Accenture Security

GAINING GROUND ON THE CYBER ATTACKER

2018 State of Cyber Resilience

Executive Summary

CONTENT

CLOSING THE GAP ON CYBER ATTACKS

Organizations are gaining ground on the damaging impact of cyber attacks—and proving that recent security investments are paying off. Despite the number of targeted cybersecurity attacks doubling, organizations are improving cyber resilience and showing they can perform better under greater pressure.

But there is more work to be done. Now is the time to build on this momentum by drawing on investment capacity to fully realize the benefits of cyber resilience.

Accenture research reveals the five steps that can help business leaders not only close the gap on cyber attackers, but also continue to transform and embed security into the fabric of their organizations within the next two to three years.

IMPROVING CYBER RESILIENCE

The digital revolution continues to transform the way we work and live. This puts innovation and growth at the heart of the business agenda for CEOs and boards globally.

To ensure lasting success, executives should transform their existing organizations while developing new digitally enabled opportunities at the same time. But, this can increase the attack surface and make their organizations more vulnerable to the threat of cyber attacks.

An attack needs to be successful only once, whereas organizations' cyber resilience needs to be effective every time—and it has significantly improved over the last year. Despite the increased pressure from attacks—with ransomware attacks, for example, more than doubling last year[1]—organizations are demonstrating far more success in heading them off. Only one in eight focused attacks (see page 5) are getting through in 2018, compared with the one in three that caused considerable disruption to organizations just over a year ago. And CISOs—as well as the C-suite and the board—can take much of the credit, as cybersecurity capabilities, ranked according to performance levels, have improved 42 percent since last year.

Interestingly, the digital technologies that created market disruption and spawned the next wave of successful cyber attacks are also proving to be part of the solution to tackling cybersecurity. The research shows that 83 percent of survey respondents believe that breakthrough technologies, such as artificial intelligence (AI), machine or deep learning, user behavior analytics, and blockchain, are essential to securing the future of their organizations. Indeed, it is breakthrough technologies that will drive the next round of cyber resilience—although only two out of five business leaders are already investing in areas like machine learning/AI and automation.

C-level executives and board directors should take heart; the analysis shows their growing support for cybersecurity in recent years is starting to pay dividends and, as a result, business leaders are gaining ground on cyber attackers. To continue to progress, C-level executives need to build on this momentum to fully realize the benefits of investments in cyber resilience. Indeed, the prospect of embedding cybersecurity into the fabric of the business could soon become a reality, especially for leaders who keep pace with change and continue to invest in breakthrough technologies.

1 2017 Cost of Cyber Crime Study, Accenture and the Ponemon Institute.

What is cyber resilience?

The cyber-resilient business brings together the capabilities of cybersecurity, business continuity and enterprise resilience. It applies fluid security strategies to respond quickly to threats, so it can minimize the damage and continue to operate under attack. As a result, the cyber-resilient business can introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence.

Targeted cyber attacks

Cyber attacks take many forms and have different degrees of impact. The average organization is subjected to a daily deluge of hundreds—if not thousands—of speculative attacks, which are handled by mature security technologies, such as firewalls.

For the purposes of this Accenture research, we investigated targeted cyber attacks which have the potential to both penetrate network defenses and cause damage to or extract high-value assets and processes from within the organization.

About the research

In 2017, Accenture Security surveyed 2,000 executives to understand the extent to which organizations prioritize security, how comprehensive their security plans are, what security capabilities they have, and their level of spend on security. Just over a year later, Accenture Security undertook a similar survey, this time interviewing 4,600 executives representing companies with annual revenues of US$1 billion or more from 19 industries and 15 countries across North and South America, Europe and Asia Pacific. More than 98 percent of respondents were sole or key decision makers in cybersecurity strategy and spending for their organization.

TRANSFORMING SECURITY

This comprehensive study, which aims to better understand the state of cyber resilience across key markets and geographies, sheds a positive light on the future. Cybersecurity faces much the same trajectory as digital before it.

