HIGH PERFORMANCE SECURITY
REPORT 2016

BUILDING CONFIDENCE

FACING THE CYBERSECURITY CONUNDRUM

Accenture Security

A DANGEROUS DISCONNECT

One in three focused breach attempts get through, yet most organizations are "confident" in their ability to protect the enterprise.

Reacting to cyber breaches is an operational reality for most organizations today, and it's accompanied by increasing amounts of chaos and dissonance. A recent Accenture global survey of 2,000 security executives representing large enterprises revealed that roughly one in three focused and targeted breach attempts succeeded, yet respondents remain confident that they are doing the right things in terms of cybersecurity, with 75 percent indicating confidence in their cybersecurity strategies. This dissonance may partially result from attempts to toe the company line, but it reveals a cybersecurity disconnect.

The failure rate in preventing security breaches is alarmingly high, but this is amplified when you understand the sheer volume of attacks. In addition to the thousands to millions of random attempts that company networks repel each week, on average, an organization will face more than a hundred focused and targeted breach attempts every year, and respondents say one in three of these will result in a successful security breach. That's two to three effective attacks per month.

The length of time taken to detect these security breaches often compounds the problem. Consistent with other studies, 51 percent of Accenture survey respondents admit it takes "months" to detect successful breaches, while another 17 percent identify them "within a year" or longer.

Additionally, internal security teams discover only 65 percent of effective breaches, with employees, law enforcement and "white hats" (e.g., "ethical" hackers) finding most of the rest.

Part of the security challenge is prioritizing where to focus resources to effectively protect the organization. More than 50 percent of survey respondents say internal breaches made by malicious insiders have the greatest cybersecurity impact. Even so, two out of three respondents say they lack confidence in their organizations' abilities to monitor internally for breach activities.

Further, despite this explicit recognition of the impact of internal threats, the majority of respondents continue to focus on external security issues. For example, 58 percent prioritize heightened capabilities in perimeter-based controls against outsiders, instead of pivoting to address high-impact internal threats. Ultimately, many remain unsure of their ability to manage the internal threats with the greatest cybersecurity impact even as they continue to prioritize external initiatives that produce the lowest return on investment.

One in three focused attacks results in a security breach.

MISPLACED CONFIDENCE DESPITE HIGH-IMPACT BREACHES

One in three focused attacks results in a breach; internal attacks have a major impact; and security teams admit they lack the necessary tools to detect breaches (and, in a third of cases, don't discover the breaches at all). Nevertheless, three out of four respondents express confidence in their abilities to protect their organizations from cyber attacks. Not only that, 70 percent say that their organizations have completely embedded cybersecurity into their cultures and that it is a board-level concern supported by their top executives.

One potential contributor to this dissonance is that there is still too much emphasis on compliance, in part because it seems more tangible and measurable. Many cybersecurity departments measure performance based on achieving compliance objectives as opposed to mitigating negative business impacts. Security control frameworks and compliance programs are extremely helpful in defining foundational thinking; however, they often fail to reflect real-world dynamics. Just as adhering to generally accepted accounting principles does not ensure protection against financial fraud, cybersecurity compliance alone will not protect a company from successful incursions.

What's more, the sentiment among those surveyed suggests organizations should expect more of the same. For example, given extra budget, 44 to 54 percent of respondents would double down on their current cybersecurity priorities—investments that are failing to prevent breaches. These priorities include protecting the company's reputation (54 percent), safeguarding company information (47 percent), and protecting customer data (44 percent). Far fewer organizations would invest the extra cash in efforts that more directly affect their bottom lines, such as mitigating against financial losses (28 percent) or investing in cybersecurity training(17 percent)—an area Accenture research reveals as an increasingly important cybersecurity pillar. In our "State of Cybersecurity and Digital Trust" [1] research published in June 2016, 31 percent of respondents identified a lack of training or staffing budget as the single biggest inhibitor to cybersecurity readiness.

Another example of potential cognitive dissonance: While three-quarters of all survey takers say they have high cybersecurity confidence levels, far fewer indicate similar confidence in their organization's ability to deal with breaches. For example, only 37 percent claim they have confidence in their organization's ability to monitor for breaches, and 36 percent said the same about minimizing disruptions.

1 The State of Cybersecurity and Digital Trust 2016, Copyright © 2016, Accenture and HfS Research, Ltd https://www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016

FORCING PERCEPTION TO FACE REALITY

To survive in this contradictory and increasingly risky landscape, organizations need to reboot their approaches to cybersecurity.

Protecting a company requires an end-to-end approach that considers threats across the spectrum of the industry-specific value chain and the company's ecosystem, identifying and minimizing business exposure and focusing on protecting priority assets. The following steps can help organizations to overcome limited perceptions and deal effectively with the high-impact cyber threats they face.

DEFINE CYBERSECURITY SUCCESS

Organizations need to answer several critical questions in order to reframe their cybersecurity perceptions and build a new definition of success:

- **Are you confident that you have identified all priority business data assets and their location?**
- **Are you able to defend the organization from a motivated adversary?**
- **Do you have the tools and techniques to react and respond to a targeted attack?**
- **Do you know what the adversary is really after?**
- **How often does your organization "practice" its plan to get better at responses?**
- **How do these attacks affect your business?**
- **Do you have the right alignment, structure, team members, and other resources to execute your cybersecurity mission?**

We believe security organizations need to improve the alignment of their cybersecurity strategies with business imperatives. And while many firms are clearly making progress in compliance and risk management, security programs need to continue to improve their ability to detect and prevent advanced attack scenarios.

