Engaging with Law Enforcement

Accenture Cybersecurity Forum
Global Executive Leadership Network

04 August 2022
Session Summary

From the ACF Chair

Most of us have had at least one CISO experience with law enforcement, and many of those experiences were in the middle of a crisis, robbing of us of the opportunity to build a deeper understanding in the moment.

So, when Accenture Cybersecurity Forum members said they wanted to hear from national and global law enforcement, we decided to assemble panelists from the U.S. Department of Justice, the U.S. Secret Service and Interpol. They came prepared to share practical advice and to answer some tough questions. We all appreciated their participation; the follow-up feedback from members confirmed the usefulness of the discussion.

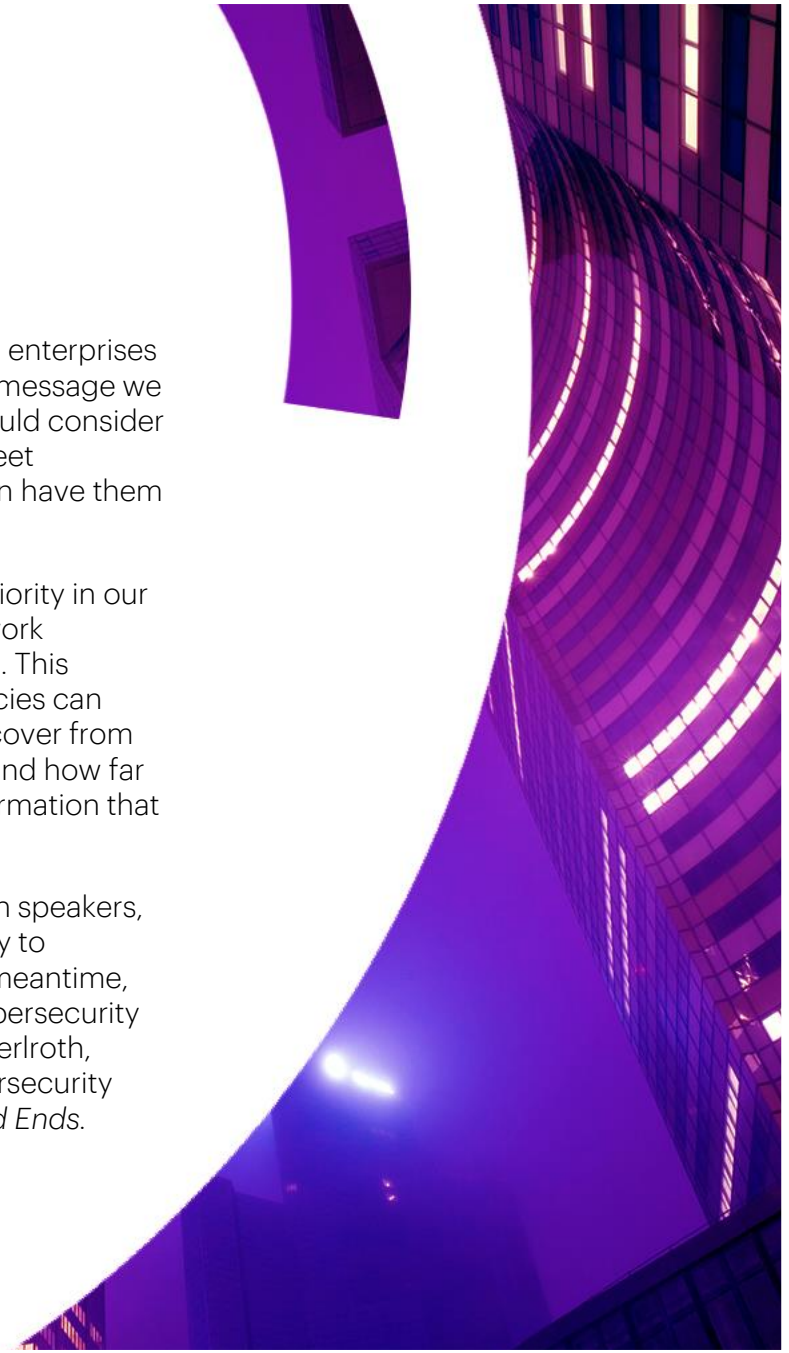
I personally came away with some fresh perspectives and several adds to my to-do list.

