Updating security controls and risk management in light of workforce disruption and COVID-19 cyber threats

In a continuing series of virtual roundtables on the cybersecurity impacts of the disruption caused by the coronavirus, Accenture Cybersecurity Forum (ACF) members convened on April 16 to discuss how they are addressing security controls and risk management priorities. Our two subject-matter experts were an international cybersecurity executive and Jeff Recor, Accenture integrated risk management lead. 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.

Three phases of the disruption lifecycle

From the CISO's perspective, the response to the COVID-19 disruption is rolling out over three phases. Each phase requires specific remediation efforts.

1. **Stabilize.** Enterprises must stabilize operations to maintain business continuity and the safety and security of employees and other stakeholders. As employees rapidly migrate to a remote work environment, the focus of information security shifts from enterprise infrastructure to cloud and virtualized infrastructure. Work-from-home (WFH) employees must rely on home W-Fi routers and VPN connections, increasing the risk of data leakage and theft of sensitive company information. CISOs are encrypting Wi-Fi access and interrogating WFH machines for public and private anomalies.
2. **Normalize.** As employees adapt to working from home, CISOs can start to strengthen security by analyzing risks and controls across the three dimensions of people, processes and technology. Cybersecurity executives need to plan on executing months-long business continuity plans, including security monitoring and response, while operating under quarantine conditions. CISOs must account for the economic and operational impacts of the disruption, which will create financial and budget challenges even as CISOs are expected to maintain or strengthen cybersecurity controls.
3. **Optimize.** Innovative enterprises are preparing to conduct business in new ways, including making working from home more secure, productive and less stressful. CISOs are using the disruption as an opportunity to help senior management focus on the most important security priorities and improve network security and other security measures, particularly those that might have been overlooked in the process of initially stabilizing operations. Participants pointed to the following examples:
    - Workforce analytics and increased network monitoring activity are protecting WFH call center employees from network intrusions.
    - Enterprises are moving from hard/physical tokens to soft/digital tokens to authenticate data access.

- Time tracking apps are helping onsite employees maintain social distancing by reducing the risk of congregating around a single device as they arrive for work.
- Enterprises are revising the terms of their third-party licensing agreements to accommodate working together in a “new normal.”

In addition, members reported increased collaboration within and across industries, and across the supply chain, to share best practices and implement mutually beneficial security controls. Collaboration will be essential as bad actors become more sophisticated in exploiting COVID-19 concerns and new targets, such as stimulus payments to individuals and enterprises.

Communications will remain a critical factor across all three phases, CISOs agreed. Continuing disruption is stressing corporate culture and employee well-being and performance. Leaders must maintain ongoing, consistent and pervasive communications to mitigate the risk that people will fall back on old habits.

Risk management best practices

CISOs should anticipate that threat actor activity will escalate. We have not yet seen the full impact. Cybersecurity threats will come from many corners. State-sponsored cyber terrorists will conduct phishing, espionage and disinformation campaigns and ransomware attacks. Rogue threat actors are eager to exploit the disruption for financial gain. Increased unemployment and employee dissatisfaction may drive an increase in opportunistic hacktivist activity.

Real situations point to potential problems. For example, what if a well-intentioned employee shared information with a threat actor posing as a journalist? What if a nation state-sponsored cyber criminal posing as a potential customer acquired data to use to establish a lower-cost competitor? The human elements apply to risk management and cyber risk mitigation.

Best practices shared during the roundtable include:

1. Stress-test your cybersecurity defenses and identify threat vectors before attacks by bad actors.
2. Regularly engage senior management and operations teams in new scenario planning and tabletop exercises as the threat landscape evolves.
3. Gather deeper threat intelligence to inform months-long business continuity plans.
4. Continue monitoring e-mail and other endpoints to manage the risks of social engineering attacks.
5. Examine security across your business ecosystem, including telecom companies, ISPs, cloud providers and application providers.

Conclusion

The health and safety of people will continue to be everyone’s No. 1 priority. CISOs understand that there are no simple solutions to the challenges presented by the disruption, but are finding that collaboration within the enterprise and across the business ecosystem can help manage risk and produce better cybersecurity outcomes. Executives are also becoming more creative in leveraging the dimensions of people, process and technology to stabilize, normalize and ultimately optimize the performance of the enterprise.

CONTACT US

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 in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of advanced technology and intelligent operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. 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 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 the Accenture Security blog.

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

Copyright © 2020 Accenture All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.