
**Incident Response: Perspectives from the Front Line**

The recent ransomware attack on U.S. fuel pipeline operator Colonial Pipeline was a timely reminder of just how vulnerable businesses are to cyber incidents—and how CISOs are on the front lines of both business and professional resilience.

At our May 13, 2021 Accenture Cybersecurity Forum Women's Council virtual roundtable, top women enterprise security leaders, women board members and male allies shared their insights and professional growth around managing major incidents. The discussion explored which incident response activities attendees were most comfortable with and areas they felt they needed to grow. Attendees also exchanged ideas on the evolving role of the CISO as a communicator for their organizations and the skills needed to be successful in that role.

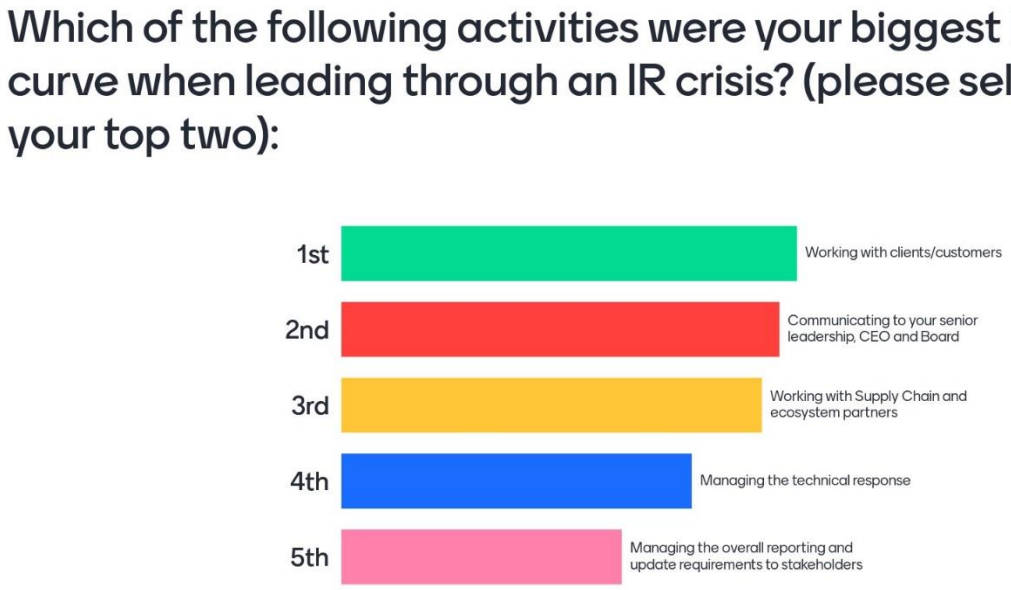
Leadership communication expert and coach Dr. Laura Sicola moderated the discussion and shared tips for communicating clearly, creating confidence, and getting results.

The following is a high-level summary of the rich, candid conversation.

## Comfort and Discomfort During a Time of Crisis

The conversation kicked off with two polling questions for attendees. The first question asked which key incident response activities they were most comfortable performing. The results show that members are most comfortable communicating details to the board and leadership, followed by managing overall reporting and update requirements.


The second poll question asked members what areas they felt they had the biggest learning curve when leading an incident response crisis. Working with clients/customers was most often selected, with communicating to leadership a close second.



That “communicating to leadership” ranked high for both polls was a surprise to many, but the post poll discussion revealed that comfort likely comes from:

- **Experience in the role.** “…communicating up for those of us that have been doing it for a while tends to be just very second nature,” a participant said.
- **Nature of the conversation.** Gone are the days of lengthy technical explanations to the Board, which can prove challenging for CISOs without technical backgrounds. Now CISOs must communicate quickly and accurately as to what and how a breach or disruption happened, and more importantly, what is being done to minimize the impact. One participant said, “the board wants to know that you understand how it's impacting the business and you're doing the right thing for the company.”

## Succeeding in the Communicator Role

Members pointed out that the role of CISO has greatly expanded over the years. Today, they have a more visible role and are being asked to speak directly to investors and the board, and even appear before Congress. “You have to be the face and the voice in front of the operations as well, whether it's to internal or external audiences,” a participant said.

For most, being a public spokesperson is not a natural skillset, but a necessary one. Attendees shared strategies and suggestions to become successful communicators.

- **Have a consistent core message.** It is extremely important to be clear and unwavering on what your core message is as it relates to your brand, what your commitment is to customers/ partners/shareholders, and what level of trust you want to continue to inspire in your audience.
- **Do not get “stuck in the expert curse.”** Female CISOs often feel compelled to demonstrate their own technical credentials which often detracts from their briefings to leadership. In communicating to the Board, a participant shared, “…conversations around those technical details and networks are not as relevant as they were three to five years ago.”
- **Be ready so you are not caught off-guard.** “Too often the security responders are so technically focused and busy following the thread that they lose sight of the broader engagement needs that are essential,” a participant said. One member shared that she has a standing agenda for IR calls to ensure that response focus is appropriately balanced across technical and non-technical response activities.
- **Be clear in ALL your communications.** “When you're briefing, whether it's in government or on these boards, distill down to ‘here are the facts versus here's what I'm opining on,’ so they understand that threshold,” a participant said. This hold true for notes and emails—make sure nothing gets lost in translation as you never know who will be forwarded the information.
- **Improve your communication style.** Dr. Sicola added the importance of communicating in a confident way. She shared that this is especially important in our current mode of video conference calls where even the visual and audio can reenforce or undermine your messaging. What bad habits do you have when you are nervous? Do you hold your breath or breathe

irregularly causing your voice to trail off when you finish a sentence? Or does your voice go up at the end of sentences making everything sound like a question? She recommended training yourself (or working with a coach) to use a full voice and let your pitch drop so you speak declaratively.