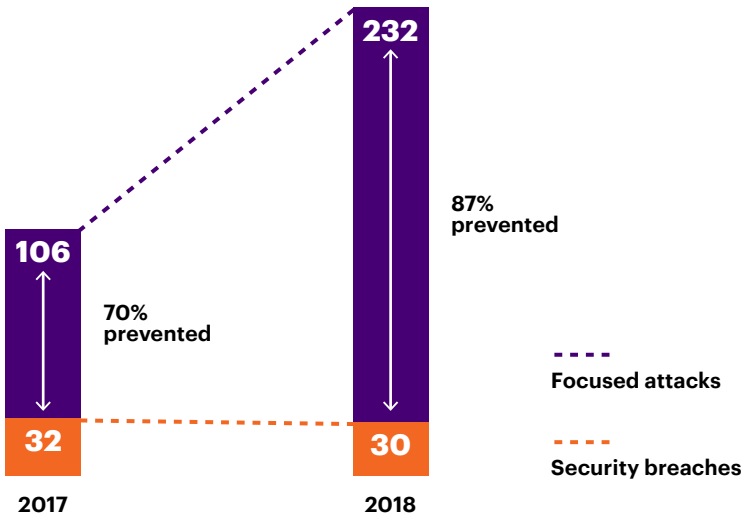
In the early days, digital technologies were alien to existing organizational cultures. Yet, as the C-suite and board became more familiar with the digital world, dedicated roles began to appear within the organization, digital became integral to the core business strategy and is now becoming embedded in the ethos and outcomes of the organization. Today, we are poised to do the same with cybersecurity.

Five findings illustrate the current state of cyber resilience in 2018.

1 Security teams have made great progress—but there is still more work to be done on the basics

Previous cybersecurity reports have often cast a shadow of doubt on whether organizations are ever going to be one step ahead of their cyber attackers. Growing sophistication and the constant introduction of powerful, breakthrough technologies have meant that CISOs and their organizations' senior executives, have felt they are swimming against the tide—riding waves of increasing magnitude. But the 2018 study highlights positive progress for security teams across the world. With significant ransomware incidents like WannaCry in 2017, targeted attacks have more than doubled in the space of a year (232 on average in 2018 versus 106 in 2017). Yet, organizations have been able to raise their game and prevent 87 percent of them, compared with only 70 percent in 2017 (Figure 1). It shows that their efforts are paying off. Yet, since organizations, on average, are facing two to three security breaches per month, there is still room for improvement.

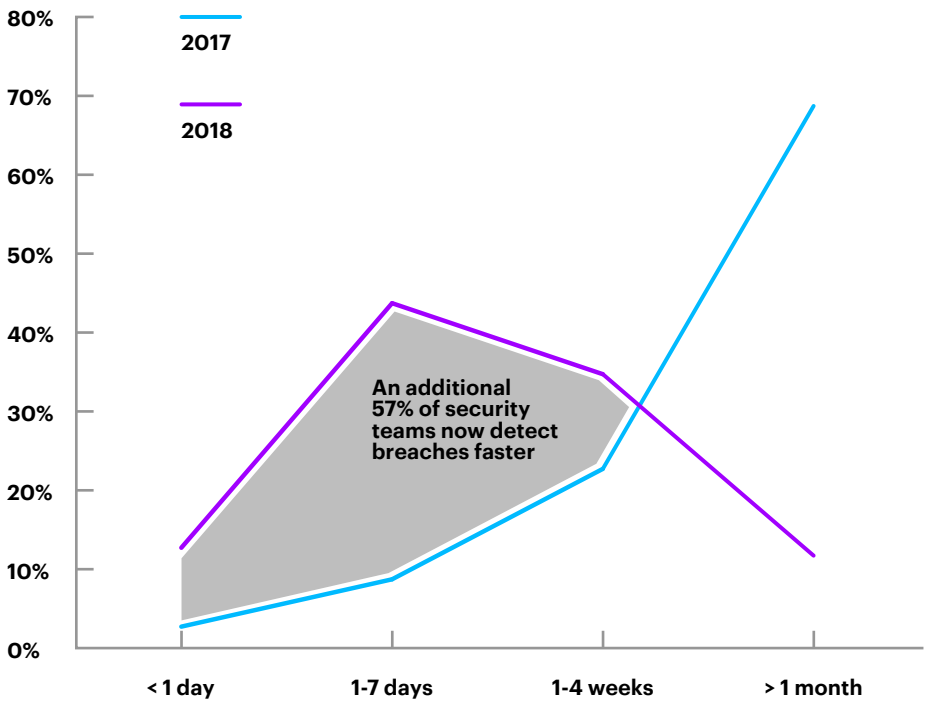
Figure 1—Improved defense against focused attacks



