Addressing a breach in the COVID-19 environment

Accenture Cybersecurity Forum (ACF) members and invited Accenture Security clients convened virtually on July 27, 2020, to discuss **"Addressing a breach in the COVID-19 environment."** We explored how security executives in the Middle East are protecting their enterprises from a range of known and emerging threats while their organizations have been undergoing significant shifts in operating practices.

Our subject-matter experts were two veteran incident responders: a partner and data privacy and cybersecurity authority in a major law firm who has helped respond to more than a thousand data breaches; and Justin Harvey, Accenture Security managing director and incident response lead. The session was co-hosted by Andy Vautier, Accenture CISO and ACF chair; and Ahmed Etman, Accenture Security managing director and Middle East 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.

Impacts of the disruption

Cybersecurity threats are coming from many corners. State-sponsored cyberterrorists are conducting 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 new and opportunistic hacktivist activity. Uninformed insiders are more inclined to fall victim to phishing e-mails and texts.

The cybersecurity response capabilities of many enterprises have been significantly impacted by the disruption. While speed is of the essence in incident response, new ways of working remotely may slow mitigation efforts. Virtual collaboration tools can be useful, but are no substitute for face-to-face interaction or a physical war room.

CISOs and their teams are adapting to new working models and trying to keep stakeholders informed of key cybersecurity developments. Some CISOs have had to reduce or furlough security operations center staff. Travel restrictions and social distancing make it harder to convene team members.

In fact, the impacts of the disruption are being felt across the dimensions of people, process and technology that are fundamental to cybersecurity effectiveness.

People: Managing multiple stakeholders

Internally, CISOs are advised to lead with a "human first" mindset. Ensure that incident response teams—the front lines of defense—are taken care of physically and emotionally. This may be more challenging now given the pressures of the disruption.

Engage senior management and peers who are collaborating in a crisis. CEOs, concerned with enterprise financial performance and reputational risk, should be brought into security discussions on a regular bases to help strike the right balance between security and business continuity. The roles of legal and communications teams should be clearly defined.

Third parties also have a stake in incident response. Incident response in the Middle East often requires considerable dependence on third-party providers. CISOs, with a limited supply of local response resources and high expectations for reliable business continuity, face challenges in balancing security and business priorities. A reliance on operational technology and difficulty getting incident response resources on site make breach mitigation particularly challenging for many Middle East enterprises. In addition, regulators continue to enforce laws and policies in spite of hardships enterprises may experience during difficult times. Insurance companies are imposing new requirements and constraints. National and international law enforcement agencies are taking a more active interest in cybersecurity breaches. While engaging with law enforcement can help identify the source of an attack, it can also create risks in keeping data secure or open the enterprise to legal discovery demands. That is particularly important because an increase in litigation is common during disruptions.

Process: Prepare for now and the future

Security preparedness is essential and should be a top priority. Ideally, incident response plans should be developed long before an incident.

Traditionally, incident response playbooks follow a structure such as the NIST framework: 1) identify, 2) protect, 3) detect, 4) respond, 5) recover. But under extraordinarily disruptive conditions, how can services be restored quickly and safely? How will you determine why a breach occurred and who is responsible? The answer, according to roundtable participants, is to regularly refresh playbooks and "test, test, test."

Conduct tabletop exercises, red team/blue team simulations and drills now to address breaches in the current environment. Yesterday's plans may not work today. Test and train simultaneously. Middle East CISOs acknowledged the importance of testing, training and automation, even while more urgent priorities often take precedence.

An updated incident response plan should:

1. Prepare the enterprise for worst-case scenarios specific to current conditions.
2. Include plans to work with media, customers, law enforcement and regulators. Define roles and responsibilities of all involved.
3. Identify multiple third-party incident response resources. They may be in short supply when needed most.
4. Identify clean channels of communication in the new operating environment
5. Account for the fact that a remote workforce may not be able to respond to an incident as quickly as a team that is used to convening in a war room.
6. Prepare to quickly produce evidence and data. Meeting regulatory and insurer requirements may be tougher in today's environment.

Technology: Focus on vulnerabilities

Security teams are stretched thin and may overlook vulnerabilities, such as a recent acquisition's network. Threat actors are specifically targeting these kinds of non-core network assets. The 2020 Accenture

Security *State of Cyber Resilience Report for Saudi Arabia* reveals that 49 percent of breaches in Saudi Arabian companies are indirect attacks that target weak links in the supply chain.

Zero trust security models are becoming more prevalent, but it is not safe to assume that past security procedures will be sufficient in a new operating model. Security practices from a traditional computing environment cannot simply be transferred to the cloud. Multi-factor authentication, an effective threat-actor deterrent, must be implemented broadly to optimize security. Endpoint controls and data back-up require careful attention, particularly as employees working from home rely on their own devices and connections.

Don't lose sight of data hygiene. Back up all data to minimize loss. Offline back-ups are critical.

Conclusion

The COVID-19 disruption has made it more difficult to remediate a security breach. CISOs need to be responsive, resilient and transparent to guide their enterprises through a cyber crisis. Prepare now by focusing on business risks, increasing agility, strengthening response plans, and empowering workforces and partners to contribute to a sound security posture.

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 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.

Copyright © 2020 Accenture All rights reserved.

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