## Rise in Third-Party Risk

Managing the security needs of your own organization is a full-time job. In addition to leading the security program, the role now requires an understanding and management of the risks your customers/clients and supply chain (third- and-fourth-party) might introduce. For many attendees third-party risk is a new and persistent challenge. Results from the poll suggest it is an area members feel they have much to learn. Below are helpful insights attendees offered on managing that risk:

- **Lower your expectations.** "Understand that not everybody is as prepared to handle an incident as we would think they would be," a participant said. If you are working an incident with a client, vendor, or customer who does not have all the things they should have in place, do not be afraid to tell them what they need to know and what they need to do. In the end, you will earn their trust and get what you need from them in an emergency.
- **Rethink contracting and build in a notification clause.** You do not want to learn via the news or a third-party that your vendor, partner, or client had a breach or incident. As part of your security program, you should have language regarding incident communication in your third-party contracts and SLAs.
- **Build a partnership.** Some members spoke candidly of recent third-party cyber incidents and noted challenges around the lack (or complete absence) of timely information shared with them. When it comes to working with your ecosystem and getting third-party vendors to share sensitive information early, it might be easier when you already have a trusted relationship. One member suggested building trusted, collaborative relationships could be the better approach to change the culture going forward.
- **Expand your IR playbook.** Given the significant rise in third- and fourth-party breaches, be prepared by creating a playbook that specifically addresses what to do when faced with these types of breaches.
- **Prepare your team.** Some attendees shared that clients have asked to talk to their security teams, revealing a new requirement: the need to train team members to be client-facing. Rather than be caught off-guard, CISOs should ensure their staff knows the core message, what they are allowed to say, how to message it to different groups, and how to present themselves to establish credibility.

## Steps for a Successful Incident Response

Improving operational resilience has been a growing focus for many sectors, but the global pandemic and the rise in cyber attacks has put resilience on the agenda of almost every company. This shift has

put the spotlight on incident response and its role in the success or failure of a business hit by an attack. Attendees shared a variety of suggestions and best practices for improving incident response.

- **Make security a company responsibility.** Having everyone at your company feel responsible for security is an earmark of a mature security program. While getting your company to embrace the idea that "it's not a security incident, it's a company incident" can be a long journey, but worth the effort.
- **Take time to understand your business**. Get to know the different areas of your business and what may be critical to them before an incident happens. You will be better prepared to respond with the right amount of expediency to help them get back up and running.
- **Build relationships early and often.** A participant said, "It's not always a great experience to meet somebody for the first time when their functions having an issue." Introductions within your company shouldn't start when you have an incident. Instead, become a part of the onboarding process. Introduce yourself, your team, and your function to new executives or key roles, like customer experience, to establish a relationship and trust. If you do not have time to establish those key relationships, one attendee suggested developing a document that details what to expect during an incident, what your team provides/does, and what you will need from them.
- **Do not be afraid to ask questions.** "Early on in my career I wished I would have asked, 'I know we have this plan, but how does it actually work?'" a participant said. You will save yourself time (and possibly embarrassment) and likely build trust among your team by admitting what you do not know and leaning on them to help you.
- **Empower your team.** Successful incident response is a team effort, but some CISOs—particularly those with IR backgrounds—admitted difficulty stepping back and letting technical teams do the hands-on stuff. This can deter teams to feel empowered and be proactive. CISOs need to allow the technical teams to do their work**.**
- **Build confidence among your team.** Regular (not every 2 years) training and exercising your IR playbooks ensures everyone knows what they are supposed to do and gives them an opportunity to do it. "When you train and let them know they can do it, and then you exercise and have them do it, you help them build that confidence," a participant said.
- **Establish clear decision makers.** For large organizations there can be ambiguity as to who can and should make critical decisions during an incident response. To circumvent that issue, one CISO established a formal role of Incident Commander in her company. When this person is not leading an active incident response, he or she is conducting IR drills, incident planning, process improvement, and continuing education. The role is also part of a career track, allowing event analysts to advance to instant responder and then to incident commander.

## Words of Wisdom

We closed with a request to Council members to share three words or phrases of advice they would give to a new Women's Council CISO facing her first major incident. We captured those thoughts in a visual below. While the word cloud is filled with encouraging statements and advice, the most often cited

words—transparency, confidence, communications, and breathe—speak strongly to the importance of communication skills and a reminded of how much the requirements of the CISO have evolved.


Contact Information for Executive Communication Coach Laura Sicola, PhD:
laura@vocalimpactproductions.com
vocalimpactproductions.com

**Forum Contacts**

Valerie Abend
Accenture Security Managing Director
Accenture Cybersecurity Forum Women's Council Co-Chair

Lisa O'Connor
Accenture Security Managing Director
Accenture Cybersecurity Forum Women's Council Co-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 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.