accenture security

# ACCENTURE CYBERSECURITY FORUM

## Threat intelligence and actions steps in light of increased Middle East tensions

**VIRTUAL ROUNDTABLE SUMMARY**
**JANUARY 7, 2020**

# DISCUSSION

**In response to rising Middle East tensions, the Accenture Cybersecurity Forum (ACF) convened a special 60-minute virtual roundtable on January 7 to discuss the topic "Threat intelligence and actions steps in light of increased Middle East tensions." Our focus was on the current threat intelligence landscape; what to hunt for; and steps CISOs can take immediately, in the next week, and in the long term to protect their enterprises.**

Our three subject-matter experts for the discussion were Jason Lewkowicz, Accenture deputy CISO; Justin Harvey, Accenture Security managing director and incident response lead; and Howard Marshall, Accenture Security managing director and intelligence director for cyber threat intelligence services. They were joined by ACF chair Andy Vautier, Accenture CISO; and Valerie Abend, Accenture Security managing director and regulatory and financial services lead, North America, and chair of the ACF Women's Council.

Below is a summary of the discussion. The subject-matter experts' comments during the roundtable were drawn from numerous sources, including posts from many providers as well as the Accenture Security iDefense "Situation Report: Iranian Retaliatory Cyberattacks Likely After Soleimani Killing in Baghdad Drone Attack," which estimated with moderate to high confidence that threat groups based in Iran or sympathetic to the aims of the Iranian government are likely to carry out cyberattacks at some time in the future in retaliation for the event, unless tensions de-escalate first.

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.

## Threats and threat actors

Vautier noted that recent events and escalation of geopolitical tensions mark a material change in the threat landscape. As such, they constitute a call to action beyond the routine hygiene CISOs use to defend their enterprises every day. Marshall declared, “When, not if, retaliation will occur is a foregone conclusion. The only questions are ‘how’ and ‘to what extent.’” According to Accenture Security iDefense analysis, the highest risk industry targets include industrial, oil and gas, financial services, government, universities, technological and research organizations, and airlines. Among the key groups associated with potential retaliatory activity are PIPEFISH, BLACKSTURGEON, SKATE, and BREAM, as well as various hacktivists-for-hire. Key anomalies to be on the look-out for include irregularities in outbound and inbound network traffic, e-mail vectors, and windows logs and events.

## Immediate responses in light of potential threats

Well aware of the threats posed by recent geopolitical tensions, CISOs are focusing on maintaining business continuity, mitigating the impact of potential threats on customers, and coordinating closely with vendors and other partners across their ecosystems. Members are engaging with their operational technology partners to reaffirm and update recovery processes.

Accenture’s immediate response includes doubling down on routine defense and hygiene processes, and taking specific actions related to threat hunting and identifying potential Iranian and proxy threat actors. Lewkowicz added that Accenture, in collaboration with partners, has identified eight specific high-priority threat actors and is analyzing their techniques to identify likely threats. Furthermore, Accenture is looking across all domains to identify and prioritize potential threats and vulnerabilities that might require immediate remediation.

Cross-border coordination is top of mind in global organizations. They are taking steps to provide protections for overseas employees, such as notifying them of diplomatic services in the event personnel must quickly leave a country and making secure VPNs available for communications. CISOs are working closely with physical security teams to determine how recent events affect travel, physical security and response plans from a people point of view.

Members agreed that it is essential to keep executive management informed of threats and enterprise preparedness. One participant emphasized the importance of “no surprises.” Many CISOs said that communication was an immediate priority. Howard recommended, “Never let a crisis go to waste. Stand up, stay positive and be proactive.” Vautier added that this kind of leadership can pay dividends during budget discussions.

## Best practices

Roundtable participants discussed specific actions CISOs should take in the context of their cybersecurity preparedness, including the following:

- Have discussions with security teams internally and across the ecosystem to agree on threat responses. (“If this happens, what will we do?”)
- Amplify awareness across the enterprise about threats to IT, OT and workforce safety, and about what the enterprise is doing in response to potential threats.
- Look for bad-actor behavior in authentication and privileged account access. Review current telemetry for specific Iranian threat vectors that might impact IPs, domains and URLs.
- Know your high-value assets and prioritize defenses.
- Focus on protecting administration and privileged access to systems, the most likely vector of attacks.

- Ensure the capacity of response teams, including breach remediation partners, to handle attacks, particularly since attacks often occur outside normal operating hours.
- Collaborate with supply chain partners to confirm appropriate responses and processes for addressing attacks. Establish recovery plans in the event of disruptions.
- Obtain access to a variety of credible threat intelligence sources, both to receive alerts and to ask questions as the threat landscape evolves. The MITRE Corporation, for example, provides federally funded cybersecurity research and development resources with specific information on Iranian threat actors.

## CONCLUSION

In closing, Vautier said it is clear that the CISOs on the call are taking a disciplined approach to addressing recent developments in the threat landscape. This is important because the threats, while unclear, are real. CISOs are approaching the situation from multiple dimensions—IT and OT, physical and digital, internally and across their supply chains and ecosystem partners.

## CONTACT

**ANDY VAUTIER**
Accenture CISO
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 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**