- I have a greater appreciation for just how complex it is to work with multiple law enforcement agencies. We need to take that complexity—multiple jurisdictions, agency capabilities, priorities and points of contact—into account when we refresh our incident response plans and update management and the board. This will help us and the agencies save time and do a better job.
- Law enforcement's willingness to treat our enterprises as victims of cybercrime was a refreshing message we heard from all the representatives. We should consider their offers to have regular discussions, meet representatives of other agencies and even have them participate in our tabletop exercises.
- Law enforcement relationships will be a priority in our risk management strategy. We'll need to work together to set expectations on both sides. This includes who to call, when, and how agencies can contribute to our defenses and help us recover from attacks. And the agencies should understand how far we can and cannot go in contributing information that will serve the common good.

If you want to connect with any of the session speakers, or other Forum members, we would be happy to facilitate. Just drop me an email here. In the meantime, looking forward to seeing you at the next Cybersecurity Forum on September 29, with guest Nicole Perlroth, *New York Times* alum and author of the cybersecurity best seller, *This is How They Tell Me the World Ends*.

Cheers,
Kris Burkhardt
Accenture CISO, ACF Chair

LinkedIn: Kristian Burkhardt



Engaging with Law Enforcement

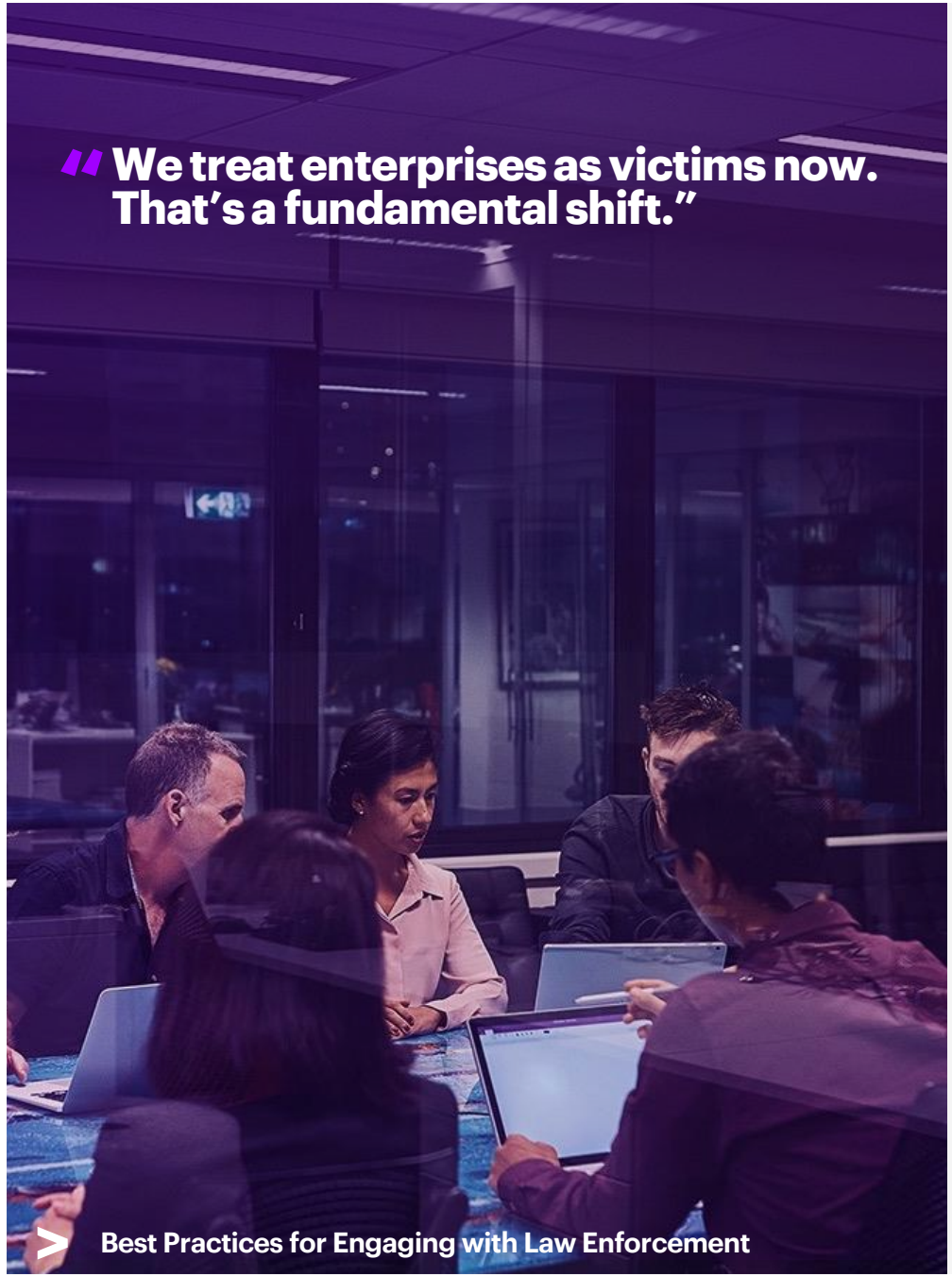
Best Practices

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Best Practices for Engaging with Law Enforcement,” on August 4, 2022. Members heard from representatives from the U.S. Department of Justice, the U.S. Secret Service and Interpol.

Forum members believe that engagement with law enforcement is of great interest. They seek clarity regarding the nature of support and value they will receive before, during and after a breach or an extortion event. They also seek assurance that their collaboration, as the victim of cybercrime, will be properly recognized by law enforcement.

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:



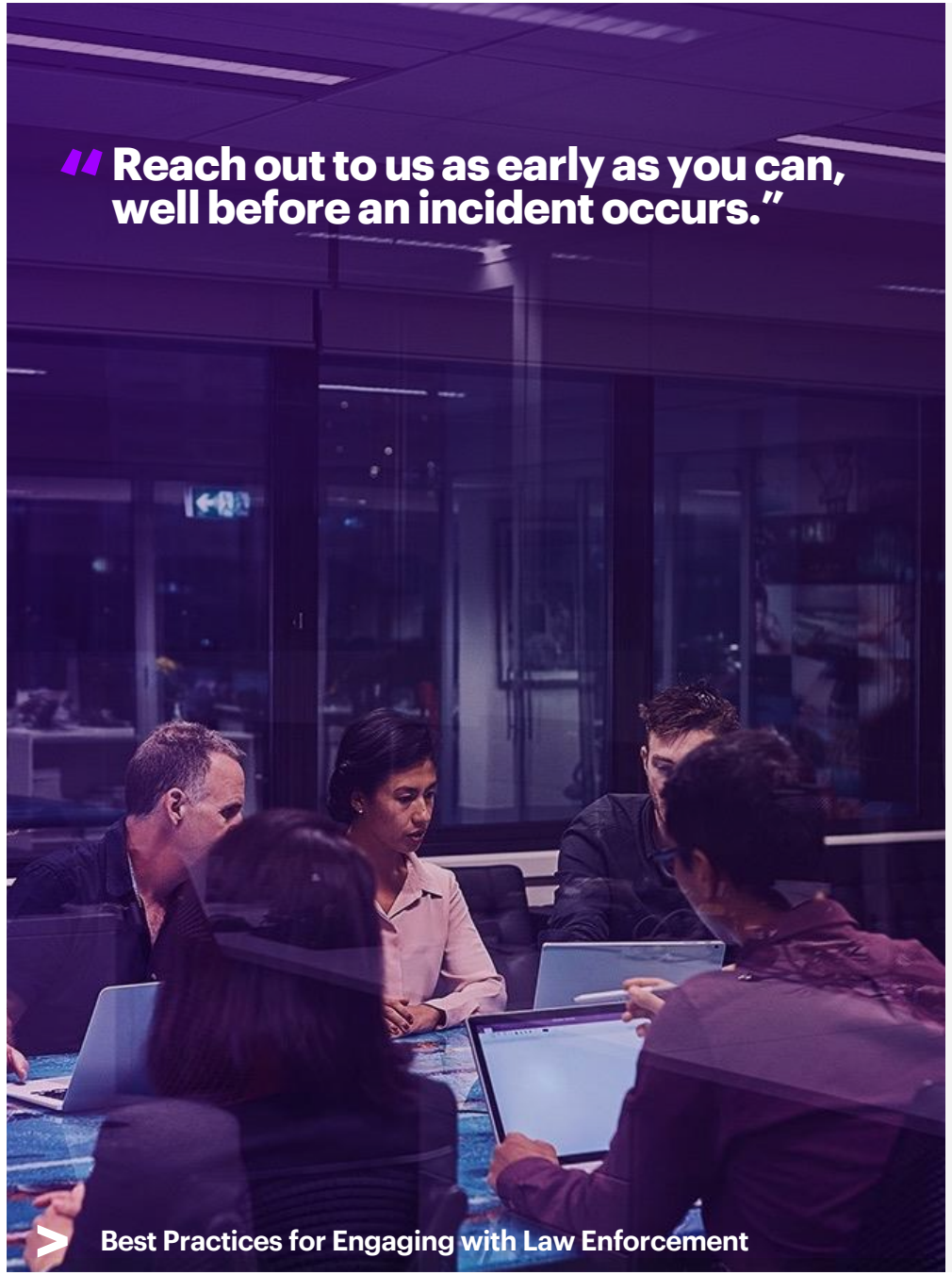
Evolution of the relationship between law enforcement and the private sector

