (52 percent) base their cybersecurity investments solely on today's known risks and cybersecurity needs, and do not consider future business needs in the investment plan.

In general, companies are not governed, organized, and managed to deal with the pervasive risks of the future business. Responsibility for security is left largely to the CISO and the cybersecurity team. Business-unit leaders are rarely asked to build security into product designs or other offerings—or held accountable for cybersecurity. Business-unit leaders are accountable for cybersecurity in only 22 percent of the organizations surveyed.

While most companies have hired a CISO or assigned cybersecurity to a C-suite executive, such as a CIO, often, these leaders have limited impact beyond the security organization. Nearly half of respondents say the CISO is brought into discussions only after a new business opportunity has been agreed by top management, for example.

Companies are doing little to spread security knowledge among employees and create a "security-first" culture that will support pervasive cyber resilience. In our survey, only half of respondents said all employees receive cybersecurity training upon joining the organization and then receive regular updates throughout their employment. Only 40 percent of CISOs said establishing or expanding an insider threat program is a high priority.



How to protect the future

To make the future business cyber resilient, companies must prepare for the risks that come with new business models and intelligent technologies, such as artificial intelligence and machine learning. Machines are now attacking machines. Companies not only need to link security with the business, they also need to employ the same intelligent technologies (AI, machine learning) that the business—and the hackers—are using. Three-quarters of C-suite respondents in our survey expect cybersecurity risks to diminish substantially in the next few years, thanks to new cybersecurity technologies.

New technologies alone will not do the job. To build the pervasive cyber resilience needed for the intelligent enterprise to grow safely, companies need to embed security into everything that they do. Companies must instill a “security-first” mind-set—connecting security to the business, making security everybody’s job, and extending protection beyond the boundaries of the enterprise. Companies can start by developing a coherent cyber strategy and investment plan that focuses on the key issues of data governance and protection. Companies will need to make structural changes to disperse security expertise and accountability across the organization. They will need to educate the workforce and customers, and work with strategic partners, third parties, and industry alliances.

1) Make your business leaders Resilience Leaders.

Cybersecurity must be woven into corporate strategy, product design, budgets, and permeate down to daily business activities. Today, it remains largely siloed and separated from the business. To adjust this will require organizational changes and investments directed by top leadership.

Include security in business strategy. Security must be in the room when strategy is being decided and options are being weighed. In our survey, only 38 percent of respondents say the CISO is brought in before a new business is considered. When security is an afterthought or an add-on, the new business will not be truly cyber resilient. The potential ramifications of cybersecurity breaches are on par with the damages that companies face from other financial and business risks and should get the same strategic attention from CEOs and boards.

Extend security responsibility to the frontline. Today, in most companies, security experts are not on the ground when business units develop new products, services, and processes—all of which involve some sort of cyber risk. In our survey, 73 percent of respondents agree that cybersecurity staff and activities need to be dispersed throughout the organization, but cybersecurity remains centralized in 74 percent of companies. Moreover, there is little indication that C-suite executives expect to shift more responsibility for cybersecurity to business units: 25 percent of non-CISO executives say business-unit leaders are accountable for cybersecurity today and a similar number say business-unit leaders should be responsible in the future. It takes leadership to spread accountability for security within the

CISOS ACROSS THE BUSINESS

General Electric runs many different businesses that operate in markets around the world and leadership is acutely aware of the challenge to make every business unit cyber resilient. Global CISO Nasrin Rezai has dual responsibility for enterprise as well as product security, reflected in her title of Global Chief Information and Product Security Officer. The company has appointed multiple CISOs for regions and businesses, all of whom report to her. A primary goal for these frontline CISOs is to weave security into the product life cycle, ensuring that products are secure and the people and organizations using them are protected. GE's approach also makes it easy for CISOs to share best practices and knowledge about cyber risks, which differ from one business unit to another and between regions.[2]

business. GE, for example, has created CISO roles in business units and geographies to disperse security expertise throughout the organization (see "CISOs across the business").

