
**“A Perspective on Nation State Security Risks"**

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “A Perspective on Nation State Security Risks," on May 6, 2021.

During this roundtable our subject-matter expert shared his views on the past, present and future of cybersecurity, and Forum members engaged in a peer-to-peer discussion about the role of the CISO in protecting the enterprise, the US and the global community against increasingly sophisticated cyber criminals.

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, nor participants, is revealed.

We are sharing a brief summary from the call for both attendees and those who were unable to participate:

- The evolution of cyber conflict is analogous to the evolution of the airplane, said the subject-matter expert. The US military before World War I saw the early airplane as a surveillance tool to capture information about adversarial troop movements. Only later was the airplane recognized as an offensive weapon that could deliver weapons, and later it became the delivery mechanism for strategic weapons. Similarly, cyberweapons have evolved from a means of intercepting data to a powerful tool of competitive advantage, disruption, disinformation and theft.
- The subject-matter expert said that different nation-state threat actors have different strategic intent, reflecting their national interests -- and paralleling their actions in the bricks-and-mortar world. China is using cyber to capture intellectual property, control anti-government activity, and spread its global power by building the networks other nations rely on. (Huawei's 5G networks are a good example.) Russia, which may have relied on more than 1,000 people to execute the Solar Winds attack, according to an estimate by Microsoft, is acting as a disruptor, attempting to undermine elections, destabilize governments, even threatening to destroy underseas cables that enable internet traffic. Iran is focusing on both disruption and disinformation, using cyber means to retaliate for the sanctions against it. North Korean cyberattacks aim to redirect cash to that financially strapped nation, sometimes stealing from central banks.
- When asked about the threat that the internet might someday be disabled, the subject-matter expert said that the interconnections among nations contributed to a higher level of safety. He cautioned, however, that nations such as North Korea or Iran that are less dependent on

foreign trade or the internet, might be inclined to use an internet attack as a response to sanctions.

- Cyber conflict is complicated by the diversity of threat actors, from nation-states and business-like criminal enterprises to rogue actors and tech-savvy teenagers. This makes classic deterrence, of the kind that has worked in the nuclear arena among superpowers, far less useful in cyber. There is no equivalent of "mutually assured destruction," which was a key to nuclear deterrence. No single defense works in every case. Furthermore, nation-states are engaging criminal enterprises to conduct attacks because the difficulty in attributing responsibility gives them deniability.
- A Forum member expects that the nation will get better at cybersecurity defense but that the problem will be with us perpetually. The subject matter expert agreed, noting that new forms of malicious cyber activity arise regularly. He pointed to the rapid rise of ransomware, which is funding the next generation of attacks. (The most recent ransomware attack on Colonial Pipeline is a good example.) He added that the US has the talent to improve defenses, singling out the phenomenal talent within the NSA capable of developing offensive weapons.
- CISOs should think about cybersecurity in terms of both defense and resilience. Detection techniques, two-factor authentication and other defenses are important but not sufficient. Enterprises also need resiliency. For example, threat actors might be discouraged from attacking an energy grid if they knew three backup systems were in place, and that the attack was bound to fail. CISOs should also remember that “cyberattacks aren’t always about you,” as the subject matter expert put it. Threat actors tend to seek to dismantle larger systems beyond the enterprise.
- Thinking about cybersecurity as a mere technology problem is short-sighted. It is a political problem, a policy problem and a technology problem -- the best analogy may lie in countering terrorism, where good defenses are matched with government offenses. At the national level, enterprises and government must partner to deploy diplomacy and retaliation to counter threat actors. Enterprises cannot do this alone. The US government wants to avoid responsibility for cybersecurity that enterprises take on themselves but doesn’t want enterprises engaging in unilateral retaliatory strikes. Sorting out the responsibility for strategic cybersecurity decisions about technology, diplomacy and retaliation requires public/private partnership.
- The subject-matter expert said the US executive order (EO) on cybersecurity could help strengthen the nation’s base level of security but would not provide protection from Solar Winds-type attacks where networks were already invaded. And while it sets a good example -- one that may trickle through the private sector -- the President can only mandate the activities of companies that do business with the Federal government. It would take Congress to set requirements for the private sector, an effort that has failed repeatedly.
- Forum members advocated for real-time information sharing. The impact of other efforts, for example, by the United Nations, the US Cyber Command and the government of Denmark, have been mixed, at best.

**Action items**

Actions that the subject-matter expert raised during the discussion include:

- When speaking to other C-level executives who may be uncomfortable with technology, CISOS should explain that cybersecurity is at the center of global conflict. They should tell stories to help non-technical executives understand the bigger picture and engage them in understanding what happened and why it is important—all in terms that are easily understood.

- Operating in China requires in-depth management discussions about the extent to which an enterprise is willing to segregate operations and encrypt data. A useful guide to China's intent is to review the nation's latest five-year plan for greater self-reliance. A useful example is to look at the extensive coverage of the compromises that companies like Apple have had to make in order to continue doing business in China.
- The subject-matter expert recommended a strong after-action review of the Solar Winds incident but said that, unfortunately, there doesn't seem to be any real interest in that. An NTSB-type oversight organization might be helpful in generating lessons learned from major incidents; a prototype is mandated in the executive order.
- He suggested that information-sharing could be improved if the government declassified almost all cyber incident information. CISOs raised the idea of an institutions such as a digital Geneva Convention to set standards and provide enforcement.

**CONTACT**

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

**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 514,000 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.

View the entire suite of ACF roundtable summaries on our webpage – here.