In a continuing series of roundtables on the cybersecurity impacts of the COVID-19 disruption, Accenture Cybersecurity Forum (ACF) members convened virtually on April 1, 2020, to discuss **"Three CISO perspectives: Assessing our efforts in the COVID-19 disruption."** Participants shared insights on the challenges CISOs must address and potential solutions and best practices.

Four cybersecurity executives in the financial services, government, travel and technology industries served as our subject-matter experts. The session was hosted by ACF Chair Andy Vautier, Accenture CISO.

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.

Empowering employees

Vautier noted that many companies are now in a "new normal," with significant numbers of employees working from home.

Empowering employees to work from home, often for the first time, requires:

1. Expanding and securing computing and remote communications capacity
2. Maintaining compliance with company security policies
3. Alerting customers and employees about new threats and security procedures as phishing campaigns seek to disrupt financial transactions and supply chain practices
4. Aligning leadership to maintain consistent, up-to-date communications with all stakeholders

Employees who are working from home and anxious about the pandemic may be more likely to make bad decisions that compromise cybersecurity. Security leadership needs to "communicate, communicate, communicate" with your own teams, employees, partners and customers. For example, one enterprise is publishing daily work-from-home updates, holding virtual town halls several times a week, and maintaining a COVID-19 page on its intranet.

Because some employees may still be working in the field, leadership must adapt communications to acknowledge differences in categories of employees, such as essential employees who cannot work from home and others who are working from home for the first time.

Maintaining business continuity

Enterprises benefit from a culture that promotes flexibility. For example, employees working from home are adapting to social-distancing policies associated with dropping off and picking up equipment, and are using video conference calls to collaborate. While the term "business continuity" may imply a focus on only the

most critical processes, many organizations are trying to empower all functions to work in the new environment.

CISOs are weighing the right balance between matching the cybersecurity practices they had when everyone worked in office and further hardening their defenses as more people work remotely. Many organizations are rapidly increasing computing capacity to accommodate large numbers of people working from home. Even so, in many cases, employees are being asked to identify continuity-critical communications to prioritize stretched computing capacity. In addition, employees need guidance on securing their home networks and maintaining compliance.

CISOs need to look three to six months ahead at what might be the "new normal" for our enterprises, what our security posture might look like and what affect this will have on our existing control environment.

Assessing cyber threats

Threat actors are adapting to the opportunities created by the pandemic. There have been significant increases in cyber threat activity, including phishing attacks that leverage COVID-19 terms, and efforts to compromise financial assets.

CISOs are encouraged to access the U.S. Department of Homeland Security CISA website https://www.cisa.gov/coronavirus for reliable information about such topics as risk management, telework guidance and breaking news. The agency closely monitors the evolving COVID-19 situation, participates in interagency and industry coordination calls, and works with critical infrastructure partners to prepare for possible disruptions.

The pandemic is driving a concentration of threats. COVID-19 disinformation campaigns against many countries have ramped up. Ransomware attacks aimed at small and medium-sized business are on the rise. CISOs should anticipate how their organizations might respond to a major breach if some security team members were unavailable.

Mitigating cyber attacks

As security breaches occur across a distributed environment, mitigation becomes more complex. Prioritization and triage must occur rapidly even as distance and separation make security team collaboration more difficult. For example, virtual security teams need to find new ways of working together and rely on offline communication channels when traditional channels have been compromised by attackers. Security teams must look farther and deeper across their networks to identify threats that may have been handled more easily when everyone operated in an office environment.

CISOs must continue to be as agile as possible. Accenture, for example, is distributing e-mail alerts about emerging COVID-19-related phishing attacks in a matter of hours and deploying solutions in a matter of days instead of weeks. Focus on changes that can have the greatest positive impact in a compressed timeframe.

Many enterprises are stepping up security testing by executing phantom e-mail campaigns using lures related to COVID-19. The campaigns aim to reinforce a high level of threat awareness among employees and guide them in effective ways to cope with anxiety. Follow-up communications focus on encouraging and empowering employees to comply with security procedures. Messages offer constructive feedback, rather than punitive measures, and convey guidance on how to recognize scams.

Best practices

Participants shared a number of responses their organizations are making to strengthening enterprise security:

1. **Communications: Be consistent and pervasive.** Threat actors will adapt their phishing campaigns to take advantage of the news of the day. Disinformation campaigns aim to sow anxiety

and confusion. Keep stakeholders aware of emerging bad-actor efforts and updated security procedures.

2. **Architecture: Harden the work-from-home environment.** Many CISOs are rolling out secure collaboration tools, increasing VPN capacity or migrating to cloud services. Ensure that the computers and devices used by work-from-home employees are updated with the most current system and application versions.
3. **Compliance: Convert employees into data custodians.** Fully inform employees of company information protection procedures, including those regarding hard drives and file encryption in storage and in transit. Brief employees on home-network best practices and how to configure and connect to company VPN providers.
4. **Threat awareness: Cast a wide net.** Use testing to identify ways human behavior is undermining enterprise security posture. Seek reliable sources of information. Look across all threat vectors to identify and prioritize potential weaknesses.

Conclusion

Vautier summed up the situation CISOs are facing: Many of the attributes of the new threat landscape are well understood. People are more alert to the risks of phishing and e-mail compromise. Most enterprises are implementing sound communications practices with leadership, employees, partners and customers. Technology infrastructures are being stressed, but so far are generally holding up well. While expansion of work-from-home has forced the temporary relaxation of some security controls, companies are focusing on strengthening their defenses. Still unclear is whether there will be a “new normal” of cybersecurity and what it might look like as we work our way through the pandemic.

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 505,000 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 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