Make wiser bets on future-resilience spending. Getting protection for the future business right starts with budgets and planning. Today, only 13 percent of companies include assessments of future needs when allocating money for cybersecurity—the rest focus only on known risks. Only in fewer than one-third of companies surveyed do the CISO and business leaders even collaborate on a cybersecurity plan and budget. Not surprisingly, the companies that look at future needs are having a richer dialog about security needs (see Figure 2). Respondents say their companies craft budgets and strategy to protect their most valuable assets, but their priorities tend to skew toward protecting IT systems and critical assets, such as servers; new digital systems, data, and connections, are not getting the same attention or investment.

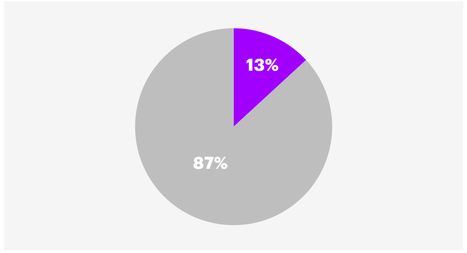
Fewer than one-third of companies have a strategic cybersecurity plan created collaboratively with security and business leaders that indicates where to allocate budget.

FIGURE 2

Investment readiness and internal collaboration

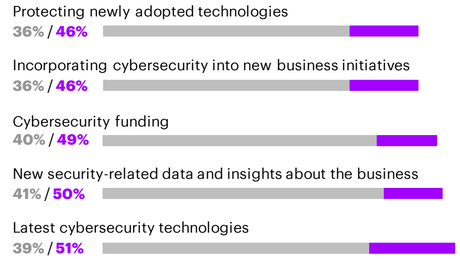
Companies that invest in future needs as well as current needs have a broader perspective

Organizations' approach to determine cybersecurity investment



...CISOs and CXOs from organizations that invest in future needs, are more likely to confer on strategic topics

Topics of discussion between CISO and CXO



Investment is based on assessment of **past, present and future** cybersecurity needs

Investment is based on assessment of **past** or **present** cybersecurity needs and associated known risks

Note: Key is the same for both charts

(Numbers denote percentage of respondents) – **Source:** Accenture Survey 2018, see "About the research"

2) Support the security leader as a trusted business enabler.

Our research shows that CISOs are well established in the large companies (more than US$1 billion in revenue) we surveyed. Yet, few CISOs have the authority and visibility they need to influence business units and build cyber resilience into their strategy. This is due to many factors, including a lack of understanding of cyber risks among business executives, and sometimes, a failure by CISOs to take the initiative to collaborate: only 40 percent of CISOs say they always confer with business-unit leaders to understand the business before proposing a security approach. For CISOs to function as sought-after collaborators and trusted partners—not just the chiefs of the security police or innovation gatekeepers—they need to work closely with business units to enable the transformation and growth initiatives envisioned by top leadership. This will require CISOs to become more business savvy. To succeed as business enablers, they need the correct priorities and relevant measures of success.

Upgrade security talent to link with business units. While CISOs and other security professionals are doing a good job defending companies against well-established threats, new roles and skills are needed to implement pervasive cyber resilience. One approach that reflects the wide-ranging needs of the future business is the creation of a “Chief Digital Trust, Security, and Resilience Officer,” who can oversee security in the broadest possible context and serve as a bridge between security and business units, as well as with the CEO and board. In our research, more than three-quarters of respondents agreed that some kind of high-level role is needed to be a

bridge between security and business units. Nearly half of CISOs acknowledge that their responsibilities for securing the organization are growing faster than their ability to address security issues. Companies can also consider adding specialized security talent, such as security leads for consumer data and product design. These experts would work with business units to build security into new offerings, practices, and processes.

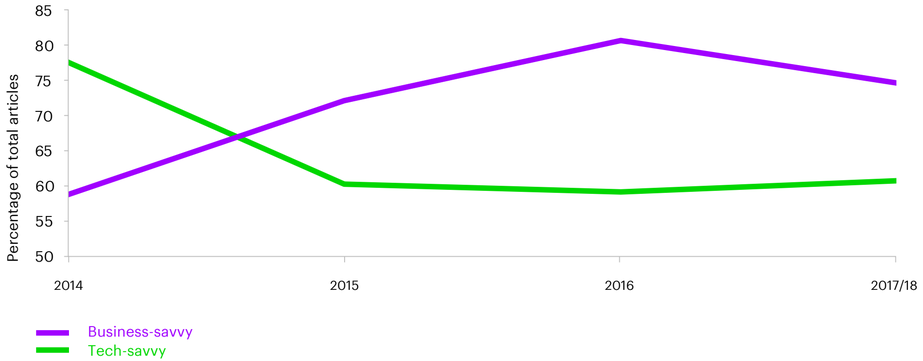
Nearly half of CISOs surveyed acknowledge that their responsibilities for securing the organization are growing faster than their ability to address security issues.

