The Cyber Weapons Arms Race

and the Future of Cyber Defense

Accenture Cybersecurity Forum
Global Executive Leadership Network

29 September 2022
Session Summary

From the ACF Chair

It is useful, although sometimes a bit anxiety-inducing, to look at the threat landscape through a global lens, beyond the horizon of my own enterprise. The immediate threats associated with Russia's attack on Ukraine make that wider perspective even more valuable.

That's why, like other Accenture Cybersecurity Forum members, I was particularly interested in hearing about "The Cyber Weapons Arms Race and the Future of Cyber Defense" from a best-selling author who has written extensively about cybersecurity and nation-state threat actors.

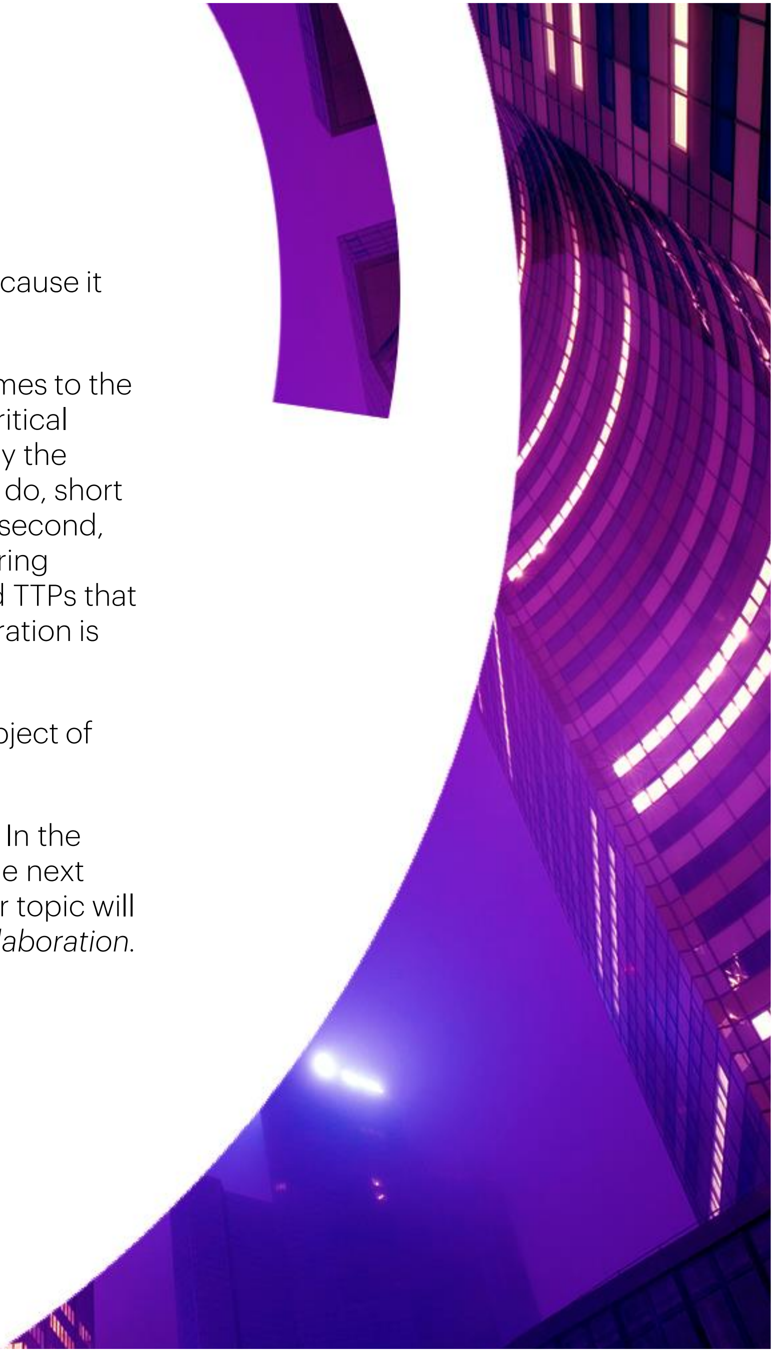
Our guest subject-matter expert, who now is an advisor to CISA, actually gave me reasons for optimism. Among her insights:

- "Russia clearly has significant capabilities and we're still nowhere where we need to be as a country in terms of what I call a cyber iron dome. But we are in a much better place than we were even two years ago."
- "Ransomware was a blessing in disguise because it pen tested the United States."
- "The NSA has a huge blind spot when it comes to the cyber landscape and potential threats on critical infrastructure because 85% of it is owned by the private sector. I think the only thing we can do, short of regulation, is what we're doing right this second, which is getting on Slack channels and sharing indicators of compromise and malware and TTPs that we're seeing on our networks. That collaboration is working."
- "Board conversations are moving to the subject of cyber resilience, which is terrific."

