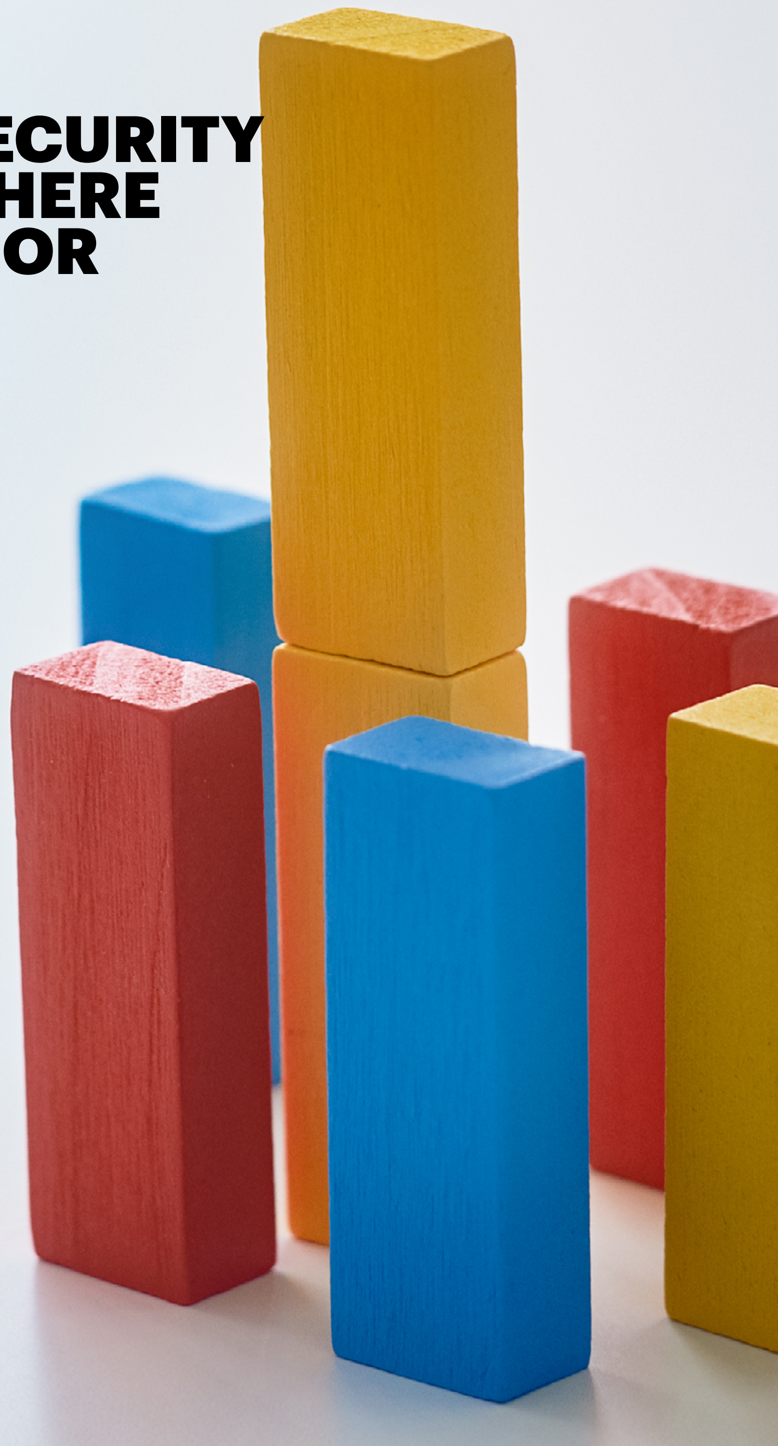
accenture security

# ACCENTURE CYBERSECURITY FORUM

## OPTIMIZING CYBERSECURITY INVESTMENTS: ARE THERE MEASURABLY SUPERIOR APPROACHES?



**VIRTUAL ROUNDTABLE SUMMARY**
**OCTOBER 15, 2019**

**On October 15, 2019, the Accenture Cybersecurity Forum (ACF) hosted a roundtable discussion on optimizing cybersecurity investments. CISOs from multiple industries and organizations joined the call to discuss highlights of recent Accenture Security cyber resilience research, share their own experiences, and explore implications for prioritizing cybersecurity investments.**

The first of the Accenture Security "2019 State of Cyber Resilience" reports suggests that cyber resilience is correlated with a specific set of managerial initiatives and investments. Why do leading organizations achieve significantly better results from their cybersecurity investments than other organizations? What should CISOs, other C-suite leaders and boards do to make sure that their investments are protecting their organizations?

Our subject-matter expert for the call was Floris van den Dool, Accenture Security managing director. The session was hosted by ACF Chair Andy Vautier, Accenture CISO.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed. Below is a high-level summary of the discussion, without attribution, for both attendees and those who were unable to participate.

## PERSPECTIVES

Vautier began the discussion by noting that CISOs are challenged by "security fatigue," facing an increasingly difficult threat landscape with more sophisticated threat actors, a greater variety of risks, and mounting regulation. In addition, enterprise leadership is expecting a larger return on cybersecurity investments and higher "resiliency value." How are some organizations successful in realizing high returns on their cybersecurity investments, while others lag behind?

