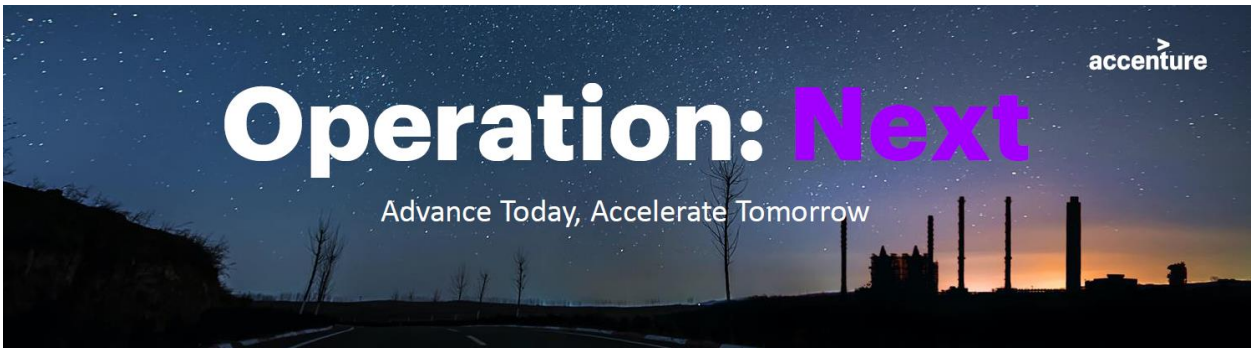

"Future OT security challenges"

As part of Accenture Security's half-day virtual summit, Operation: Next, on March 24, 2021, European and United States senior security executives were invited to join two time zone-appropriate virtual roundtables with peer cybersecurity executives, board members and operational technology (OT) security luminaries. Participants explored OT security challenges and opportunities, including how OT security stakeholders, across various industries, are getting program buy-in, articulating risk, maximizing budget and implementing programs. A number of Accenture Cybersecurity Forum members participated in the discussions.

At the conclusion of each roundtable, subject-matter experts and OT leaders discussed OT security priorities going forward, including adoption challenges, governance, balancing people, processes and technology and getting board of directors' buy-in.

People and process priorities

- **Managing the pace of change**—Security executives feel the pressure to get control over their physical assets and OT networks. The rush is driven by ambitious threat actors, C-suite and board risk management concerns and digital transformation. However, the complexity of OT solutions makes rapid deployment difficult. One subject-matter expert said: "OT is now where IT was several years ago, but the pace of network technology has only increased from that time. When IT was figuring out how to improve its security posture, it did not have to simultaneously figure out how to integrate cloud dataflows, Edge computing solutions that require substantial external connectivity and other modern use cases."
- **Integrated solutions and platforms**—There is a need for integrated solutions and tools that work together and for platforms that support the delivery of OT and IT security outcomes. "We need collaboration and we need to bring all the enterprise defenders together in aligned harmony to defeat the bad guys," said one OT security expert.
- **Talent and capabilities**—"It took years to build a security culture within our enterprise," said a CISO. One security expert cautioned, "A lack of knowledge transfer creates real risks to our capabilities because a lot of OT talent will be retiring in the near future. The OT environment will never be replaced as quickly as the IT environment so we should be thinking about knowledge transfer now."

- **Adoption**—"Even if the mandate for greater OT security comes from the top down, there can be a hundred credible reasons, or excuses, not to adopt new cybersecurity measures," said a subject-matter expert. "Focus on the three or four things that make the site manager's job easier and then build credibility so you can build out security more broadly. You can spend a lot of money up front, but you need frontline support to maintain security over the long haul."

  A security executive noted that change management is culturally dependent; the context of the shop floor or the way operations are run must be taken into account. He suggested, "Try to build the OT cybersecurity program around things the field is already doing, such as equipment maintenance. Getting 'sticky' controls that fit into traditional operations is a critical component of successful risk management."

  Another security executive added, "The concerns are deeper down in the organization where they may have had an outage in the past and are reluctant to try anything new that they think might cause disruptions. You have to get buy-in from the middle layers of the organization who can resist change."

  "Be a partner, not a hindrance, to the business," said an executive. "We must be seen as an enabler of progress, greater efficiency and plant performance. Our goal is to manage risk, not to say no. Present options and define the risks in ways operations executives can understand. Talk about value, not technology, for example, how monitoring vendor performance can inform decisions about increasing vendor productivity."

- **Third-party collaboration**—Several executives noted that OT security will only truly succeed with collaboration across the entire supply chain. However, one security executive noted that a lack of trust between nations across global supply chains will make OT cybersecurity more difficult for the foreseeable future.

  Several subject-matter experts discussed the challenge—and importance—of information sharing among OT cybersecurity professionals. "Nobody wants to share what happens during a cyber breach because they're afraid of what will happen to the company's reputation," said one expert. "It's an unfortunate reality that we all live in, but we have to get better at collaboration to understand what 'good' looks like. There will be repercussions to sharing, but the more that we can learn from each other, the quicker we can respond to new threats."

- **Governance**—Who will pay for investments, decide where should they be made and held accountable for delivery? One executive suggested building a risk management security community within the enterprise to drive OT security defense. "Have the CIO, COO and CISO aligned and accountable for people, process and technology." Another executive added, "We should strive for unified IT and OT governance and leadership within the C-suite so that accountability and objectives are held at a high level.