If you want to connect, just drop me an email. In the meantime, looking forward to seeing you at the next Cybersecurity Forum on October 27, when our topic will be, *Cracking the Code on C-level Security Collaboration*.

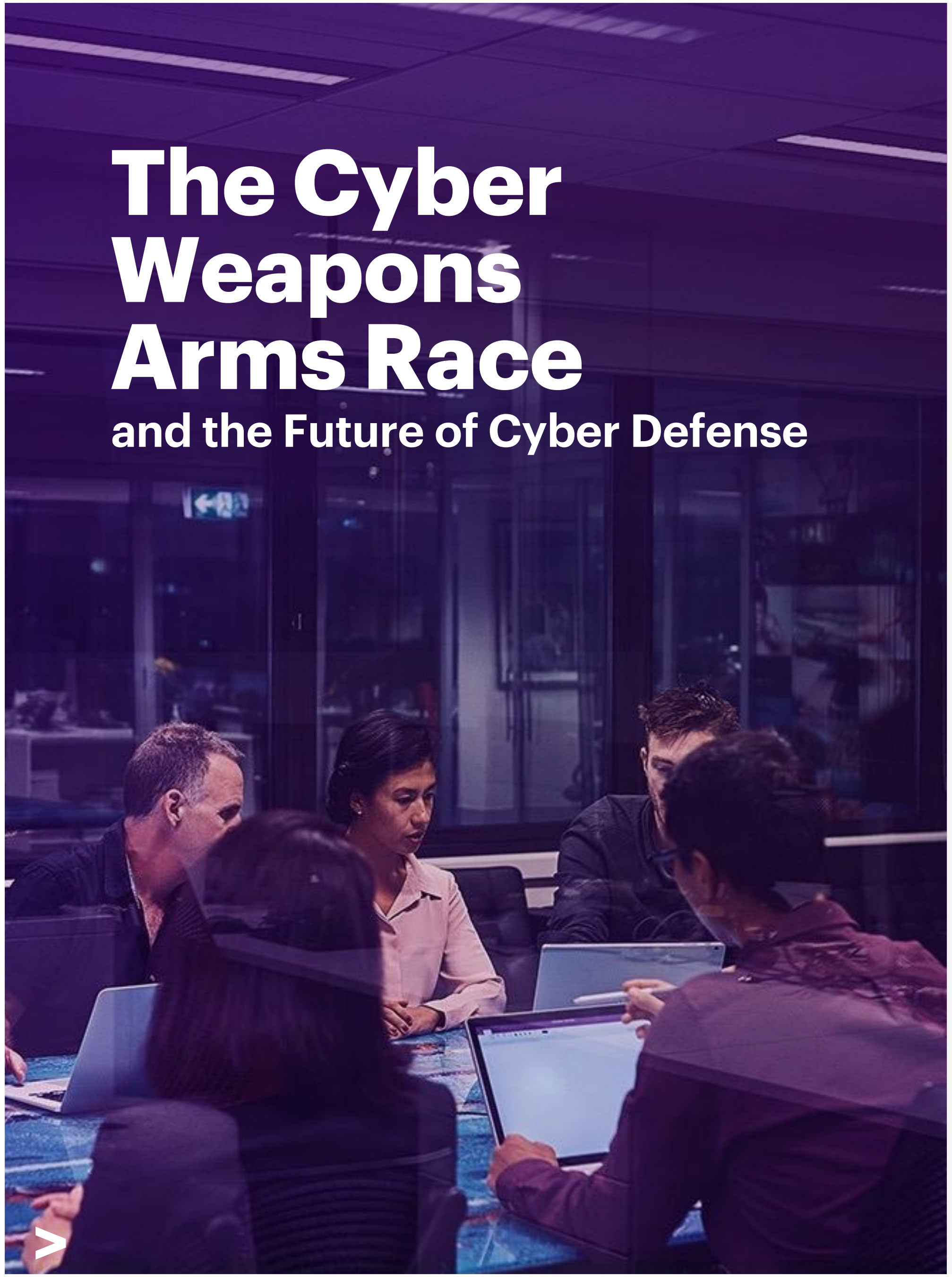
Cheers,
Kris Burkhardt
Accenture CISO, ACF Chair