Ensure that CISOs are business-savvy. Four out of five survey respondents say that the CISO role will evolve from "authoritative enforcer" to "influencer/coach" for C-suite colleagues. To do this, the CISO needs to speak to business leaders in their own language. Both CISOs and business executives say that CISOs need to be more business-savvy. Today however, only 46 percent of CISOs believe that they understand the language of business. There is growing consensus that CISOs must become competent business advisors and this is reflected in recent media coverage of CISO hiring and management moves (see Figure 3). Increasingly, the discussion in CISO appointments emphasizes the role of CISOs as business partners, using terms such as "business advisor" and "collaborator" and fewer terms that reflect technical abilities, such as "security architect" and "IT security."

FIGURE 3

Next-generation CISO is more business-savvy

Proportion of total number of articles that make reference to each category of skills



Source: Factiva – **Dates:** 01/01/2014 to 04/18/2018 – **Total number of articles:** 1889 – **Subject:** Management moves OR Recruitment

Provide clear guidance on cyber priorities. When asked what they need to know from the C-suite and board to understand how the business links to their responsibilities, CISOs said the top two priorities were to identify business areas where attacks would cause the greatest business loss and identify the company's most valuable digital assets. Yet, only about half of executives surveyed said that their cybersecurity policy defines a formal process to identify business-relevant risks and high-value assets. AT&T's Security Advisory Council, for example, is a forum that brings security and business leaders together to address strategy and security priorities. (See "A group effort").

A GROUP EFFORT

At AT&T, the Chief Security Officer (CSO) leads the Security Advisory Council, a group of key business and functional leaders that meets regularly to discuss corporate security strategy, vision, and concerns. The CSO works in partnership with AT&T business unit leaders to evaluate threats, determine protective measures, create response capabilities, and audit compliance with best security practices. AT&T has also funded a Security Research Center under the CSO, which works on future security issues in communications and computing.[3]

Redefine measures of success. As the CISO becomes a stronger partner with business leaders, the metrics of cybersecurity success need to expand. Three-quarters of respondents said that their companies use simple pass/fail metrics that are designed for performance audits. Conventional metrics for the CISO and the security team encourage threat detection and response, but metrics need to evolve to capture additional criteria, such as how well the cybersecurity function is protecting the risks associated with future business or how well it is spreading cyber-resilience knowledge to the frontline. Today, more than two-thirds of respondents concede that cybersecurity metrics are too technical for business leaders to understand.

3) Make employees part of the solution.

By accident or intent, employees enable many cyber attacks. The accidental publication of confidential information by

employees and insider attacks were major concerns for executives polled in the Accenture 2018 State of Cyber Resilience survey, and were second only to outside attacks in executives' list of concerns.[4] Yet, little is being done to invest in employee training and enforcement.

To reduce breaches and embed cybersecurity into the fabric of the organization, companies first must make clear that employees are accountable for security. Only 16 percent of CISOs in our survey said employees are responsible for cybersecurity today (although 26 percent of non-CISO executives said employees are accountable). Security experts must not only provide ongoing training and skill reinforcement (with phishing tests, for example), they must also give employees the tools and incentives to assist in defining and addressing risks.

To enact an effective insider threat program, the CEO must rally human resources, learning and development, legal and IT teams to work closely with the security office and business units.

More than two-thirds of respondents concede that cybersecurity metrics are too technical for business leaders to understand.

