The COVID-19 disruption: Addressing cyber threats and maintaining business continuity

Accenture Cybersecurity Forum (ACF) members and invited Accenture Security clients convened on April 16 to discuss **"The COVID-19 disruption: Addressing cyber threats and maintaining business continuity."** We explored how security executives in the Middle East region are addressing potential cyber risks and operational challenges.

Our subject-matter experts were a financial services risk officer and three Accenture business continuity and threat intelligence executives. 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

The COVID-19 disruption has forced significant changes in how enterprises operate. While the specific impacts and responses vary across the Middle East, enterprises are implementing work-from-home (WFH) practices, managing through travel restrictions, and facing an evolving threat landscape.

The disruption is compelling companies to reconsider their practices on data access as more people work remotely. Across the supply chain, organizations are reviewing and, in some cases, revising contractual security requirements to maintain business continuity.

The threat landscape is changing dramatically. Threats are expected to continue to rise. Iran cyber criminals are ramping up activity, such as attacking the World Health Organization.

More than 6,000 COVID-19-related domain names were established in January alone. Many of these are the work of threat actors. As the disruption evolves, so will phishing campaigns, preying on anxiety and uncertainty. Some reports estimate that phishing attempts, many directed at logistics and distribution operations, have increased as much as sevenfold.

Travel restrictions and expatriate departures are creating talent shortages. Many customer contracts are being renegotiated to accommodate the increase in WFH employees.

CISOs are learning that meeting all these challenges requires compassion, agility and leadership.

Reliable information in a dynamic threat landscape

Bad actors are executing disinformation and social engineering campaigns to exploit anxiety and uncertainty about COVID-19. Malware and threat tools are being sold on the dark web during a single month at a rate 10 times that of a typical year. Phishing campaigns leveraging COVID-19-related lures are on the rise, even as traditional social engineering attempts continue. VPNs are constantly being probed for

weaknesses. Industrial control systems, particularly in healthcare, face new threats. Government disinformation campaigns against political adversaries, first originating in Russia, China, Pakistan and Iran, are expected to emerge from other countries.

CISOs recognize that reliable information is crucial. Sources include:

1. The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) website offers a variety of information, including risk management, telework guidance and breaking news.
2. The National Cyber Security Alliance COVID-19 Security Resource Library features information on current scams, cyber threats, risk management, remote working, disaster relief and more.
3. The National Institute of Standards and Technology blog, "Preventing Eavesdropping and Protecting Privacy on Virtual Meetings," addresses security concerns about virtual meetings.
4. The Cyber Readiness Institute has developed a guide, "Securing a Remote Workforce."

Three phases of the disruption lifecycle

CISOs are guiding their organizations through three major phases in responding to the disruption. Each phase has unique characteristics and requires specific remediation efforts. Enterprises will work through these phases at their own pace, depending on a variety of factors.

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. 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. Additional high-priority stabilization practices include:
    - Enabling remote working, including secure remote access to critical applications, collaboration tool set-up, tech support and regular communications about security practices and controls
    - Collecting reliable threat information and concentrating efforts on the highest priority threats
    - Focusing on the greatest vulnerabilities, which often will be found in shadow IT activity, networks, and e-mail attacks on accounts payable and receivable operations
2. **Normalize.** As employees adapt to working from home, CISOs can 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. Additional normalization actions might include reviewing vendor contracts and refining digital financial operations, including identification and verification practices, to strengthen transaction security.
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 directing senior management attention to the most important security priorities and are improving network security and other security measures, particularly those that might have been overlooked in the process of initially stabilizing operations. Other important optimization practices include:
    - Focusing on monitoring and maintaining employees' mental health and well-being
    - Strengthening predictive risk assessment, including increased monitoring of cyber threats

- Pressure-testing defenses by conducting tabletop exercises and scenario planning that reflect the evolving threat landscape. Some enterprises are modeling threat scenarios with senior management once a month.
- Using the disruption as an opportunity to demonstrate ROI and make the case for cybersecurity investments
- Collaborating with industry peers, customers and suppliers, such as sharing ways of identifying and mitigating threats, to strengthen the enterprise ecosystem
- Considering which new practices to keep, refine or abandon in a return to pre-disruption business conduct

Participants agreed that communications will remain a critical factor across all three phases. Ongoing disruption stresses corporate culture and employee well-being and performance. Timely, consistent communications can help mitigate the risk that people will revert to old habits or fall victim to social engineering scams.

Conclusion

Maintaining business continuity and countering cyber threats require working across the three dimensions of people, processes and technology:

1. People—CISOs acknowledged that the health and safety of employees and other stakeholders was their top priority. During this stressful time, particularly for people who are working from home, show compassion in monitoring and supporting employees' well-being. Communicate frequently and consistently to reinforce sound cybersecurity behavior.
2. Processes—Enterprises are being forced to adopt new processes to enable working from home, to keep employees in the field safe, and to meet customer requirements. For example, rules for using personal devices for business must be established for cases in which company-supported technology is not available.
3. Technology—Challenges range from laptop enablement to gathering threat intelligence, adopting new tools and gaining senior leadership support. Network considerations are paramount, such as how to connect remote employees to company networks and secure at-home networks and personal devices that might be used for business.

Enterprises that are successful in leveraging these three factors may well emerge from the disruption even stronger and more secure. CISOs are demonstrating the ROI of cybersecurity investments and setting the stage for further innovation. Collaboration with industry peers, customers and suppliers will strengthen the business ecosystem. Accelerating the delivery of new, secure digital services can improve the customer experience. Implementing the best of the new business practices can create valuable efficiencies and increase employee satisfaction.

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