LinkedIn: Kristian Burkhardt



The Cyber Weapons Arms Race

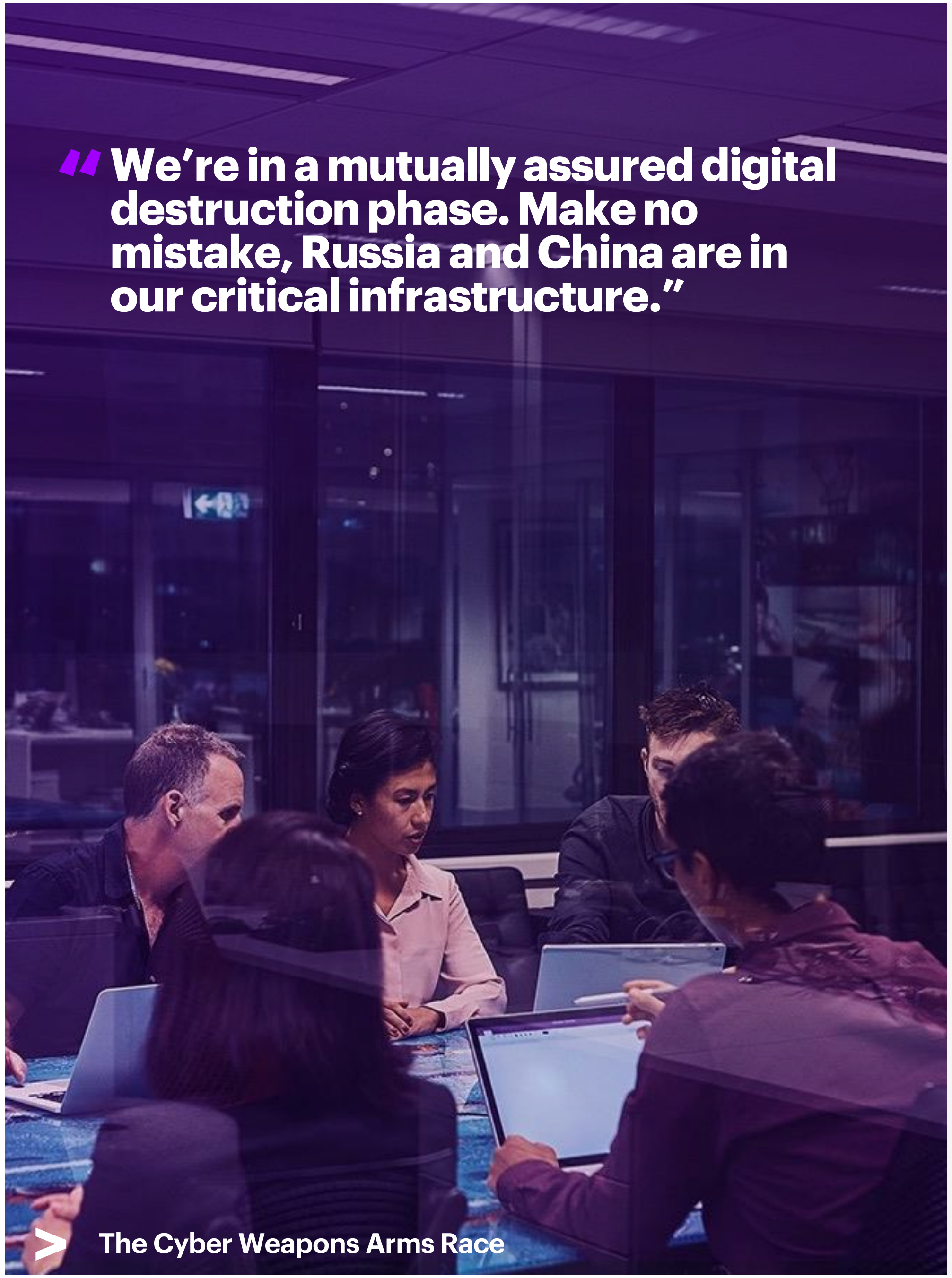
and the Future of Cyber Defense



The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “The Cyber Weapons Arms Race and the Future of Cyber Defense,” on September 29, 2022. Members heard from a best-selling author who has written extensively about the impact of cyber attacks and the challenge of securing our enterprises, and who currently serves in an advisory capacity with the US Cybersecurity and Infrastructure Security Agency (CISA).