Despite the rising pressure of targeted cyber attacks—with cyber criminals scaling their operations using more sophisticated business models like ransomware-as-a-service and DDoS-for-Hire[2] and monetizing these efforts through cryptocurrencies—security teams continue to identify nearly two-thirds of all breach attempts on average. However, this masks a divergence in performance among organizations. The number of respondents in the top category—able to identify between 76 percent and 100 percent of breach attempts—has more than doubled to 23 percent. At the same time, more organizations than last year (24 percent) fall into the lowest category—able to detect less than half of all breach attempts—compared with 14 percent in 2017. So, while many organizations are performing well, some are clearly struggling with the increased pressure of attacks.

Interestingly, the majority of security teams are getting more effective at finding breaches faster. It is taking less time to detect a security breach; from months and years to just days and weeks. Eighty-nine percent of respondents said that breaches are now being detected within one month compared with a corresponding detection rate of only 32 percent last time around. This year, 55 percent took one week or less to detect a breach compared with 10 percent last year (Figure 2).

Figure 2—Improvements in the detection of security breaches



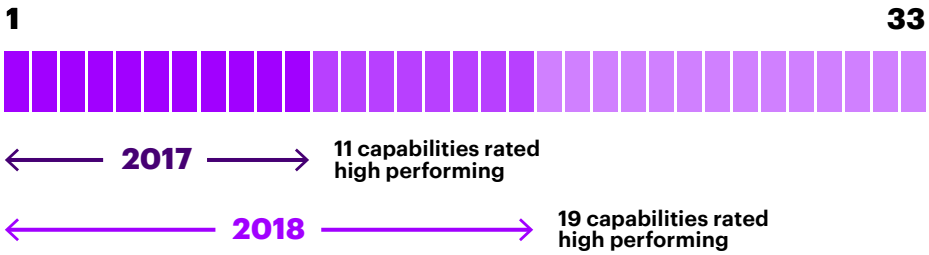
2 2017 Cyber Threatscape Report: Midyear Cybersecurity Risk Review Forecast and Remediations, Accenture Security

Such collaboration is positive and needs to grow further—even among competitors—as there is safety in numbers when defending against cyber attacks.

Of course, security teams are not always the first to know about attacks. The insidious nature of cyber crime means that there are continually evolving ways to infiltrate an organization. But more collaboration is taking place for the attacks that security teams do not identify. When the survey asked how they learn about breaches undetected by the security team, 21 percent said from responsible members of the security community—up from 14 percent in 2017—and 17 percent said externally, through a peer or competitor, up from just 1 percent previously. Such collaboration and threat information sharing is positive and needs to grow further—even among competitors—as there is safety in numbers when defending against cyber attacks.