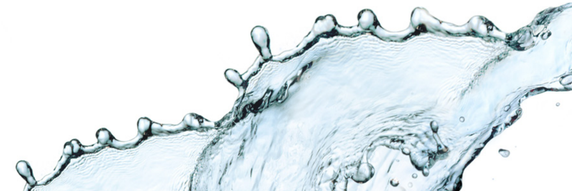
Train and reinforce safe behaviors. Without a security-first mind-set, employees will remain the weakest link. New work arrangements—greater use of contractors and remote work—only make the need for employee training more urgent. Yet, training employees to think and act with security in mind is the most underfunded activity in cybersecurity budgets.[5] Some

companies, however, are not stinting on training. Since 2012, for example, Cisco has funded a training program for all employees called “Security Ninja,” which also includes ongoing skill-reinforcement activities (see “Calling all employees” on the next page).

Build cybersecurity champions. With the right approaches, employees can become cybersecurity champions and advocates. Gartner estimates that 35 percent of enterprises will implement a security champion program by 2021, up from less than 10 percent in 2017.[6] Cybersecurity champions can not only act as advocates for security across the organization, they can also provide feedback to the central team on the effectiveness of security programs.

Reward “security-first” behaviors. Reward employees who report malicious activity or criminal colleagues, and offer incentives for security advocates. In our survey, only 41 percent of companies offer incentives for business leaders who are committed to cybersecurity. Rewards will help stimulate the desired cybersecurity hygiene.

Maintain strong defenses. Training and reinforcement can reduce the risk of employees accidentally helping cyber criminals. To catch employees who are actively pursuing or abetting cyber crime, companies can monitor employees, in addition to using standard data protection techniques, such as encryption and rights management. User and entity behavior analytics (UEBA) systems, for example, can flag suspicious employee activity, such as unusual file transfers that could indicate criminal intent.



CALLING ALL EMPLOYEES

Getting all employees to join the cybersecurity effort requires a big commitment. Network equipment supplier Cisco is crafting a “horizontal” cybersecurity culture that weaves cybersecurity into every part of the business. All employees go through the “Cisco Security Ninja” training program, in which employees who master the basics earn a “white belt” certification. Software developers, engineers, and managers can earn more rigorous green, brown, or black belt certification with modules customized to their roles, which focus on building products and services in a secure way. Cisco continually reinforces a defensive mind-set and best practices by, for example, sending fake phishing e-mails to employees to test their awareness. If the employee clicks on the malicious link, it redirects them to Cisco’s Phish Pond, where the information security team explains what they did wrong. Cisco said the Phish Pond initiative has reduced clicks on malicious links by more than 60 percent.[7]

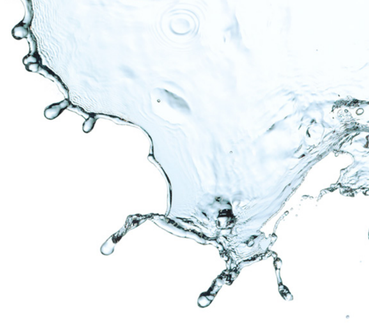
4) Be an advocate for protecting customers.

Companies in our survey say that managing customer requirements (for data protection) is the second most urgent priority for their cybersecurity investments, just after their top priority of preventing high-profile incidents. Three-quarters of respondents expect the use of sensitive or confidential customer information by their companies to increase. Yet, only 43 percent of respondents say customer data is protected by current cybersecurity strategy.

Companies will need to do a better job on this front, both because they will be forced to do so through new regulations and because it is essential for maintaining trust—which is crucial in digital business. We think companies can go beyond compliance and become advocates for their customers when it comes to protecting data. They need to:

Prioritize security by design. Digital trust and privacy are becoming major factors for consumers in their purchase decisions. Companies must prioritize security in the design and development process of connected products and services. For example, Apple announced that it will make it harder to get data from iPhones in the absence of proper authorization. The method, called a USB Restricted Mode, will close down access to data through iPhone's Lightning port if the phone has not been unlocked in the past hour.[8]

Prepare for new regulation. In response to theft and abuse of customer data, regulators are creating new rules to protect consumers. The EU General Data Protection Regulation (GDPR), which became effective from May 2018, covers the data of European citizens wherever it is located. Among other things, GDPR requires organizations to encrypt customer data and prevent loss of data. Violations carry fines of up to €20 million. GDPR points to a new norm for organizations, requiring



transparent and explainable security programs, which they will be expected to share with customers.[9] Similar rules on data privacy are implemented or underway in Asian countries and the United States.