PRESSURE-TEST SECURITY CAPABILITIES THE WAY ADVERSARIES DO

Organizations need to establish a realistic assessment of their capabilities to protect against high-impact threats, whether internal or external. Pressure-testing company defenses can help leaders understand whether they can withstand a targeted, focused attack. Similar in effect to military live-fire training programs, organizations can engage white hat external hackers in "sparring matches" with their cybersecurity teams to assess preparedness and response effectiveness.

PROTECT FROM THE INSIDE OUT

Many organizations fail to limit internal access to key information, monitor for unusual employee network activities or regularly review access. Adversaries know what they want, but they don't know where key assets live. In contrast, cybersecurity professionals have the advantage of knowing which key assets need to be protected.

By prioritizing energy on these key assets organizations can build a more effective cybersecurity foundation: instead of attempting to anticipate a seemingly infinite variety of external breach possibilities, organizations can concentrate on the relatively fewer internal incursions that have the greatest impact.

INVEST TO INNOVATE AND OUTMANEUVER

When it comes to cybersecurity, standing still is no longer an option. Organizations need to innovate continually to stay ahead of potential attackers, which may require redirecting some resources to new strategies and programs rather than investing more in current programs.

But where to invest?

Organizations seeking to identify opportunities to invest in cybersecurity innovation can examine seven key domains. Such a focus will improve a company's cybersecurity capabilities, and strengthen its resilience to cyber attacks, but it can require continual and systematic security investments.

Only about a third of survey respondents expressed confidence in their capabilities in any of the seven cybersecurity domains, which highlights a need to make investing in these areas a priority.

Business alignment assesses cybersecurity incident scenarios to better understand those that could materially affect the business, and identifies key drivers, decision points, and barriers to the development of remediation and transformation strategies.

Strategic threat context explores cybersecurity threats, including an analysis of competitive and geo-political risks, peer monitoring, and other areas to align the security program with the business strategy.

The extended ecosystem should be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements, and focus on regulatory compliance.

Governance and leadership focuses on cybersecurity accountability, nurtures a security-minded culture, measures and reports cybersecurity performance, develops attractive cybersecurity incentives for employees and creates a clear-cut cybersecurity chain of command.

Cyber resilience is operational excellence in the face of disruptive cyber adversaries. From technology and process foundations to cyber incidence recovery performance, the company seeks to understand the threat landscape, designs key asset protection approaches and uses "design for resilience" techniques to limit a cyber attack's impact.

Cyber response readiness means having a robust response plan, strong cyber incident communications, tested plans for the protection and recovery of key assets, effective cyber incident escalation paths and the ability to ensure solid stakeholder involvement across all business functions.

Investment efficiency is understanding investments across cybersecurity domains and the allocation of funding and resources. It also compares organizational investments against industry benchmarks, organizational business objectives, and cybersecurity trends.

MAKE SECURITY EVERYONE'S JOB

Employees also play a critical role in detecting and potentially preventing breaches. Fully 98 percent of survey respondents said that for breaches not detected by the security team, the company learned about them most frequently from employees. In fact, people represent its first line of defense, which is why organization need to prioritize training and continually refresh cyber talent across the business.

98% **of breaches not detected by the security team, were discovered by employees.**

To build a culture of cybersecurity awareness, organizations should view state-of-the-art cybersecurity as an organizational mindset—one capable of continually evolving and adapting to counter changing threats. To foster a culture of cybersecurity and digital trust, organizations must emphasize an adaptive, evolutionary approach to addressing all aspects of security on an ongoing basis.

Many enterprise cybersecurity teams still struggle to overcome the gap between the security talent they need and the talent available. In a separate Accenture survey on digital trust, 42% of respondents said they have sufficient security technology budgets, but need additional budget for hiring security talent and training.

42% **of organizations need additional budget for hiring security talent and/or training.**

LEAD FROM THE TOP

While the cybersecurity issue has gained full attention on company agendas, many chief information security officers (CISOs) may feel locked out of the C-suite. This isn't necessarily a conscious snub on the part of organizations; instead, it's a question of the security organization's maturity level. To succeed, many CISOs need to step beyond their comfort zones (e.g. compliance audits, cyber technology) and materially engage with enterprise leadership on a day-to-day basis to effectively discuss the business issues at the core of cybersecurity.

Doing so will require them to speak the language of business in order to make the case that the cybersecurity team represents a critical pillar in the battle to protect company value. At the same time, the CISO needs to build the board's cyber literacy with the goal of making it a priority equal to business risk assessment.

Build the board's cyber literacy with the goal of making it an equal priority to business risk assessment.

BUILD ON PAST LESSONS

Effective cybersecurity requires organizations to achieve greater maturity and improve its ability to protect the business from devastating losses. Fortunately, organizations have done this before, with efforts such as the huge push toward higher quality over the past three decades. For many organizations, quality remained an afterthought until new competitors arrived offering superior quality at lower prices. Feeling the bottom-line impact of this incursion, organizations quickly began to act. A similar reaction is beginning to happen now with cybersecurity. As their digital security strategies and organizations mature and new solutions emerge, organizations that tie cybersecurity efforts to real business needs will gain justifiable confidence in their ability to deal with cyber threats.

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 384,000 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 THE ACCENTURE GLOBAL HIGH PERFORMANCE SECURITY RESEARCH

In 2016 Accenture Security surveyed 2,000 executives from 12 industries and 15 countries across North and South America, Europe and Asia Pacific. The survey objective was to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security. The survey aimed to measure security capabilities across seven cybersecurity strategy domains identified by Accenture: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. More than 50 percent of respondents were key decision-makers in cybersecurity strategy and spending, including security, IT and business executives at director level and above at companies with revenues of US$1 billion or more.

CONTRIBUTORS

Kevin Richards, Managing Director, North America
Ryan M. LaSalle, Managing Director, Growth & Strategy
Rik Parker, Managing Director
David M. Cooper, Senior Manager