This 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.

In this summary:



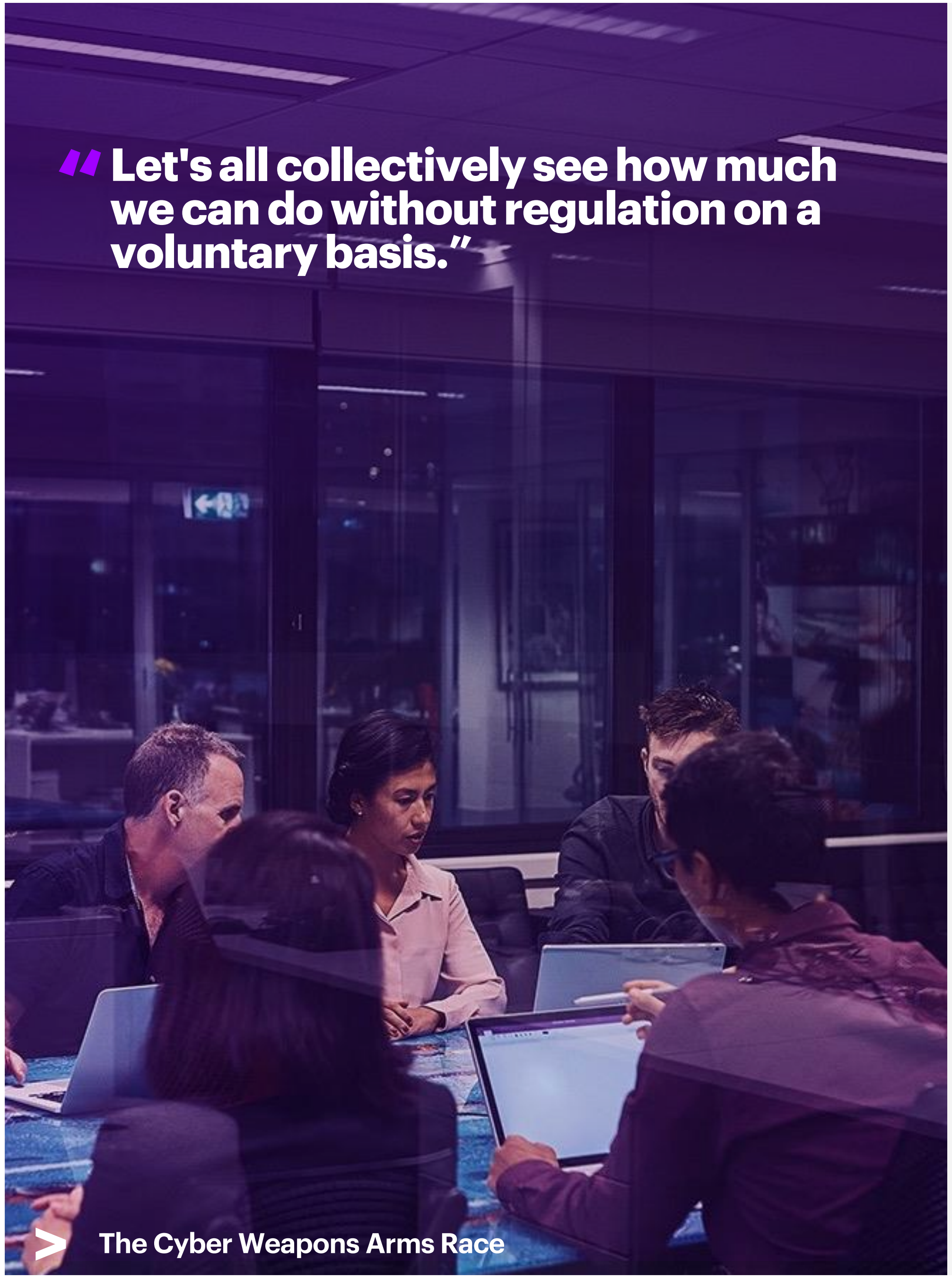
> “We’re in a mutually assured digital destruction phase. Make no mistake, Russia and China are in our critical infrastructure.”