  Is there a risk that objectives will be mandated from outside the enterprise? One global cybersecurity expert posed the question, "Who will drive innovation? Will it be governments, insurance companies and tool providers? I can assure you that a year from now Moody's will come out with cybersecurity ratings. Will that include OT and will it spearhead and facilitate change?"

- **Investment decisions**—While OT is still early in the maturity curve, investment conversations are shifting from "why" a few years ago, to "how," said an enterprise security leader. Several speakers

said that while security executives can't entirely eliminate risk, they should assess enterprise risk and help set OT security priorities through the lens of enterprise risk management.

Where to begin? One subject-matter expert said, "Start with the value you're trying to create and the specific problems you're trying to address."

"Keep in mind that the CEO needs to quantify risk," said a subject-matter expert. "Security executives should be prepared to clearly and simply explain investment proposals in terms of the financial and reputational risks you're trying to mitigate and the likelihood of an attack."

Another subject-matter expert added, ""If you only invest in cybersecurity, the motivation typically is fear. A better approach is to explain how investing in cybersecurity will not only reduce risks, but contribute real value to business operations and drive better key performance indicators (KPIs)."

Another security expert said, "We have to explain that this isn't simply an IT or an OT issue; it's a matter of health and safety, customer service and enterprise resiliency."

- **Visibility into risk**—OT executives are challenged to protect a complex technology stack—from the plant floor and the edge of enterprise—and to protect both older environments and greenfield operations. One security leader said, "We need to understand the assets and processes we're protecting. Context is critical to understanding the controls we really need." A subject-matter expert added, "You can't protect what you can't see. Anomaly detection can help you see bad when it happens and then take action to stop it."

  One subject-matter expert cited a recent Gartner report that said less than 10% of Gartner's OT customer base has implemented any visibility into the OT threatscape. "Visibility is a number one priority because we don't really know the journey we're on until we know what to protect, what skills we'll need and the intentions of the bad actors."

- **Elevating awareness**—One OT subject-matter expert admitted that, "We often get lost in the conversation. Senior management knows they need to be more conversant in OT cybersecurity but we, as security executives, have to be better at communicating what it really all means in simple terms so the right decisions can be made about priorities and investments."

  Another expert added, "Many boards still don't understand the risks. We need to get better at explaining things in operational and financial terms, informing the board and management of the business consequences and various risk management options."

  A board member added that it is not the board's responsibility to be deeply knowledgeable about OT or cybersecurity risk. It is the CISO's or some other executive's responsibility to translate those risks in terms of scale and scope, financial and operational impact and competitive positioning.

  Summit participants shared a variety of ideas for getting the C-suite and board members aligned on OT risks and challenges. "We should project hope, not promote fear," said one executive. "Discuss investments not just in terms of cybersecurity risks but more broadly in terms of compliance reporting, improving operational efficiencies, reliability and customer satisfaction." Another executive added, "Senior management and the board put all risks under one umbrella. OT discussions should be in the context of detecting, reacting to and measuring the impact of all types of threats."

One executive recommended attack simulations and purple teams tests. Another suggested using smaller incidents inside the enterprise as a way of illustrating the potential impact of more serious attacks.

Opinions were mixed about the idea of taking senior executives and board members on site tours. Some summit participants thought it could be an effective means of bringing greater understanding about an attack's impact on company performance. Others expressed concerns that site visits would cause disruption and anxiety within the plants.

Technology priorities

Several subject-matter experts discussed the potential of technology in helping enterprises manage risk. There was consensus that, as one executive said, "We must think about people, process and technology and technology is the last thing I would be thinking about. An integrated approach is essential." An OT security luminary added, "The least productive investments we are seeing are where tools and processes are not working hand in hand, where the right people aren't in place and the use cases aren't buttoned down."

Among their other insights we heard:

- "There's no AI in the world that will make magic happen. There's a time and place for technology, but for us to think that one more tool will solve the problem is just wrong."
- "We need to use the tools we already have better before we start adding new ones."
- "Network anomaly detection and asset inventory tools on their own are not only valuable and can drive business outcomes, but also they are an important element of multiple other initiatives like Zero Trust, configuration management and secure remote vendor access."
- "Physical separation used to be a key component of OT security but with digital transformation that's insufficient. Because IT and OT networks are now interconnected, cybersecurity must be integrated too."
- "Avoid window-shopping for technology. Try to avoid the OPEX and complexity of point solutions that we originally saw with IT cybersecurity. Move toward a platform approach."

Conclusion

Every company is on a journey to protect its critical infrastructure and everyone is in a different place in terms of OT security maturity. A strong IT security foundation is an important advantage, but regardless, many enterprises find that they have to implement OT security better and faster than they did IT security in the past. That means not waiting until an attack. For many enterprises the first step will be a small project to improve visibility into OT vulnerabilities so that the CISO better understands the road ahead.

Progress will be made when enterprises focus on integrated, outcomes-based approaches and clear measures of success. Metrics that translate cybersecurity risks into better financial performance, greater health, safety and efficiency and increased reputational value will drive adoption from the board room to the shop floor.

Finally, I agree with my colleagues who said that collaboration makes us better together. Sharing information among peer CISOs, for example, is a much faster means of knowledge transfer than taking a CEO or board members on a tour of their own facilities.

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

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, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 537,000 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 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.