Law enforcement representatives agreed that the priority of their agencies has shifted toward building constructive relationships. “We treat enterprises as victims now. That’s a fundamental shift,” said a representative.

At the Department of Justice, “Twenty years ago we were more interested in building a criminal case. We still want to catch the bad guys, but now we want to provide the enterprise victims of cyber-attacks with customer service.” For example, Justice has been successful in capturing decryption keys used in ransomware attacks, often without the knowledge of the criminal.

The U.S. Secret Service focuses on financial crimes, including fraud and money laundering. “Prevention is our top goal, but we also help companies recover assets,” said a representative.

At Interpol, the priorities are prevention, detection, investigation and disruption. Leveraging its presence across almost 195 countries, Interpol is creating a network of public/private partnerships for sharing information, building cyber defense capabilities and even removing key personnel from criminal enterprises.



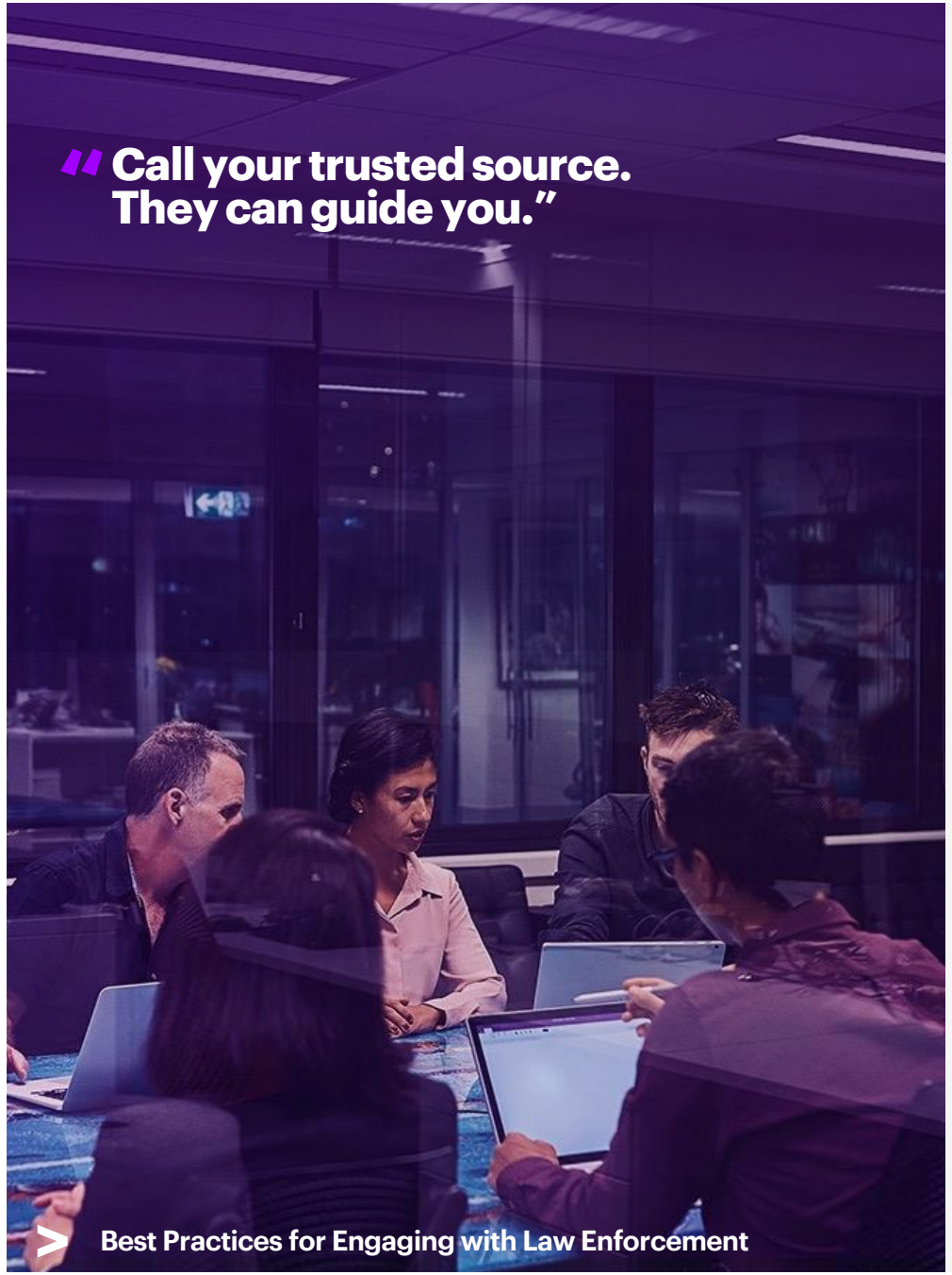
Building trusted relationships with law enforcement