Enterprise implications of the War in Ukraine

Russia’s 2017 NotPetya cyber attack on Ukrainian banks and other infrastructure was in fact also a “test kitchen” effort to assess its ability to attack the US and other countries, said the subject-matter expert. “The impact of NotPetya was significant on Ukraine, but it wasn’t that bad because that country is not that digitized, there’s not a lot of code in Ukraine’s infrastructure.”

Now the US and allied nations are using Russia’s attacks as their own test kitchen, collaborating on identifying and mitigating emerging threats such as Pipedream, a malware toolkit intended to disrupt industrial control systems. “Now the good guys, in my opinion, are using Ukraine as sort of test kitchen for what real time collaboration and public/private partnership can look like. And there is a lot to celebrate here,” the subject-matter expert said.

On a cautionary note, the expert said: “We’re in a mutually assured digital destruction phase. Make no mistake, Russia and China are in our critical infrastructure. But we’re in theirs too, and the question is, what is the geopolitical incident that will compel someone to pull the trigger?”



> “Let's all collectively see how much we can do without regulation on a voluntary basis.”

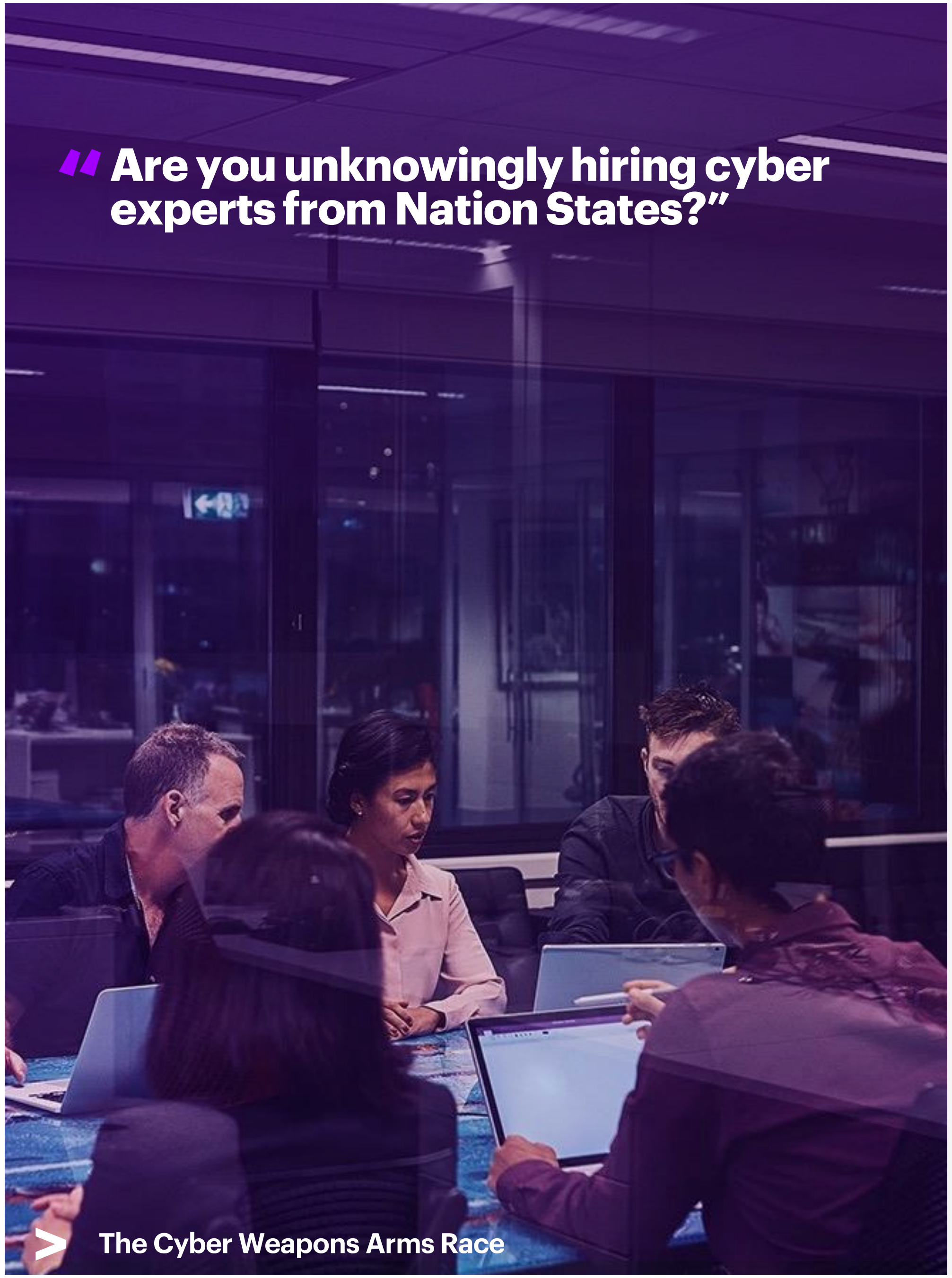
Moving from defense to resilience

Most management teams understand that cyber attacks are inevitable. While the defense basics remain essential, over the last 10 years enterprises are considering “what is the minimal viable business we can maintain in the event of an attack?” Management teams have identified the “crown jewels” that need the highest priority protection. Continuity plans are more detailed. Actions to minimize the blast radius are defined and tested.

Evolution is also occurring in the Secure DevOps space. The Chief Product Security Officer role at software suppliers is becoming more common. Security and software engineering are in concert during agile development, in effect code testing or “spell-checking” as code is being written.

Governments should consider offering incentives for stronger cyber defenses

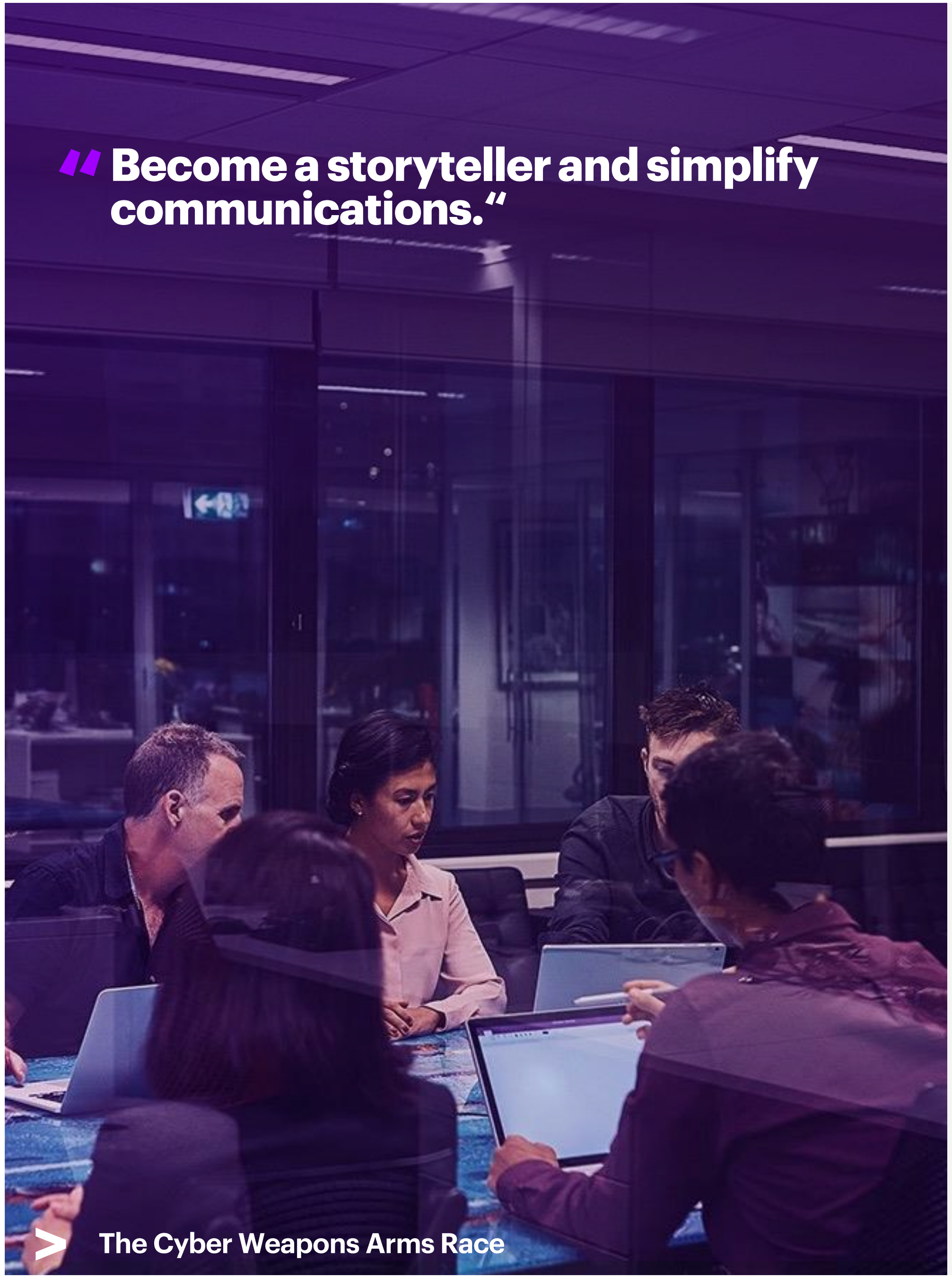
The subject-matter expert shared the attitude of Forum members who believe that tax breaks and other incentives are more effective than punitive regulations. “The Computer Fraud and Abuse Act is one of the worst blunt force policies ever created,” the expert said. “Let's all collectively see how much we can do without regulation on a voluntary basis.”