Help customers protect themselves. It is not enough to disclose all the ways that data might be used in a privacy agreement, which most customers will never read.[10] Companies that make sure that customers really understand what is happening with their data and teach customers how to protect themselves will be rewarded with customer trust. Danske Bank (see "Teaching consumers to protect themselves") and ABB (see "Taking responsibility for B2B customers") are examples of companies that are trying to show that they are advocates for their customers.

TEACHING CONSUMERS TO PROTECT THEMSELVES

Danske Bank in Denmark runs a "Keep It Safe" program, which helps customers learn how to protect their data. Based on a survey of 8,000 Nordic consumers, the bank realized that Danes have the least secure passwords, Norwegians know the least about IT security, Swedes have the riskiest behavior on the Internet, and fewer than one-third of Finnish people read the fine print when they sign an online privacy agreement. The Keep It Safe program provides advice on simple everyday routines and procedures that can protect consumer data and gives customers a way to test their computer security. The bank uses humor and a friendly communications style to make the material more accessible to consumers.[11]

TAKING RESPONSIBILITY FOR B2B CUSTOMERS

ABB, an industrial technology company, collaborates with its customers to secure some 70 million connected devices that are embedded in ABB equipment around the world. ABB offers advice and services to combat threats from networking in process automation in power, oil and gas, and other industries. The secure "myABB/My Control System" customer portal is available 24/7 and gives plant operators a central access point to cybersecurity information, recommendations, and downloads relating to ABB products and systems. The company has also established a formal vulnerability handling policy—anyone discovering a software vulnerability affecting an ABB solution is encouraged to contact ABB directly or any national computer emergency response team (CERT) or other coordinating organization.[12]

5) Think beyond your enterprise to your ecosystem.

The future enterprise might conduct business electronically with hundreds or even thousands of suppliers and partners around the world, each of which can expose the company to a cyber attack. Companies need to work with these ecosystem partners to jointly protect their organizations. Yet, only 39 percent of companies say that the data exchanged with strategic partners or third parties are adequately protected by their cybersecurity strategy. To address this risk, companies can:

Govern and manage ecosystem risks systematically. Companies can establish formal mechanisms—written contracts—as well as informal procedures to develop and maintain secure connectivity with suppliers, partners and other third parties. The American National Institute of Standards and Technology recommends a

framework for determining cybersecurity requirements for third parties, enforcing them with normal agreements, and verifying compliance through a variety of assessment technologies.[13]

Participate in your industry's security efforts. In the next three years, 82 percent of respondents expect their organizations will work with other companies in their industries to share knowledge, services, and products to improve cyber resilience. BT, for example, shares threat information with other large telecommunications companies such as Orange and Verizon, as well as with national security agencies.[14] The progress on information sharing is also an opportunity to shape participation in standards organizations. In our survey, 57 percent of companies said they are addressing cybersecurity standards in their collaborations.

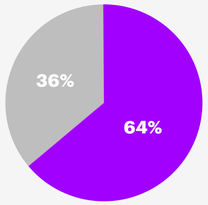
Collaborate beyond your industry. In our survey, 80 percent of respondents said that they expect to collaborate with companies in different industries on cybersecurity in the next three years. To establish a cross-sector industrial cybersecurity knowledge network, Siemens has initiated a "charter of trust" with eight founding members, including Airbus, Allianz, Daimler Group, and Deutsche Telekom.[15]

Even companies that say they are prepared for attacks are actively collaborating with ecosystem partners to increase their understanding of the cybersecurity landscape (see Figure 4).