Several Forum members mentioned the challenge of prioritizing relationships with multiple law enforcement entities. Law enforcement representatives said they recognize it can be difficult to harmonize information. They said they are trying to address it but admit more intra-agency and cross-border progress is needed.

One perspective to keep in mind is that regulators and law enforcement bring different priorities to the table. A law enforcement representative said that regulators focus on law enforcement; they are looking to apply punitive actions against unlawful behavior. Law enforcement agencies working in cybersecurity see the greatest value in collaborating with the private sector to improve overall cyber defenses for the benefit of citizens, enterprises and nations.

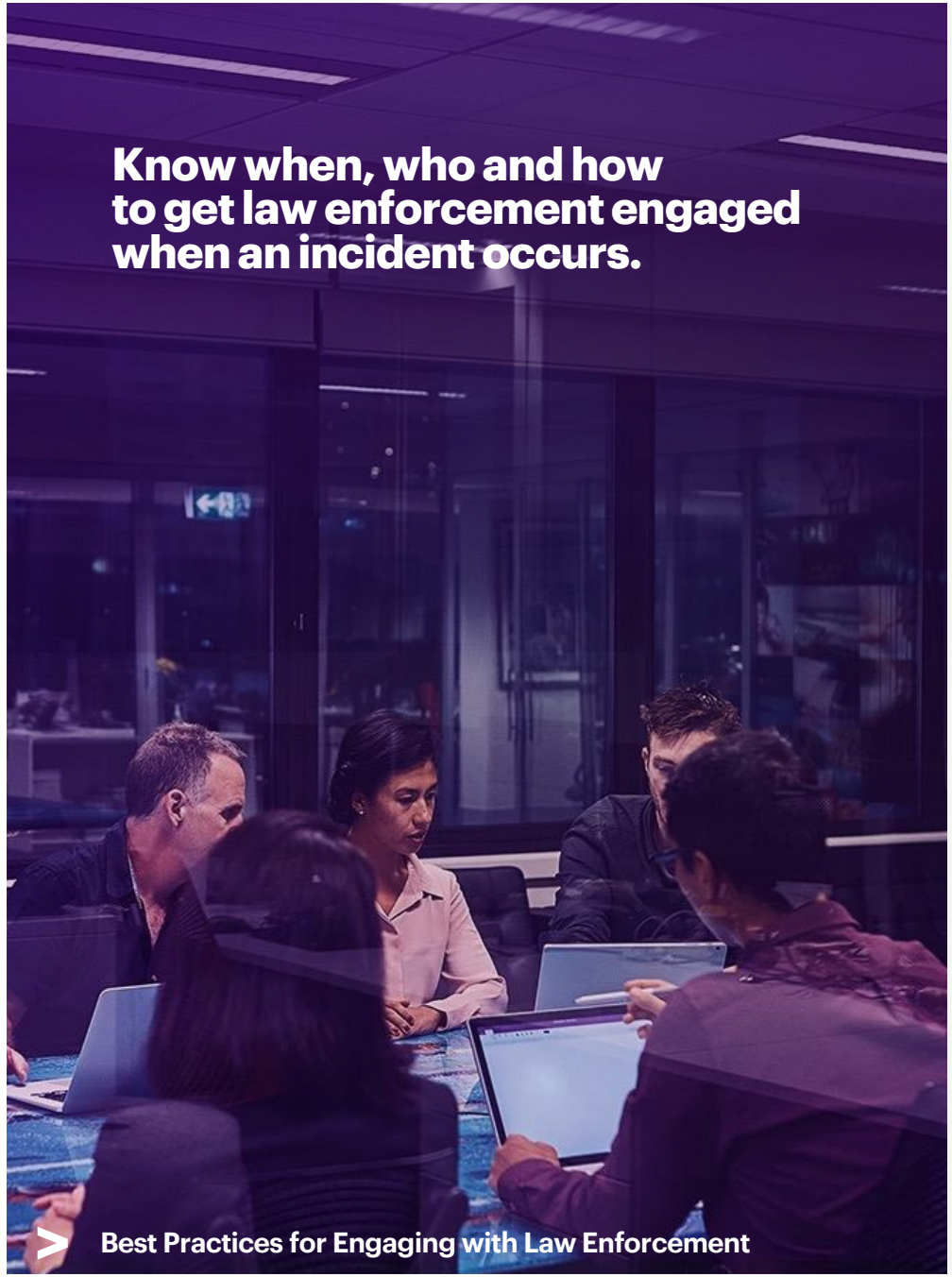
The terms “early” and “often” were expressed consistently throughout the discussion. “We encourage you to reach out to us as early as you can, well before an incident occurs,” said a law enforcement representative. Another representative said the success in recovering stolen assets greatly improves if law enforcement is notified in the first 48 hours after an incident.

Another suggested that conversations don’t necessarily need to be deep, but frequency matters. “Make friends with multiple contacts at the FBI, where you’re headquartered, where you store data and at Legal Attaché offices outside the U.S., suggested a law enforcement representative.