"Are you unknowingly hiring cyber experts from Nation States?"

Humans: The weakest link in cyber defense

The subject matter expert said insider threats present a "real quagmire" with no easy answers. But the expert also noted that some companies are actually enabling potential insider threats by, for example, hiring cyber experts from Nation States that could pose a threat.



“Become a storyteller and simplify communications.“

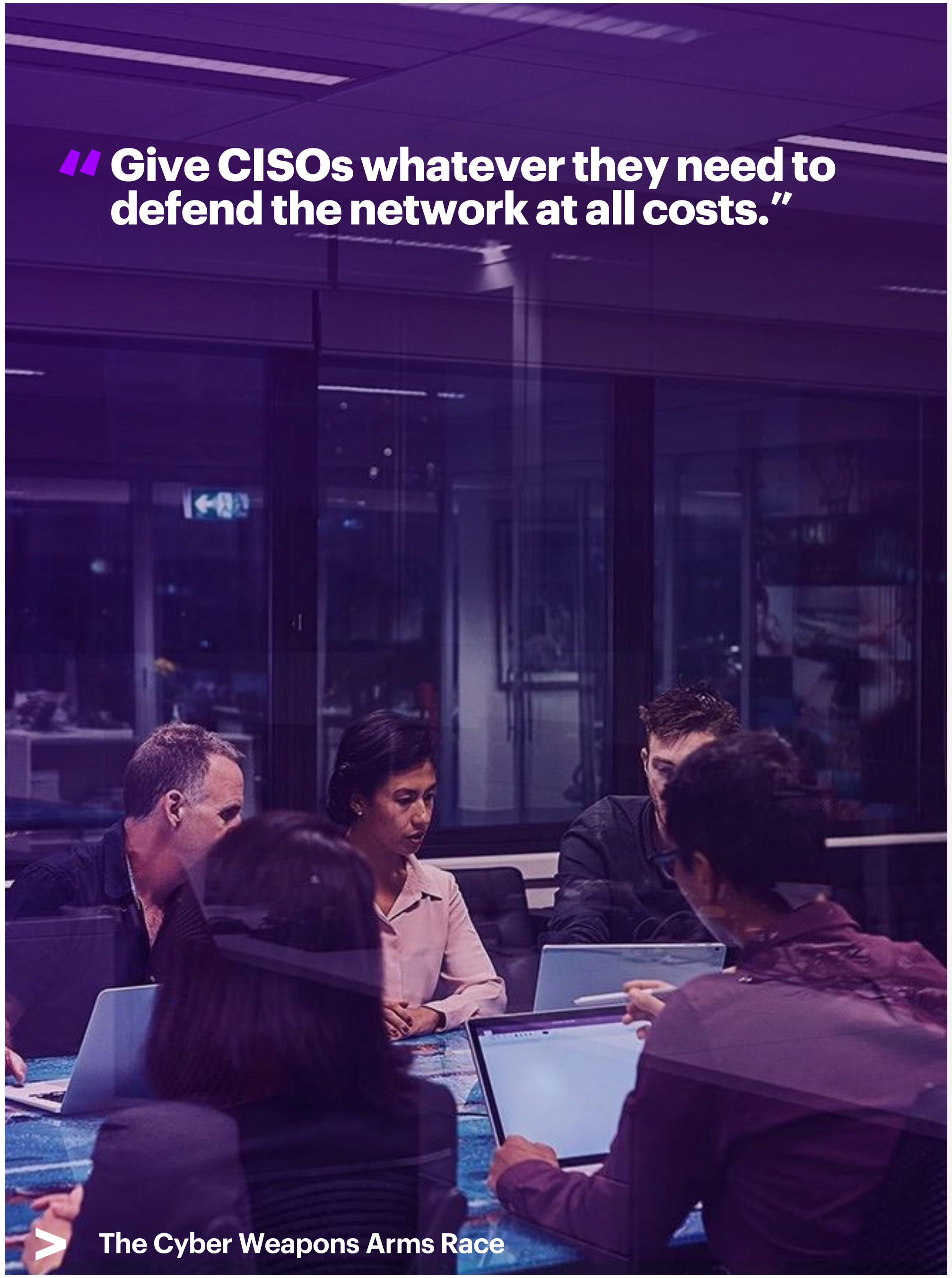
Leading practices

❑ Don’t underestimate China. That nation is taking a strategic, long-term view towards their threat posture. Spear-phishing remains a prominent weapon but phishing techniques are getting much more sophisticated and aimed more frequently at intellectual capital and other crown jewels. “It’s no longer spray-and-pray,” the subject-matter expert said. “They are in our critical infrastructure, not for the intellectual property, but to gain a foothold for an attack in the event of some future conflict.”

❑ Become a storyteller and simplify communications. “Jargon is a real obstacle in helping people understand the risks of their behavior,” said the subject matter expert. She cited a tech company that explains to everyone, from senior developers to the janitor: “If you click on a suspicious link, someone may end up in solitary confinement in a foreign country. That’s powerful.”

Another example: “A CISO developed a check list, such as ‘Do you have multi-factor authentication turned on’ and hung the list over the entrance to all the women’s bathrooms and above every urinal in the men rooms. He claimed that was the most important step he took to drive employee compliance.”