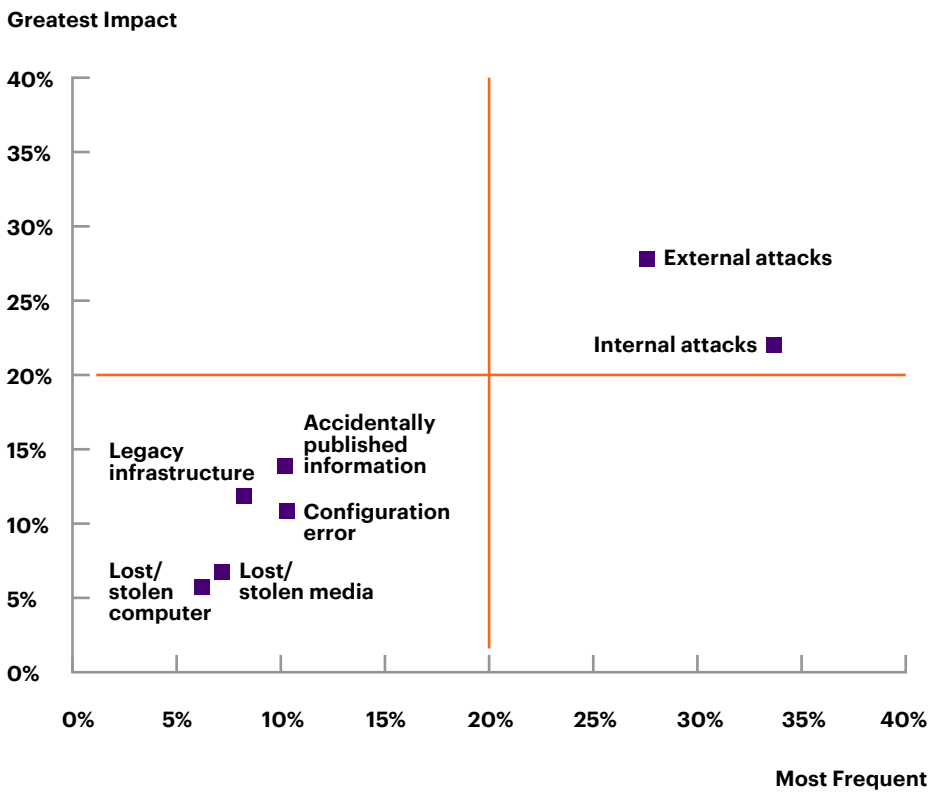
Being better at detection, prevention and collaboration is not all that executives can be proud of—they have also realized an impressive 42 percent improvement in security capabilities. Based on a list of 33 capabilities, the survey asked respondents to rate their performance level at each one of those individually defined capabilities. On average, respondents are achieving high performance in 19 out of 33 capabilities in 2018 compared with 11 out of 33 capabilities in 2017. Almost doubling their high-performing capabilities in a year is an achievement, but a proficiency of 19 out of 33 means they are still some way from being truly robust (Figure 3).

Figure 3—Cybersecurity capabilities rated high performing



In terms of delivering the next wave of improvements, it is easy to focus exclusively on counteracting external attacks, but organizations should not neglect the enemy within. When looking at the incidents security teams fail to prevent, the top two attacks with the greatest impact are external attacks, such as hackers, and internal attacks, such as malicious insiders. Here, their similarities end. External attacks have seen a 9 percent increase in impact since 2017 (28 percent of breaches in 2018 versus 19 percent in 2017). Whereas the number of respondents ranking internal attacks as one of the areas of the greatest impact on their organization was almost half the number from last year (22 percent in 2018 versus 43 percent in 2017). But it is not only the impact of breaches that matters—the relative number of such attacks is important, too. Internal incidents were more frequent for 33 percent of respondents, compared with 28 percent for external attacks. This serves as a timely reminder for organizations to protect themselves from the inside out against the equally damaging threats of internal and external attacks (Figure 4).

Figure 4—Most damaging cyber attacks by frequency and impact



Cybersecurity performance is improving and should extend beyond the organizations' own four walls, but for many organizations, they are only as good as their weakest link. Subsidiary and third-party risk is top of mind, especially when 36 percent of organizations do not apply the same—or higher—cybersecurity standards to their extended ecosystem of partners as they apply to their own business. However, on average, respondents said a cybersecurity program protects only two-thirds (67 percent) of their organization, including corporate IT and the systems in the corporate office. Protection of third parties ranked lowest of all at only 32 percent. Organizations must do more to put the basics of cybersecurity in place to protect their most valuable assets—from the inside out—across their entire industry value chain.

Internal attacks, such as malicious insiders, are one of the top two threats.

