A perspective on security innovation strategy in a COVID-19 world

On July 8, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "**A perspective on security innovation strategy in a COVID-19 world**." CISOs shared their security innovation strategies and priorities, and discussed how they are modifying their investments in response to the current disruption.

Both the operating context and the security risk landscape have changed dramatically for most enterprises as a result of the COVID-19 disruption. With budgets under pressure, should we be reducing, maintaining or increasing our investments in security innovation? How has security innovation strategy been impacted in various industries? What should our investment priorities be for security innovation?

Lisa O'Connor, Accenture Security managing director and Accenture Labs security research and development lead, joined two member CISOs in serving as subject-matter experts. The session was hosted by Andy Vautier, Accenture CISO and ACF chair.

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.

Innovating during the disruption

CISOs are approaching security innovation in a variety of ways during the pandemic. Some enterprises are cutting external spending and boosting internal staff work on innovation. Others are pursuing their current innovation roadmap, but extending the timeline. Still other organizations are implementing their security innovation plans with few, if any, changes.

Many of the members' insights and experiences are consistent with the findings presented in a new Accenture research report, "Innovating at speed and scale with implicit security." The report notes that a small set of global enterprises—the "alpha innovators"—are innovating securely for competitive differentiation. These alpha innovators are investing heavily in emerging technologies: AI, 5G, quantum computing and extended reality.

The most striking finding was that collaboration with the CISO throughout the adoption journey is essential for enterprises to innovate with emerging technology. Early adoption and major investments are not enough. Success requires significant ongoing CISO engagement and cyber risk management expertise from the beginning. Enterprises must have the right mindset, behaviors and culture to make it happen. As a result, the alpha innovators are better prepared to maintain their leadership in the marketplace through outcomes such as revenues, cost savings, market capture and new services.

The Accenture survey of 500 senior security and business executives in 12 industries revealed five factors that distinguish alpha innovators from their peers:

1. Multi-pronged strategy—Investing now across all four emerging technologies
2. Risk mindset—Fully assessing the security risk
3. Borderless collaboration—Working across all aspects of the enterprise
4. Culture of innovation—Creating an internal and external ethos
5. Defense in depth—Applying a range of protective and detective security controls and models for emerging technologies

Multi-pronged strategy

Alpha innovators are investing heavily in emerging technologies. Furthermore, CISOs of these organizations are allocating more than one-quarter of their budgets to secure the emerging technologies. This is a substantial amount and a clear indicator of the CISOs' deep, action-oriented commitment to achieving innovation. This commitment includes investing in the necessary security tools; dedicating the appropriate number of people to securing networks, applications, data and access control for the new technologies; up-skilling people with the required security skills; and supplementing as needed by building partnerships with third-party providers.

Members discussed how adoption of a widely used innovation framework, such as that of the National Institute of Standards and Technology (NIST), can accelerate innovation while reducing risk. A common language for discussing innovation with the business can help get everyone on the same page, guide risk management decisions and speed up decision-making.

Investments will occur only if CISOs "lean in" to the business strategy. CISOs must be included early in discussions about changes in business strategy. Explain how security enables business outcomes. Have a framework to understand the enterprise's biggest needs, customer pain points, and measures relied on to make investment decisions.

Risk mindset

While perceptions of security risk vary by type of technology and position in the adoption cycle, all C-suite executives are significantly more aware of the security risks of innovative technologies. What sets the alpha innovators apart is the ability to assess and reduce risks earlier in the adoption cycle, protecting the innovation investment and lowering overall lifecycle development costs.

When enterprises must implement changes quickly—for example, enabling many employees to work from home for the first time—it is important to identify the greatest needs, and manage the risk of delaying other projects in the pipeline. In addition, build security into projects. Enabling innovative technologies requires assessing them on an ongoing basis and having security architecture patterns ready.

Borderless collaboration

Collaboration between business and security executives is essential for continuous innovation, with the alpha innovators much more likely to include the CISO from initiative kickoff through completion.

Participants confirmed that the benefits of collaboration are striking. The time horizon for executing innovations has shortened significantly. Multi-year initiatives have largely given way to multi-month timeframes. CISOs described carrying out major innovations in financial transaction processes and customer engagement in days and weeks instead of months and years.

CISOs also discussed the value of "security by design." Security professionals make the largest contributions to business value when they are integrated with other functional teams, such as customer experience, product development and manufacturing. For example, early engagement between security engineers and product developers can enable an enterprise to quickly put in place a new online customer experience while maintaining the integrity and security of customer data.

Culture of innovation

CISOs of the alpha innovator organizations realize that the skill sets needed to secure emerging technologies will change significantly, and they are committed to addressing the skills gap through training, strategic partnerships with third-party companies, and hiring new talent.

From a leadership perspective, CISOs need to have the courage to disrupt. Improve or even replace processes that hinder innovation.

As an enterprise's priorities shift rapidly, a culture of continuous learning is extremely valuable. It's not solely about the technology; critically important are the people and their skills, a learning culture and knowledge exchange to tackle new challenges.

A culture of innovation and agility is emerging among external providers. Contract negotiations are being resolved more quickly. Suppliers recognize the mutual benefit of producing results faster.

Defense in depth

Alpha innovators take an institutionalized approach to security governance, controls and data protections to attain the high bar of continuous innovation. They are applying and developing controls to create strong defenses around emerging-technology implementations.

Members discussed the many benefits of expanding automation. Automated tools and processes can significantly improve threat monitoring, incident response and recovery, and can leverage scarce cybersecurity talent.

Lastly, don't ignore the basics. Maintaining strong cybersecurity is not only good business; it also builds credibility that can draw the CISO into strategy discussions about emerging technologies with the senior leadership team.

Conclusion

The COVID-19 disruption will invariably create winners and losers among industry sectors, enterprises and CISOs. Adaptation and innovation will be key to success for all three categories in the short term. The security team has the potential to serve as an important enabler, rather than a constraint, in driving innovations that are essential to enterprise success. The CISO's engagement should extend from the board and executive leadership to cross-functional teams charged with implementing innovation. Deep engagement of security with the business can accelerate change and help ensure that security is a differentiator rather than an afterthought.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

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 more than 509,000 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 is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.