❑ Confirm cyber insurance coverage. Cyber Insurers are starting to exclude nation-backed cyber attacks from policy protections.



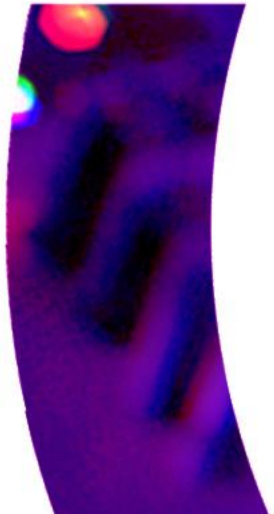
“Give CISOs whatever they need to defend the network at all costs.”

Leading practices (cont.)

- □ Empower your CISO. The subject-matter expert said she advises CEOs and boards: “Give CISOs whatever they need to defend the network at all costs. And empower them in soft ways too, such as having them speak at every all-hands meeting, even if just for five minutes, to remind everyone that cybersecurity is a huge priority.”
- □ Call upon third parties for specific expertise. Few enterprises have all the requisite tools, tactics and policies internally to provide solid defense.
- □ Help the Board understand what’s being done to improve the attack surface.
- □ Establish your minimal viable business model.
- □ Continue protecting critical infrastructure. “I think the only thing we can do, short of regulation, is what we're doing right this second, which is getting on Slack channels and sharing indicators of compromise and malware and TTPs that we're seeing on our networks. It's working.”

> “Let’s share what we know to secure what we must.”

— **Kris Burkhardt** Accenture CISO, ACF Chair



Work the network

Contact our team directly
for questions and member introductions.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 721,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at 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 @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.

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