Addressing a breach in the emerging post-COVID-19 environment

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable on June 5 to discuss **"Addressing a breach in the emerging post-COVID-19 environment."** We explored how Asia Pacific security leaders are preparing for and addressing breaches in the COVID-19 environment in which nearly every enterprise has experienced major shifts in operating practices. What is different—and more difficult—about responding to an incident today?

Three executives with significant experience in cybersecurity, incident response, data privacy, litigation, contracts, and regulation served as our subject-matter experts:

- Partner at an international law firm and a data privacy and cybersecurity authority
- CISO of an Asia Pacific energy company
- Justin Harvey, Accenture Security managing director and incident response lead

The session was co-hosted by Andy Vautier, Accenture CISO and ACF chair; and Andrew McLauchlan, Accenture Security managing director and Asia Pacific lead.

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.

Strategic priorities

C-suite executives and board members are thinking strategically about the long-term health, and even survival, of their enterprises in the evolving post-COVID-19 environment. CISOs have a significant opportunity to contribute by communicating within the context of current C-level and board concerns.

CISOs are looking ahead and reconsidering cyber strategy for a time when at least some employees and customers will return to the office. A major concern is that employees may bring into the corporate environment machines that have been compromised on a home network. Appropriate hardening of the directory environment and control over privileged accounts are critical to avoid compromise.

Traditional cybersecurity playbooks need updating to reflect the changing environment. One key factor driving this requirement is the strong stance taken by regulators. Expect regulators—and insurers—to demand documentation on how enterprises are responding to breaches, particularly escalating ransomware attacks. Victim companies are in a difficult position, but regulators are not taking a kinder, gentler approach.

Enterprises can expect to see a spike in litigation. As in the past, an economic downturn is driving an increase in litigation. Even though most litigation occurs in the United States, the impact can be felt in other countries and regions. Class action lawsuits have been initiated around some of the major breaches.

Agility is required to address evolving threat actor behavior. Many actors remain active in the Asia Pacific region, for either geopolitical or industrial espionage reasons. Rogue criminals are behaving more like nation-state bad actors. COVID-19-related phishing efforts evolve with current events. Ransomware attacks are increasing and getting more sophisticated. No longer a commodity exercise, ransomware is now more targeted and persistent. Domain admin access attacks are becoming more vicious. Perpetrators are selling access to other bad actors, which makes attribution, detection and eradication more difficult. Moreover, detection can be more difficult because attackers can be active for months before they start monetizing. In deciding how to respond to ransomware attacks, enterprises must consider legal and regulatory complexities, not to mention managing costs. A rise in ransomware payments is attributed in part to more sophisticated malware and a lack of flexibility in rebuilding infrastructure.

Tactical preparations

Several aspects of the evolving operating environment make it difficult to respond to a breach as quickly as in the past. Physical constraints such as limited access to data centers and employee laptops, lack of a war room for convening incident response teams face-to-face, and limited forensics capabilities make breach response more challenging.

CISOs are reevaluating and revising their third-party service level agreements to help ensure availability of high-demand resources in the event of a widespread, complex crisis. An incident response provider may not be able to send resources to a remote site given travel restrictions, access controls and high demand for its services. Confirm that your incident response provider can mobilize on short notice and is experienced in supporting large and complex incident response activities.

Response teams are establishing new processes to mitigate attacks. Security tools must match new operating models, such as rapid deployment to the cloud or a reliance on home networks. Recognizing that people working from home may have a lessened sense of accountability, and a greater willingness to take risks and expose themselves to information, than those working in the office, CISOs are changing how they train people on cybersecurity best practices. Innovative training approaches adopted include awarding bonuses for completing training and strengthening passwords.

Composition of the cybersecurity leadership team may have changed during the disruption. The team may have new members from other functions, such as IT, legal, finance and communications; from other geographic locations; and from third-party providers such as insurers and incident response vendors. These teams must adapt to work well together without convening face-to-face in a traditional war room.

Best practices

1. **Don’t become a victim**—Take proactive measures to avoid breaches and to respond quickly when required. In addition to adopting tactical solutions, make sure your enterprise cyber strategy continues to support incident response in a new world.
2. **Build a playbook that balances short- and long-term thinking**—Maintaining cybersecurity through waves of stabilizing, normalizing and optimizing operations requires a comprehensive perspective. Develop a cybersecurity strategy and incident response playbook that reflect the evolving operating model, such as a hybrid office-based and work-from-home environment.
3. **Update response team training**—Speed is always of the essence in incident response; roadblocks in the current environment make training more important than ever. Train response teams to conduct forensics remotely, when accessing data and machines on-site is not possible. Run extensive red team exercises. Testing is critical to determine if third-party incident response service providers can perform well in a virtual environment.
4. **Keep the C-suite and board informed of security posture**—CISOs must keep senior management and the board apprised of threats and security activity in ways that are relevant to their immediate priorities, such as P&L. Board members are particularly interested in cybersecurity now, given an uptick in public exposure of the issue, and expect the CISO to keep the enterprise

safe. Senior leadership needs to support a heightened sense of awareness and vigilance across the enterprise.

5. **Test, test, test**—As the enterprise responds rapidly to changing conditions, such as moving operations to the cloud, stress testing becomes critical. Implement stress tests and tabletop exercises that match the current operating environment. Drill response teams under multiple conditions and scenarios. Test for vulnerabilities among third-party partners.
6. **Push vendors for more integrated solutions**—Encourage vendors to close the most important gaps in their solutions. Challenge tool vendors to improve integration and innovation in their offerings to fit the current environment.

Conclusion

Incident response is more complex than ever. Ransomware attacks are more sophisticated and expensive. The enterprise needs to have the right leadership team—including cyber, IT, legal, finance and communications—in place and communicating effectively. The CISO's team must have the skills necessary to react to evolving operating environments, threat actor behaviors and expectations from the C-suite, the board, insurers, law enforcement and regulators.

At the same time, CISOs are thinking strategically about preparing for a post-COVID-19 environment characterized by both uncertainty and opportunity.

CONTACT US

Andrew McLauchlan
Managing Director and Asia Pacific Lead
Accenture Security
andrew.mclauchlan@accenture.com

Joseph Failla
Managing Director and Australia/New Zealand Lead
Accenture Security
j.failla@accenture.com

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.

Visit us at www.accenture.com

Follow us @AccentureSecure
Connect with us