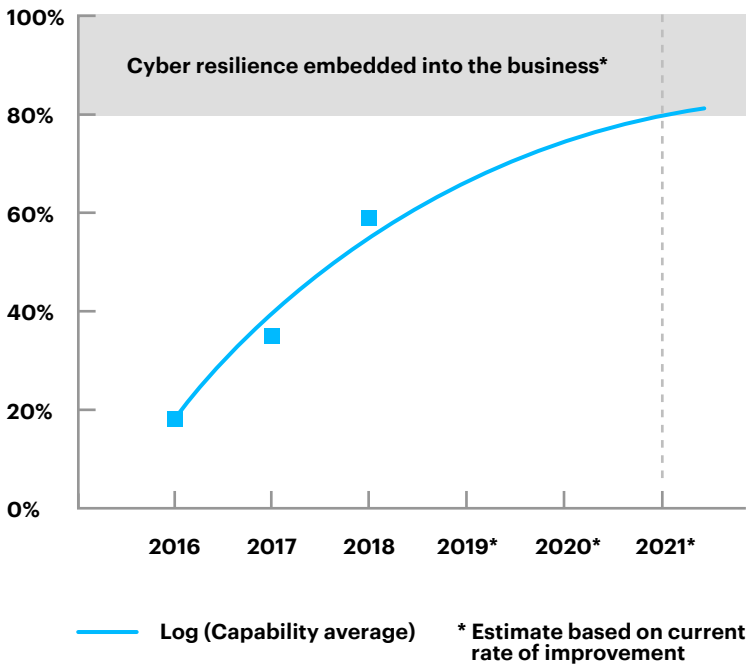
2

Organizations need two to three more years of transformation to embed cyber resilience into the business—but the pressure to perform grows daily

The general outlook for investment is positive; 90 percent of respondents expect their organization's overall investment in cybersecurity to increase in the next three years. But dig below the surface and it would appear that only 31 percent of respondents expect that increased investment to be significant (double or more)—hardly a fast-track to embedding security into the fabric of the organization.

The time to focus on building momentum with investments is now. If they follow the latest trends and continue with the transformation process, organizations could reach a sustainable level of cyber resilience in the next two to three years, one that continues to evolve and adapt (Figure 5).

Figure 5—Forecast of average cybersecurity capabilities reaching a sustainable level of cyber resilience



Aware that breaches are an ever-moving target—still running at two to three per month on average—respondents realize that cyber resilience is key. Sixty-two percent ranked the need for cyber IT resiliency as the most important measure for success of their cybersecurity programs.

Identifying breaches and remediating the immediate issues, while remaining operational, is fundamental to successful cyber resilience in the digital economy. Small wonder, then, that nearly three-quarters of respondents (72 percent) said that "it is not possible to appear strong, prepared and competent if my organization is the victim of a security breach"—further evidence of the ever-present threat of failure and the ongoing pressure to succeed.

3

Breakthrough technologies are critical to future cybersecurity success—but investment capacity is lagging behind intentions

The evolution of digital technologies is a double-edged sword. It has been essential to organizations' success globally while increasing the risk of cyber threat. At the same time, it also presents leaders with opportunities to address these challenges. The survey found that four out of five respondents (83 percent) agreed that breakthrough technologies, such as artificial intelligence, machine or deep learning, user behavior analytics, and blockchain, are essential to securing the future of the organization. And, given additional budget, they would follow through on investing in those breakthrough technologies. Sixty-two percent of respondents would spend it on filling known gaps in cybersecurity technology and 59 percent would spend it on adding innovations in cybersecurity. Approximately one-half of respondents are investing in Internet of Things (IoT) security (55 percent), security intelligence platforms (54 percent), and blockchain (48 percent).

So, executives agree advanced technologies are essential and they would commit funding to them if they could, but in practice, just two out of five are investing in machine learning/AI and automation technologies, to evolve their security programs. It may be a case of overactive optimism. As we have seen, significantly more organizations report that "cybersecurity at our organization is completely embedded into our culture" (83 percent in 2018 versus 70 percent in 2017), yet, if only 40 percent are committing investments to breakthrough technologies like machine learning/AI and automation, this number needs to increase to optimize the opportunity.

Just two out of five are investing in machine learning/AI and automation technologies, to evolve their security programs.

4 Confidence around cybersecurity measures remains high—but a more proactive approach is needed

It may be that the old maxim "success breeds success" is working for the survey respondents. Confidence is certainly higher than in 2017 around the activities that lie at the heart of security efforts, such as monitoring for breaches (82 percent), restoring normal activity after a breach (83 percent) and identifying the cause of a breach (83 percent). Confidence is also evident for four out of five respondents around the effectiveness of their cybersecurity efforts, such as password management (85 percent) and infrastructure security (85 percent).

But that confidence is being tested by the unpredictability of cyber threats; 71 percent said cyber attacks are still a "bit of a black box; we do not quite know how or when they will affect our organization"—an increase from 66 percent who felt this way in the last survey. This points to the need for more effective use of actionable threat intelligence. And when asked which capabilities were most needed to fill gaps in their cybersecurity solutions, the top two responses were activities that could get to the devil in the detail—cyber threat analytics (46 percent) and security monitoring (46 percent). By better analyzing data and applying advanced threat intelligence, organizations can start to anticipate threats and adopt a more proactive approach to defensive strategies.

