accenture security

ACCENTURE CYBERSECURITY FORUM

THREAT INTELLIGENCE AND HYBRID SECURITY: A VIEW ON EMERGING THREAT ACTOR BEHAVIORS AND RESPONSES

VIRTUAL ROUNDTABLE SUMMARY

AUGUST 8, 2019

DISCUSSION

On August 8, 2019, the Accenture Cybersecurity Forum (ACF) convened virtually and in person at Black Hat USA for a 60-minute roundtable, "Threat intelligence and hybrid security: A view on emerging threat actor behaviors and responses." The discussion focused on the increasingly challenging threat landscape, as outlined in the recent Accenture Security 2019 Cyber Threatscape Report; and best practices—strategic, operational and tactical—in effective use of threat intelligence to reduce risk.

The cyber threat landscape is becoming more complex. Where once there was a segmentation between nation-state actors and financially motivated hackers, increasingly these threat actors are working together. Hackers may penetrate an enterprise and sell that access to a nation-state perpetrator.

CISOs and senior security executives from several industries and organizations joined the roundtable to discuss the increasing sophistication of threat actors, their expanding collaboration, and the need for stepped-up threat intelligence efforts by CISOs.

Our subject-matter expert for the call was Josh Ray, managing director—Accenture Security and co-author of the Cyber Threatscape Report. Session hosts were ACF Co-chairs Andy Vautier, Accenture CISO, and John Valente, 3M 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.

The discussion addressed emerging threat actor behaviors; strategic, operational and tactical use of threat intelligence; and responses to boards of directors' concerns.

Emerging threat actor behaviors

The rising incidence and cost of cyber crime compel organizations to make effective use of actionable threat intelligence. Trends toward more costly regulation, deepening threat actor sophistication and multiplying vulnerabilities all contribute to the importance of threat intelligence.

Ray discussed several key issues raised in the Cyber Threatscape Report, which identifies top threats influencing the cyber landscape, including changes in techniques and relationships among threat actors in the underground economy. Cyber crime campaigns and high-profile advanced persistent threat groups are changing how they target victims and focusing more on intricate relationships with "secure syndicate" partnerships to disguise activity. In addition, high-profile cyber crime operating models are shifting. There is a significant increase in threat actors and groups conducting targeted intrusions for major financial gain, also referred to as "big game hunting."

Malicious cyber operations, often supported by a combination of nation states and rogue bad actors, will continue to be used to influence events. "Bad actors don't have to execute a cyber attack themselves to cause problems. They can sell access to a previously hacked network, thereby making attribution that much more difficult," Ray said. Threat actors no longer have to actively compromise or breech an organization to have the same type of impact.

The global disinformation battlefield will continue on social media. Global disinformation campaigns will expand to attempt to influence social media users as threat actors become more skilled at exploiting legitimate tools. Adversaries have adopted active measures or information operations tactics to engage in misinformation campaigns via various social media outlets to negatively impact specific companies or even whole industries at the macro level.

DISCUSSION

Ransomware will increasingly plague businesses and government infrastructure as threat groups provide network access for sale, with the number of ransomware attacks more than tripling in the past two years. The good news, Ray reported, is that malware analytics continue to improve. The bad news is that disinformation campaigns and ransomware attacks are likely to increase.

While conventional cyber crime operations remain, they are also evolving, according to Ray. Close-knit syndicates exist alongside localized underground economies, especially in non-English-speaking countries. Rogue bad actors are collaborating with nation states.

A CISO asserted that nation-state attacks are becoming much more frequent, which magnifies the importance of actionable threat intelligence. Many participants agreed that the threat landscape is getting “darker.” Some CISOs felt, however, that the threat landscape has always been this difficult, but awareness of the threats is much greater today.

Threat actors are paying even closer attention to important global events and are using them as distractions or lures to breach target networks, especially via social media platforms. There has been a sharp decline in “true” hacktivism and an increase in state-sponsored hacktivism with goals to disrupt events and influence a wide range of activities in the sponsoring nation’s favor. Nation states are increasingly outsourcing malicious cyber operations to cyber criminals to increase capabilities and attain strategic goals—blurring lines between politically and financially motivated cyber threat activities.

In addition, while threat actors remain focused on infecting legitimate software applications with malicious code to accomplish supply chain compromises, they are also changing how they work and who is part of their inner circle. They have started to close doors on the open sharing of malware and exploits and, instead, are sharing only within smaller, trusted syndicates.

The strategic value of threat intelligence

From a strategic perspective, threat intelligence should be tightly linked to the enterprise value chain and carefully considered in important business decisions such as M&A, new product development and market entry.