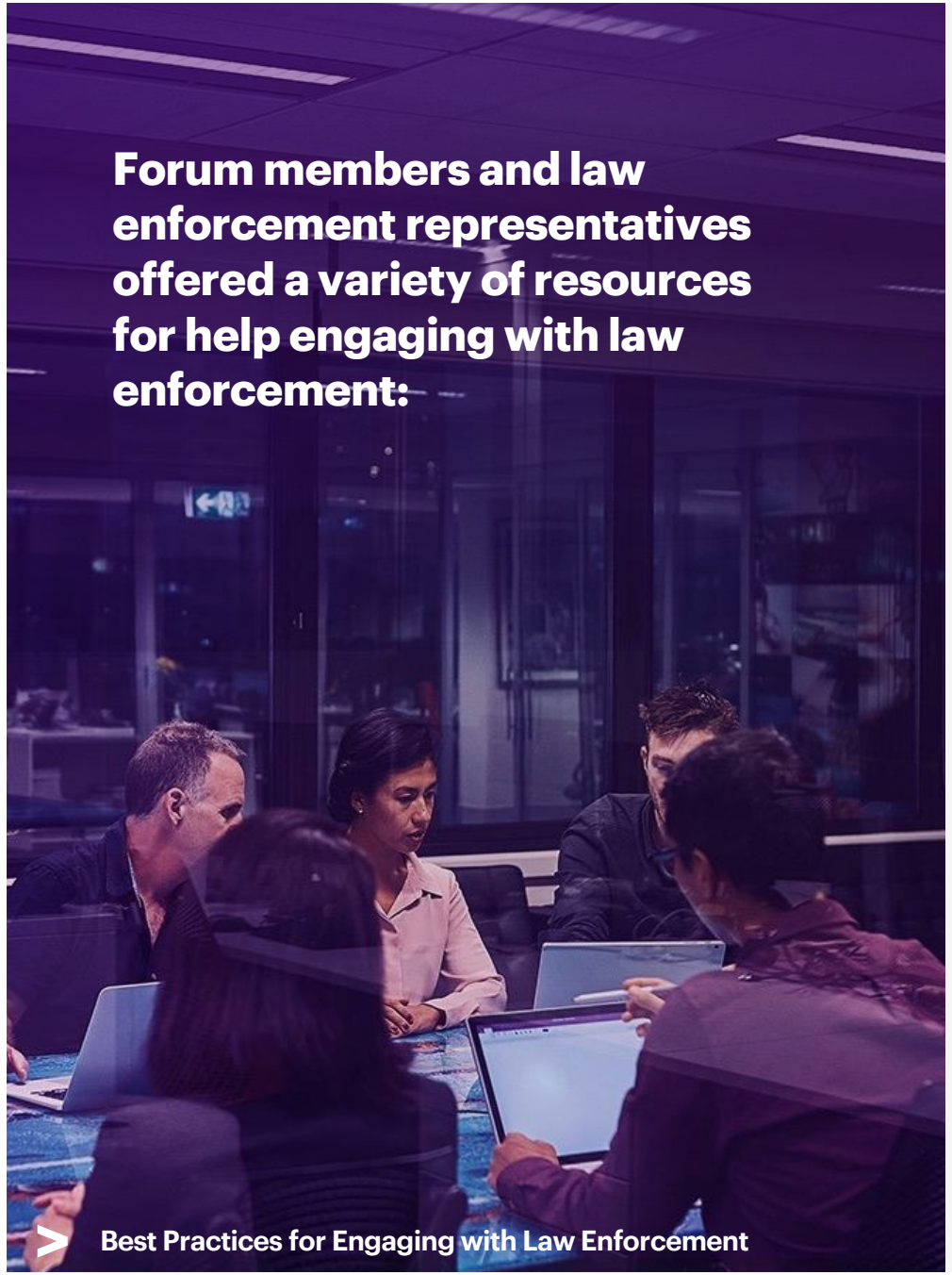
The role of legal counsel

A Forum member suggested that CISOs and legal counsel need to prepare and practice together in advance of actually engaging with law enforcement. “That can be a very fruitful collaboration,” they said. Another added, “Working with outside counsel and establishing attorney-client privilege can help keep information confidential. In my experience, working with counsel has always been positive and helped keep us out of potential trouble.”



Leading practices

- Build relationships with law enforcement before an incident. Continuous engagement can be helpful in keeping your enterprise top-of-mind. Ask for introductions to build relationships within other jurisdictions.
- Prioritize relationship-building efforts. Cyber is no single agency's responsibility, so CISOs may be operating in a very complex engagement model. Suggestions include turning first to whomever you trust most; determining which agency can be most effective in addressing your most significant risks.
- Integrate law enforcement engagement into the incident response playbook. Know when, who and how to get law enforcement engaged when an incident occurs.
- Bring law enforcement into tabletop exercises.
- Collaborate closely with your legal counsel.
- Inform the CEO and board of directors of the latest law enforcement engagement practices. It is not always common knowledge that law enforcement agencies have shifted their priorities to treating enterprises as victims of cybercrime.
- Leverage law enforcement engagement when working with regulators. A law enforcement representative said: "Regulators take an enterprise's willingness to cooperate with law enforcement into account and look favorably on that engagement as they consider a case."



Resources

Internet Crime Complaint Center (ic3.gov). The FBI encourages the victims of internet crime to file complaints through their online portal.