Seventy-one percent said cyber attacks are still a "bit of a black box; we do not quite know how or when they will affect our organization."

5 More C-suite/board members are actively engaged with cybersecurity—but the role of the CISO still needs to adapt

For most organizations, the last year has seen a significant change in the reporting structure and governance of cyber resilience within the business. Of those surveyed, 66 percent report to either the CEO or the board. Budget authorization is elevated within the organization compared with 2017; 27 percent of cybersecurity budgets are authorized by the board of directors (up from 11 percent) and 32 percent by the CEO/executive committee (up from 22 percent in 2017).

Meanwhile, the CIO has less control over funding with a drop in budget authorization to 29 percent this year versus 35 percent in 2017. Even the CISO/CSO has 9 percent budget control this year compared to 11 percent in 2017. This change in reporting structure and governance will require the CISO to report differently to the CEO and board compared with the CIO/CTO—focusing on business impact, using the language of business.

This elevated status of cyber resilience within the business is helping to fuel improvements. Security spending—both in real terms and as a percentage of IT budgets—has increased significantly since the last survey. More than three times as many respondents report spending more than 10 percent of their IT budget on security compared with 2017 (74 percent versus 22 percent). At the same time, 90 percent of organizations report an increase in their budgets over the last three years compared with only 64 percent in the last survey.

And, looking forward, there are similar commitments to fund cybersecurity initiatives. Ninety percent of respondents anticipate budget increases in the next three years compared with 65 percent in 2017. There are also signs of a shift from the more technical aspects of cybersecurity to place a greater emphasis on the business elements, both internally and externally. There is an increased focus on protecting employee privacy (31 percent, up from 22 percent in 2017) and for providing customer satisfaction (30 percent, up from 18 percent). This will increase in importance as new legislation emerges, such as the General Data Protection Regulations, adding further requirements on organizations' security practices.

When it comes to the metrics for cybersecurity success, "business risk improvement" is the least popular measure, at only 38 percent, while the top three measures cover the more technical aspects of cybersecurity performance, such as system downtime (62 percent), restoration time for normal activity (57 percent) and response time for how long it takes to identify attacks and mobilize to remediate them (56 percent).

The CISO's role is shifting to one that is required to be more integrated with the business. If they adapt, CISOs are well placed to lead the initiative to build security into the fabric of the organization.

More than three times as many respondents report spending more than 10 percent of their IT budget on security compared with 2017.

FIVE STEPS TO CYBER RESILIENCE

Organizations seeking to employ innovative business models, build extended business ecosystems and adopt more flexible workforce arrangements need to find a secure and safe way to do so. Here are five steps that can help them embrace the future on their own terms.

1 Build on a strong foundation: Harden and protect core assets

Respondents to the Accenture survey confirmed that, on average, cybersecurity efforts only protect 67 percent of their organization, with malicious insiders being one of the top two threats. So, there is clearly more work to be done on protecting an organization's most valuable assets from the inside out.

Identify your high-value assets

High-value assets are the data most critical to your operations, subject to the most stringent regulatory penalties, and most important to your trade secrets and differentiation in the market. However, 41 percent of organizations fall below the expected level of performance for the identification of high-value assets and processes and many still lack even a basic asset inventory. A comprehensive asset inventory is an essential building block of a strong foundation.

Harden your high-value assets

"Hardening" high-value assets means making it as difficult and costly as possible for adversaries to achieve their goals and limiting the damage they can cause if they do obtain access. Design and execute your overall security program with cyber attacks in mind. Use multiple techniques including encryption, tokenization, micro-segmentation, privilege and digital rights management, selective redaction, and data scrambling. And remember that with the focus on securing data—encrypting it and keeping it in the safest of systems—if the same controls are not applied to people who have access to the data, you have simply moved the point of failure. To fully protect your high-value assets, it is critical to keep "the people dimension" in mind and ensure that effective monitoring is in place.

Prioritize legacy applications

If your high-value assets are on legacy systems, do not try to harden those assets all at once. Instead, layer in additional protection and increase visibility over control points or points of access until you migrate or modernize the legacy systems. If you have legacy systems that cannot be suitably hardened, look for opportunities to restrict access and improve your monitoring. Focus on timely detection at your weakest links.