Participants agreed that cybersecurity investment decisions are always challenging. Ray advocated a hierarchical approach that looks at the enterprise ecosystem and prioritizes threat intelligence investments in points of greatest value. He encouraged CISOs to identify which links in the value chain drive profit and competitive advantage, and to work with ecosystem partners to pinpoint the greatest risks and opportunities to mitigate risk through threat intelligence.

In addition, CISOs should look at risks from the attacker's or threat actor's perspective, Ray said. "See what information they're after and what motivates their behavior in order to inform your own activities. Understand from your adversaries' perspective how they are looking at your enterprise."

The impact of threat intelligence on business operations

The CISO must help the business understand how enterprise operations—and those of supply chain partners and other third parties—may be at risk. Threat intelligence must encompass the extended enterprise ecosystem and not be limited to the four walls of the organization. Drawing on threat intelligence, CISOs must help the broader business leadership understand what threat actors are interested in, their objectives, and possible activities and impacts. Encourage business leaders to ask, "What would happen to our operations if a particular system went down?" Cybersecurity needs to be a discussion of business value, Ray asserted. "It's not just about technology; it needs to be part of your operational DNA." Specific points of discussion between CISOs and the business could include the following:

- Increase business leader awareness that while each new layer of technology may add value, it also creates new risks.
- Regularly provide a candid, real-time view of the good and bad of the cybersecurity landscape. Vautier reminded the group, “Your cybersecurity measures are never good enough forever.” The evolving effects of cyber threats on supply chain management, third-party risk, and M&A functions mean organizations must adopt proactive, intelligence-driven approaches to cyber defense.

Tactical execution

Cyber crime operations are constantly evolving. Tactically, the focus should be on protecting the enterprise’s high-value targets and being able to respond rapidly. Well-trained cybersecurity talent is essential. However, given a shortage of cybersecurity professionals to meet demand, machine learning and other technologies should also be used to identify security anomalies. Along with threat intelligence, automation is essential to maintaining strong enterprise cybersecurity.

Testing is also crucial. Adversary simulations and red teaming are among several activities enterprises can use to verify security.

CISOs need to anticipate the secondary effects of attacks, such as the deeper implications of a ransomware intrusion. Consider what kinds of intelligence you would need to get a system back up and running, recommended one CISO. Each layer of technology can improve your ability to react and protect your assets.

Vautier added, “The tooling and automation you deploy need to be ubiquitous and real-time in response.” As various sites or elements of infrastructure are weaponized, you need to be able to detect the event and shut them down.

Boards of directors’ concerns

Board communication was a key topic of conversation among roundtable participants. In light of the expanding threatscape, cybersecurity should be discussed with the full board, not just the audit or risk committee. CISOs should outline for the board how threats could affect the extended enterprise ecosystem.

Furthermore, cybersecurity at the board level should not be left to the CISO’s updates alone. CISOs and other members of the leadership team should make joint presentations about how strategic decisions might impact the enterprise risk profile. For example, one CISO stated that his enterprise’s communications with the board include a quarterly threat actor matrix review, high-level reports of actual events and how the cybersecurity team responded, and a deeper dive to inform the board about key issues such as cloud security and risks to international operations. Roundtable participants agreed that they should encourage the business to surface cybersecurity implications in management discussions with the board.

CONCLUSION

Ray outlined three recommendations:

- **Protect what's valuable and focus your intelligence efforts there.** Know how your enterprise creates value and be aware of the threats to those activities. Prioritize resources in high-value areas.
- **Use threat intelligence across the enterprise ecosystem.** Collaborate with participants throughout your ecosystem to protect value. Include suppliers, customers and employees in discussions about behaviors required to increase cybersecurity.
- **Create a culture that shares intelligence and best practices among peers.** Engage with CISO peer groups, both industry and geographical, as an added line of defense.

Valente reminded members that ongoing risk analysis is needed as changes occur in both organizations and the threatscape. He reinforced the value of building strong networks with other CISOs to discuss challenges and possible solutions.

Vautier agreed, emphasizing that growing risks underscore the importance of threat intelligence and CISO peer networks. "Engagement with other CISOs is essential as we deal with the live fire of an increasing variety of security threats." The challenge for CISOs is to get high-value threat intelligence, combine it with a nuanced view of the enterprise's specific threat landscape and technology environment, and use these insights to guide enterprise strategies and activities.

CONTACT

ANDY VAUTIER
CISO, Accenture
Co-chair, Accenture
Cybersecurity Forum

JOHN VALENTE
CISO, 3M
Co-chair, Accenture
Cybersecurity Forum

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 482,000 people serving clients in more than 20 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 drive 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 www.accenture.com/security.

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us