## DISCUSSION

Van den Dool provided an overview of the cyber resilience research results. Compared to other organizations, cybersecurity leaders (17 percent of survey respondents) do three things differently to get the greatest value from their security investments:

- **Scale more.** Scaling technology investments quickly across the business is a best practice of leaders. They move more than half of their tools from pilot to full-scale deployment relatively fast, which helps contain the impact of security breaches. For the best at scaling, only 5 percent of cyberattacks resulted in a security breach, compared to 21 percent for other organizations. Cybersecurity programs for the best-at-scaling actively protect three-quarters of all key assets; other organizations cover only half of their key assets. CISOs must decide how to scale effectively at reasonable cost.
- **Train more.** Organizations best at training are two times better than the rest at defending against attacks. The CISO has a very important role to play in setting cybersecurity training budgets for the entire organization—not just the cyber team—and should sit at a place in the organization where he or she can make a big impact. When training is an investment priority, organizations are faster at finding breaches and better at stopping cyberattacks, and they protect more key assets.
- **Collaborate more.** Organizations best at collaborating are two times better than the rest at defending against attacks. These leaders are significantly better protected by their cybersecurity programs; realize a higher return on their technology investments; more effectively contain business impacts of breaches; provide greater protection of their key assets and extended ecosystems; and achieve closer regulatory alignment. Collaborators can include ecosystem partners, the security community, industry colleagues, cybersecurity consortiums, regulators and internal business units. In the research study, organizations using five or more methods of collaboration were found to have a breach ratio of 6 percent, compared to an average of 13 percent among other respondents.

## New tools

Security teams should keep pace with attack groups by embracing advanced technologies. One of the primary purposes of new technology tools is to help fuel an organization's resilience—not only by preventing attacks, but also by aiding quick and efficient recovery from breaches. Investment in new technologies is leading to a proliferation of tools for most organizations—yet they are seeing only 53 percent returns on average for these investments, according to the research report. One reason may be that the tools are not being tested or fully used throughout the enterprise: On average, only one-quarter of all security tools adopted are piloted and scaled across the organization. "Too often we start with technology without considering the objectives we are trying to meet, how well it can scale in our organization or the training requirements," van den Dool said.

Roundtable participants discussed the value of seamless integration of tools in the context of an architecture or platform. Tools are just one element of a security equation; having a larger picture is essential. Van den Dool agreed: "Tools should be part of a well-thought-out architecture so we know which problem we are going to solve with this tool, which assets we are going to cover, where it fits in our architecture, and what risks we might not be covering."

CISOs can find a best-in-class point solution for just about any need. But an approach that allows seamless integration lends itself to scale. Widely used security frameworks such as NIST can be helpful in decision making.

## Metrics

The Accenture Security research report identifies four key metrics in assessing cybersecurity performance: low breach ratio, fast detection speed, fast remediation speed, and minimal damage. Roundtable participants generally find some value in benchmarks such as the Information Security Forum Security Healthcheck. Boards of directors understand peer benchmarking and don't want the organization to appear to be "the weakest kid on the block."

## Mitigating complacency

Many security executives—“victims of their own success,” in effect—find it difficult to gain budget increases when their cybersecurity programs are viewed as successful by senior leadership. Van den Dool pointed out that it is important to consider that while direct attacks on an organization are decreasing, attacks on its enterprise ecosystem are increasing. The risks to the overall ecosystem are now even higher and have to be addressed.

CEOs must be mindful also of the rising impact of regulation. The cost of fines has escalated in recent years, and the risk of fines by regulators can be persuasive with senior management.

Participants agreed that cybersecurity investments must keep pace with changing business models and needs. Proactive security requires investing two to three years out rather than playing catch-up.

## Investment priorities

When asked, “If you had an incremental $10 million in security funding, where would you allocate it?,” participants had one answer: people. Most of the CISOs are struggling to attract and retain qualified people, and lack the human resources needed to fully use all the cybersecurity tools they have. Some CISOs are using managed services providers to help correlate data and perform other functions, but also need resources with enough internal knowledge to do more with the data and discuss its implications with the rest of the business. Continuous training in such areas as threats and technologies is essential to keep security teams sharp.

Van den Dool acknowledged the shortage of cybersecurity talent, and suggested investing half of the incremental dollars in innovation. Newer technologies such as AI, machine learning and robotic process automation can be deployed to automate mundane tasks and free up scarce cybersecurity talent, speed up response, improve quality of detection, and focus on sophisticated, emerging threats and strategic challenges such as supply chain risk and other third-party ecosystem security.

CISOs can feel at a disadvantage when competing with the rest of the business for investment dollars. Lines of business often can point to how an investment will contribute to the bottom line. Security executives, on the other hand, often have difficulty demonstrating ROI and must make the business case based on cost avoidance and risk reduction. CISOs can adopt an approach of explaining risks to the business units and earning their buy-in on cybersecurity investments.

Van den Dool said the Accenture Security research found little difference between leaders and all other organizations in the percentage of IT budget spent on cybersecurity. “The differentiating factor is not how much they spend, but how well tools are integrated and scaled,” he reported.

## Conclusion

Van den Dool agreed with the participants that while technology is important, CISOs need to keep a holistic view. According to the Accenture Security research, organizations are protecting on average only 60 percent of their business ecosystem assets with their security investments—a statistic that needs to improve. He offered a call to action:

- We need to scale better, and a security architecture approach can help.
- We need to improve cybersecurity maturity, and that’s where training comes in.
- We need to collaborate more and with a broader set of third parties, so that we can share deeper insights.

Vautier agreed. He noted that the research revealed that even the leaders were deploying protection well below 100 percent, and the non-leaders lagged significantly. Clearly, we CISOs have a ways to go to provide the ubiquitous security protection expected by senior leadership and boards. The research and the discussion among ACF members confirm that CISOs cannot afford to focus on just one dimension of scaling, training or collaborating.

## CONTACT

**ANDY VAUTIER**
Accenture CISO
Accenture Cybersecurity Forum Chair

## 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 482,000 people serving clients in more than 20 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 drive 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 organizations' 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 or visit the Accenture Security **blog**.

**Visit us at www.accenture.com**

**Follow us @AccentureSecure**

**Connect with us**