Prepare for the worst

Transform your incident response plan into a crisis management plan—one that includes both business continuity and disaster recovery—that can be actioned quickly in a "worst-case" scenario. The plan needs to consider destructive cyber attacks as well as data center outages and site unavailability—and should include alternative strategies for data recovery. Include business leaders, legal and communications teams in the planning process to ensure a coordinated response. Then test the plan, repeatedly, so that the organization builds a "muscle memory" response and identifies areas for improvement before a genuine crisis occurs. Be ready for a catastrophic cyber attack—where e-mail, voice over IP, and other communication systems become unavailable. The time and energy spent preparing will pay strong dividends if—or when—the crisis event happens.

2

Pressure-test your resilience: Coached incident simulation

Conventional ways to "stress-test" defenses—where a red attack team is tasked with infiltrating security systems, and a blue defense team is tasked with detecting, monitoring and mitigating the attacks—tend to fall short of assessing cyber-readiness realistically or accurately.

Even the best red team/blue team exercises have limitations, where people can have difficulty behaving like a real adversary, a constant stream of demoralizing attacks can lead to blue team fatigue, and an unhealthy "silo" effect can set in when the difference in incentives and end-goals can create an aversion to communication between red and blue teams before, during, and after an exercise.

Coached incident simulation—which is sometimes referred to as purple teaming—starts to address these issues and brings a new level of realism to testing defenses by building on the red team/blue team model. Threat intelligence and advanced adversary simulation techniques are used by the red attack team to raise the sophistication and realism of their tactics and targets. The blue team gains from experienced player-coaches who are in close contact with the red team and use threat intelligence to better anticipate attacks. On the blue side, the player-coaches observe the blue team as it responds to red team attacks, and coach in real time to help improve detection and response processes, enable the use of technologies, exploit logging techniques, and advise on alternative approaches. These player-coaches not only bring their expertise, but also, more specifically, their first-hand experience of hunting and expelling adversaries from large organizations.

After the exercise, the player-coaches provide a full analysis of what worked and what did not, what lessons can be learned and where improvements need to be made. The result is a specific list of recommendations for improving the organization's overall cyber defense strategy that helps to close the gap between how secure a business thinks it is and the reality.

3 Employ breakthrough technologies: Automate defenses

Many organizations may be spending too much on technologies that do not minimize the impact of cyber attacks. Accenture has analyzed nine security technologies to better understand the effectiveness of investment decisions and areas where organizations can effectively free up investment capacity. Organizations were overspending on areas such as advanced perimeter controls, automated policy management and enterprise deployment of governance, risk and compliance.[3] By rebalancing their funding and investing in breakthrough innovations, organizations have an opportunity to evaluate potential overspending in areas like these and create the investment capacity to deliver more positive value. The following are examples of breakthrough technologies that can make a difference.

Automated orchestration capabilities

Use AI, big-data analytics, and machine learning to enable security teams to react and respond in nanoseconds and milliseconds, not minutes, hours or days. As threats or risks change, the self-sustaining enterprise would use this same approach to dynamically segment network traffic or resources to manage business risk or contain an incident.

Market solutions take advantage of automation and orchestration to enable fast provisioning and deprovisioning of networks. With security in mind, they leverage this capability to instantly segment, protect, cloak, failover or revoke any device or resource on the network. Dynamic segmentation and micro-segmentation capabilities enable security organizations to respond to threats, adapting protections to address adversaries in real time.

Advanced identity access management

The next generation of digital identity brings together multi-factor authentication, user behavior monitoring, AI-driven access provisioning and deprovisioning, and robotics—supporting employees, shareholders, and customers.

Multi-factor authentication (MFA) raises the bar by requiring context and additional information before enabling access to critical transactions or applications. User behavior monitoring looks for activities that are unexpected. AI and robotics provide a reliable, consistent and automated way to give the right person—and only the right person—access to critical data. In addition, advanced identity management is a critical element of stopping, or minimally slowing, a cyber adversary.

3 2017 Cost of Cyber Crime Study, Accenture and the Ponemon Institute.

