Contradictions abound
Recognizing the signs of overconfidence

Accenture’s report, “High Performance Security Survey 2016,” reveals that most respondents remain confident that they are doing the right things in terms of cybersecurity, with 73 (75)* percent indicating confidence in their cybersecurity strategies. Not only that, 73 (70) percent say that their organizations have completely embedded cybersecurity into their cultures and that it is a board-level concern supported by their highest-level executives. At the same time, the survey revealed that organizations are realizing an astounding level of breaches. An organization will face more than 90 (100) targeted breach attempts every year, a third of which will result in a successful security breach—that’s two to three effective attacks per month. This dissonance reveals a serious cybersecurity disconnect.

The length of time taken to detect these security breaches often compounds the problem. Consistent with other studies, 63 (51) percent admit it takes “months” to detect successful breaches, while another 7 (17) percent identify them “within a year” or longer. Additionally, internal security teams discover only 65 (65) percent of effective breaches, with employees, law enforcement and “white hats” (e.g., “ethical” hackers) finding most of the rest.

Where do high impact threats originate?
Prioritizing where to focus resources when protecting the organization can be a real security challenge. Almost 50 percent of survey respondents say internal breaches have the greatest cybersecurity impact, but 55 (62) percent of respondents also say they lack confidence in their organizations’ abilities to monitor internally for breach activities. And despite widespread recognition of the impact of internal threats, most respondents continue to focus on external security issues. For example, 53 (58) percent prioritize heightened capabilities in perimeter-based controls against outsiders, instead of pivoting to address high-impact internal threats.

Facing reality: Time to reboot cybersecurity?
To survive in this contradictory and increasingly risky landscape, we believe organizations need to reboot their approaches to cybersecurity. The following steps can help organizations to overcome erroneous perceptions and deal effectively with the high-impact cyber threats they face.

* Communications result first, global result in brackets.
Define cybersecurity success

Organizations must 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 your business 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 on your mission?

Pressure test defenses

Pressure-testing company defenses can enable leaders to understand whether they can really withstand a targeted, focused attack. Organizations can engage white hat external hackers in a real "sparring match" with their cybersecurity team to quickly determine whether it's ready for primetime. To quickly determine whether it's ready for primetime.

Protect from the inside out

Attackers know what they want, but usually not where they are located on the network. In contrast, cybersecurity professionals have the advantage of knowing which key assets need to be protected. By focusing on these key assets, organizations can concentrate on the relatively fewer internal incursions that have the greatest impact.

Invest to innovate and outmaneuver

One reliable approach involves looking across seven key cyber-security domains to identify potential opportunities for future investments in innovation. Currently, only about a third of respondents express confidence in their capabilities regarding any of the seven domains.

- Business alignment assesses cybersecurity incident scenarios to better understand those that could materially affect the business.
- Governance and leadership means focusing on cybersecurity accountability, nurturing a security-minded culture, developing incentives for employees and creating a cybersecurity chain of command.
- Strategic threat context drives organizations to explore cybersecurity threats in order to align the security program with the business strategy.
- Cyber resilience is the company's ability to deliver operational excellence in the face of disruptive cyber adversaries.
- 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.
- The extended ecosystem should be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements, and focus on regulatory compliance.
- Investment efficiency strives to drive financial understanding concerning investments across cybersecurity domains and the allocation of funding and resources.

Make security everyone's job

Fully 97 (98) percent of survey respondents say that the company most frequently learned about breaches not detected by the security team from employees. In fact, a company’s people represent its first line of defense, which is why firms need to prioritize training and continually refresh cyber talent across the business.

Lead from the top

To succeed, 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. 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.

Building justifiable confidence

As digital security strategies and capabilities 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.

For More Information:

www.accenture.com/cybersecurityreport

Key Contacts:

Paolo Dal Cin, Managing Director, Accenture Security—CMT
Ryan M. LaSalle, Managing Director, Accenture Security—Growth & Strategy
Kevin Richards, Managing Director, Accenture Security—North America