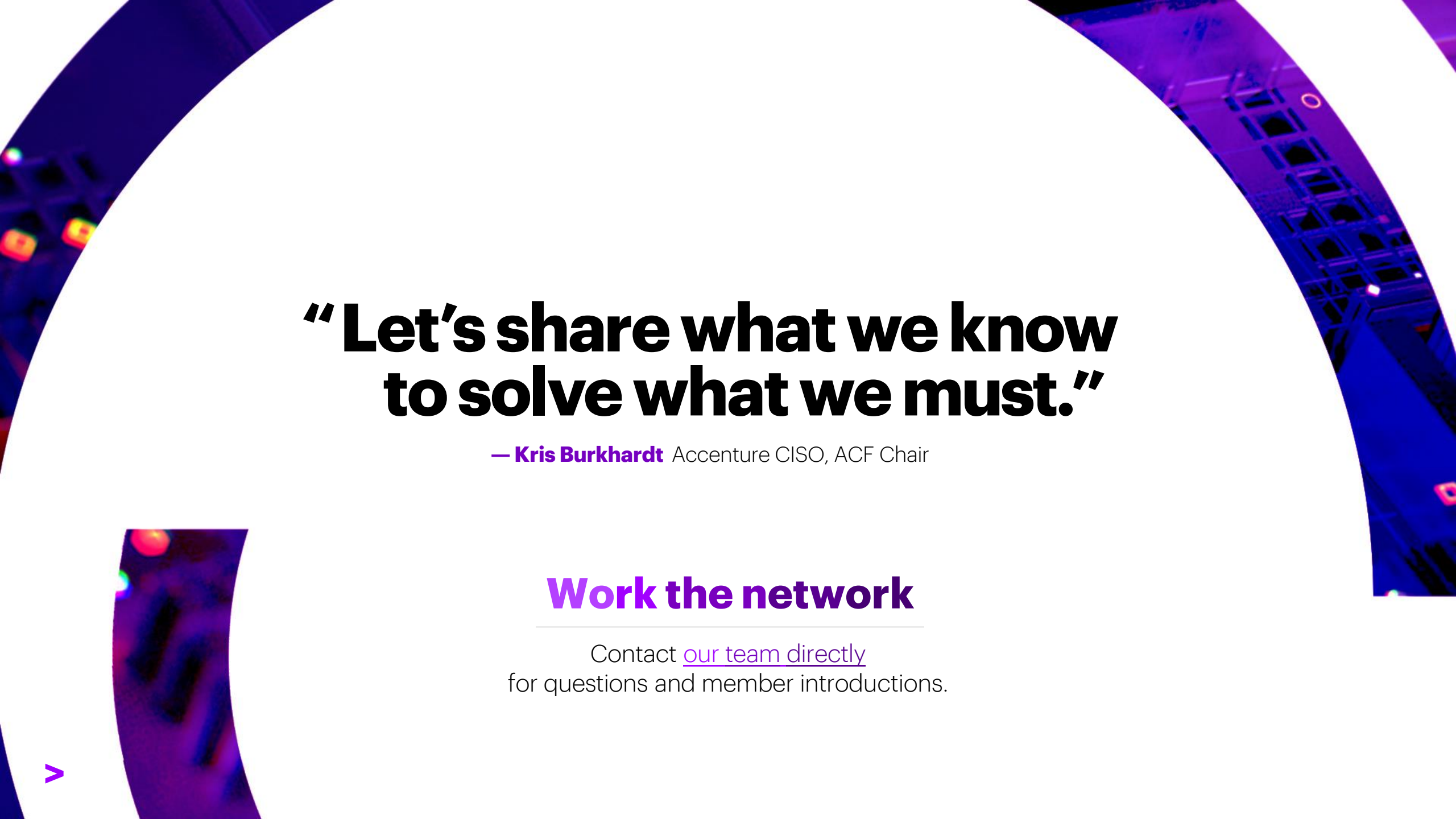
InfraGard, a partnership between the FBI and the public sector, protects U.S. critical infrastructure by sharing industry-specific insight about emerging technologies and threats. A Department of Justice representative said that CISOs may find "PINs" (Private Industry Notifications) and "Flash" reports (deep technical insight) particularly valuable.

The Secret Service offers a website with information to help CISOs and their legal counsel prepare for incidents. Topics include Contacting Law Enforcement and *Reporting Cyber Incidents to the Federal Government*.

The U.S. State Department's Overseas Security Advisory Council, with chapters in more than 150 countries, published free country-specific security reports: https://www.osac.gov/

The **UK National Crime Agency** (NCA) offers support through the National Cyber Security Centre - NCSC.GOV.UK

A Forum member with substantial operations in Canada suggested turning to the **Canadian Centre for Cybersecurity**: https://cyber.gc.ca/en



“Let’s share what we know to solve 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 710,000 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.