FIGURE 4

Risk readiness and external collaboration

Two-thirds of companies say they are prepared for growing risks



...Even companies that are prepared for growing risks are collaborating with ecosystem partners

My organization is prepared for the growing cybersecurity risks associated with business transformation and emerging technologies

My organization is vulnerable to increased and more harmful attacks due to business transformation and emerging technologies

Note: Key is the same for both charts

(Numbers denote percentage of respondents who agree with the statement) – **Source:** Accenture Survey 2018, see "About the research"

Grow future business with confidence

Corporate security teams have made good progress in the war against cyber crime. But winning the next war will require both new strategies and new weapons. Top leaders can ensure the success of the connected, intelligent, autonomous business by making sure that security is a core competency across the organization. If they do this, companies will not only keep the enemy at bay, they will also build trust with customers and partners and develop the bulletproof business processes that will make them stronger competitors. With pervasive cyber resilience, the future business can grow with confidence.

Appendix

About the authors

Omar Abbosh is Chief Strategy Officer at Accenture. He is responsible for overseeing all aspects of the company's strategy, innovation programs, and investments. He is a member of the Accenture Global Management Committee.

Kelly Bissell is Global Managing Director of Accenture Security. He oversees all aspects of security globally to help clients build resilience against cyber risks, accelerate digital business growth and innovate safely.

Ryan LaSalle is Managing Director of Accenture Security—North America. His responsibilities include all aspects of security in North America, helping our clients to become more cyber resilient and giving them the ability to grow with confidence.

Madhu Vazirani is a Principal Director of Accenture Research. She specializes in strategy and policy at the intersection of business and development, and her current research focuses on digital business and future workforce.

CONTRIBUTORS

Valerie Abend, Curtis Dalton, Vik Desai, Gus Hunt, Lynn LaFiandra, Paul Nunes, Karen Swanson, Ginny Ziegler.

About the research

WHAT IS A CYBER RESILIENT ENTERPRISE?

In this study, we define the cyber resilient enterprise as: An organization that brings together the capabilities of cybersecurity and business continuity, and has strategies to quickly respond to threats, minimize damage, and continue to operate in the face of attack. As a result, the cyber resilient enterprise can proceed with innovation in digital business models, strengthen customer trust, and grow with confidence.

ABOUT THE SURVEY

In early 2018, Accenture Security surveyed 1,460 executives to understand the extent to which organizations prioritize security in new business initiatives, whether their security plans address future business needs, what security capabilities they have, and their level of internal and external collaboration on security. These executives represent companies with annual revenues of US$1 billion or more from 14 industries and 16 countries across North and South America, Europe and Asia Pacific. Half of respondents were Chief Information Security Officer or equivalent roles, while the remaining half were CEOs and other C-suite executives.

References

1: **2018 State of Cyber Resilience,** Accenture, April 2018

2: Michael Nadeau, **"How to secure the IIOT: Q&A with GE's CISO,"** CSO, October 2, 2017

3: **AT&T portal**

4: **2018 State of Cyber Resilience,** Accenture, April 2018

5: **Security Awareness Training Explosion,** *Cybersecurity Ventures,* February 6, 2017

6: **Designing a Security Champion Program,** Gartner, June 2017 and **Gartner blog,** December 2017

7: **"A Day in the Life of a CISO: Steve Martino, Cisco,"** *Wall Street Journal,* December 21, 2017

8: **www.cbsnews.com,** June 2018

9: **Accenture Security Technology Vision 2018: Rethinking the Foundations of the Intelligent Enterprise,** April 16, 2018

10: **The Privacy Paradox,** *UConn Today,* August 2016

11: **Danske Bank portal**

12: **Cybersecurity for automation,** ABB, April 24, 2017 and **ABB portal**

13: **Framework for Improving Critical Infrastructure Cybersecurity,** Version 1.1, National Institute of Standards and Technology, April 16, 2018

14: **www.securitynow.com,** July 2017 and **BT portal,** October 4, 2017

15: **Siemens press release,** February 2018

AUTHORS

Omar Abbosh
Chief Strategy Officer, Accenture
omar.abbosh@accenture.com

Kelly Bissell
Global Managing Director, Accenture Security
kelly.bissell@accenture.com

Ryan LaSalle
Managing Director, Accenture Security
North America
ryan.m.lasalle@accenture.com

Madhu Vazirani
Principal Director, Accenture Research
madhu.vazirani@accenture.com

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 approximately 442,000 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. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

ABOUT ACCENTURE RESEARCH

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 250 researchers and analysts spans 23 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Singularity—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. Visit **www.accenture.com/research.**