4

Use intelligence and data to be proactive: Threat hunting

Use a data-driven approach and advanced threat intelligence to better anticipate potential attacks and develop a more proactive security posture for the business. Organizations should not feel they can only activate their incident response plans in the event of a breach. Today, the best approach is to adopt a continuous response model—always assume you have been breached—and use your incident response and threat hunting teams to look for the next breach with the goal to "find them before they find you."

Develop strategic and tactical threat intelligence

Have a sustainable threat intelligence program that collects and curates both strategic and tactical threat intelligence. Strategic threat intelligence is human intelligence coming from a variety of both closed and open sources—for example, an e-mail explaining that certain versions of a Web server are vulnerable to attack, and how that vulnerability is exploited. Other forms of strategic intelligence can provide insights on campaigns targeting certain industries or technologies, or geopolitical trends that could change the incentives of attackers. Tactical threat intelligence includes machine indicators of compromise that feed in automatically to your systems. Stay as current as possible on both the broader threat landscape and the specific threats posed by adversaries as they relate to your organization.

Monitor for anomalous and suspicious activity

Threats from malicious insiders are not only the most frequent types of attack, they also have the second highest impact. Organizations should monitor continuously and vigilantly, not only for unauthorized access, but also for undiscovered threats and suspicious user behavior.

Use two-factor authentication as much as possible and use role-based access to make automated decisions about who is permitted to see which data and systems. Move toward micro-segmentation in your access control, recognizing that when sensitive data needs to be adjudicated by different people for different reasons, none may need to see the data in totality. Micro-segmentation can show each person what they need to see based on their role and responsibilities, while obscuring the rest. This also limits damage in the event of a breach—if any user's credentials are compromised, only a portion of the data is exposed. By limiting the exfiltration of whole objects or larger swaths of data, the adversary's job becomes far more difficult.

Use a data-driven approach and advanced threat intelligence to better anticipate potential attacks.

5

Evolve the role of the CISO: Business leadership

The next-generation CISO should be business adept and tech-savvy. With new reporting structures and elevated levels of governance within the organization, CISOs need to rethink their approach to the role.

As C-suite executives and boards prepare their plans for a cyber-resilient business, they need help from the CISO to:

- Understand how the business will have a greater "surface area" of exposure in the future and the impact this has on cyber resilience requirements
- Know what must be done to ensure the future cyber resilience of the business across all dimensions (not just the IT capabilities)
- Be clear on where cyber resilience must reside within the organization
- Understand who in the organization has both overall and individual component responsibility for cyber resilience and who is accountable for it
- Know how to measure cyber resilience exposure and risk with relevant measures and monitor these measures at the highest levels of the organization

There needs to be a new kind of CISO—one who is equally at home in the boardroom as in the security operations center. And one who can transform the role to organize and design cybersecurity programs for the needs of the intelligent enterprise, move from individual to shared accountability among senior management, and infuse a culture of cyber resilience across the organization.

There needs to be a new kind of CISO—one who is equally at home in the boardroom as in the security operations center.

SECURITY FROM THE INSIDE OUT

Organizations that "lead in the new" build enough investment capacity for change; seek and create synergies between their old and new businesses; and enable their organizations to innovate by design.

Their leaders choose to pivot wisely—knowing how and when to focus on innovation-led initiatives that can release value fast in the legacy and new businesses. And they address security from the inside out, to protect their most high-value assets across their business ecosystem.

From this study of the current state of cyber resilience, leaders should embrace the good news. Investments are proving to be wise. Performance improvements have been made, even in the face of more attacks. Security teams should feel proud that they are realizing greater success, with the right capabilities, in increasingly difficult circumstances.

But transformation does not end here—in fact, the analysis shows that if it continues and organizations follow the same path, within two to three years they could achieve a sustainable level of cyber resilience—where security becomes "business as usual," embedded into the fabric of the organization.

Within two to three years, organizations could achieve a sustainable level of cyber resilience.

KELLY BISSELL

Global Managing Director
Accenture Security

kelly.bissell@accenture.com

RYAN M. LASALLE

Managing Director
Accenture Security Growth
& Strategy and Cyber Defense

ryan.m.lasalle@accenture.com

FLORIS VAN DEN DOOL

Managing Director
Accenture Security Europe
& Latin America

floris.van.den.dool@accenture.com

JOSH KENNEDY-WHITE

Managing Director
Accenture Security Africa
& Asia Pacific

j.kennedy-white@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 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

12460630