MAPI

RESEARCH
REPORT

Securing Critical Operational Technology in Manufacturing

Managing Cyber Risk, Readiness, and Resilience

PARTNER FORTINET®

Table of Contents

Executive Summary

As digital transformation continues to bring dramatic change to industry systems and technology, the Manufacturers Alliance for Productivity and Innovation (MAPI), in partnership with Fortinet, surveyed leaders in operational technology (OT) security at large manufacturers[1] to understand practices to protect critical infrastructure.

The study focused on sizing OT cybersecurity risk, assessing incidents and response readiness, and reducing risks by understanding how to build resilience amid IT/OT convergence. Key findings include:

1. **A TOP-FIVE BUSINESS RISK**
   OT cybersecurity is seeing leadership and engagement spanning from the C-suite to the production environment. Although more than 80% of respondents expect their budgets to secure OT infrastructure to increase in the next 12 months, only 27% say the expected increase is significant.

2. **REAL AND PRESENT DANGER**
   Three in five manufacturers experienced actual breaches with unauthorized access to data in the past 12 months. Of those incidents, 42% resulted in operational outages with lost productivity.

3. **"ABOVE AVERAGE" CONFIDENCE**
   While leaders believe IT/OT convergence is critical to competitiveness, self-assessments reveal likely blind spots to complex threats.

4. **ALL-IN ON PREVENTION (ALMOST)**
   73% performed a cyber-risk audit and/or assessment of OT cybersecurity in the past 12 months. Three in five rate incidence response planning as extremely important; and two-thirds will be improving Supervisory Control and Data Acquisition or Industrial Control Systems (SCADA or ICS) security in the next year by focusing efforts on prevention/protection.

5. **UNEVEN APPROACHES TO EVERGREEN CHALLENGES**
   Despite consensus on attack surface expansion and shared management challenges responding to these attacks, there remains high variability in company security practices and capabilities, including activities for monitoring and reporting.

Introduction: An Advancing Threat

High-impact. High-likelihood. Disruption to operations and critical infrastructure from cyberattack ranks among the top five global risks, according to the World Economic Forum.[2] Today, global industrial manufacturers experience the risk daily, operating with some of the most complex networks across sectors.

With the acceleration of the Industrial Internet of Things (IIoT) and the Industry 4.0 revolution, widespread integration of new technologies into legacy systems are generating new challenges alongside breakthrough efficiencies and value creation. As information technology (IT) and operational technology (OT) converge in manufacturing – diminishing the boundary or the gap that once had separated both technologies and teams from talking with one another – increased connectivity is expanding the threat landscape.[3] Digital transformation introduces vulnerabilities when internal systems connect to outside the factory walls with assets not designed for on-site or remote data connectivity. Wireless transfer, third-party access, and supply chain are expanding the attack surface exponentially.[4]

The costs of cyber risk in the IT space are significant: it can take manufacturers months to identify and contain a data breach and millions to the average manufacturer annually.[5] IT-related attacks are increasingly affecting OT systems with costly consequences, too.[6]

However, cybersecurity for OT requires a very different approach than that for IT.[7] Priorities differ. Professionals tasked to protect company infrastructure and the production environment face a daunting, non-negotiable imperative to secure equipment, networks, and safety where the stakes are high.

Manufacturing leaders are ramping up, upgrading, and increasingly proceeding with confidence. Process management improvements are strengthening security through visibility, control, and continuous monitoring.[8] IT/OT convergence may be the root of today's security challenge, but it's also the foundation for a durable solution in enabling delivery of accurate, actionable information.

To support the manufacturing community in assessing and addressing security risks in the OT environment, MAPI partnered with Fortinet on this research initiative. We conducted an online survey of manufacturing leaders who have supervisory responsibilities in OT security at large multinational companies: the most common senior respondents include IT heads of OT operations, Chief Information Officers (CIOs), Chief Technology Officers (CTOs), Chief Operations Officers (COOs), and Chief Information Security Officers (CISOs), among others.

This report features data insights and perspective to

1. Size up OT security risk
2. Assess industry incidents and response readiness
3. Reduce risk by building greater IT/OT resilience

Note on Definitions[9]

For purposes of the research, the term operational technology (OT) includes Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), machine automation, Programmable Logic Controllers (PLC), and Distributed Control Systems (DCS).

The convergence of information technology (IT) and OT ("IT/OT Convergence") refers to the trend toward integration of the IT systems used for data-centric computing with the operational technology systems used to monitor and make adjustments to events, processes, and physical devices in industrial operations.

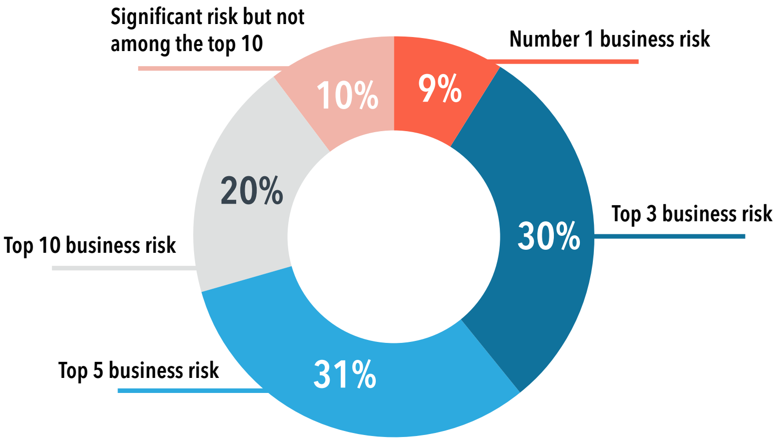
Sizing up Security Risk to OT

A Top-5 Risk with Revenue Implications

In a parallel to the World Economic Forum risk landscape assessment overall, a majority (70%) of manufacturing leaders surveyed indicate that OT cybersecurity is at least a top-5 business risk to their company.

Moreover, leaders who self-assess as above average or best-in-class in their readiness to manage OT security risks, rated the business risk higher. This suggests a strong relationship between risk prioritization and self-assessment of risk readiness. (See the "Confidence in Readiness" section for more.)

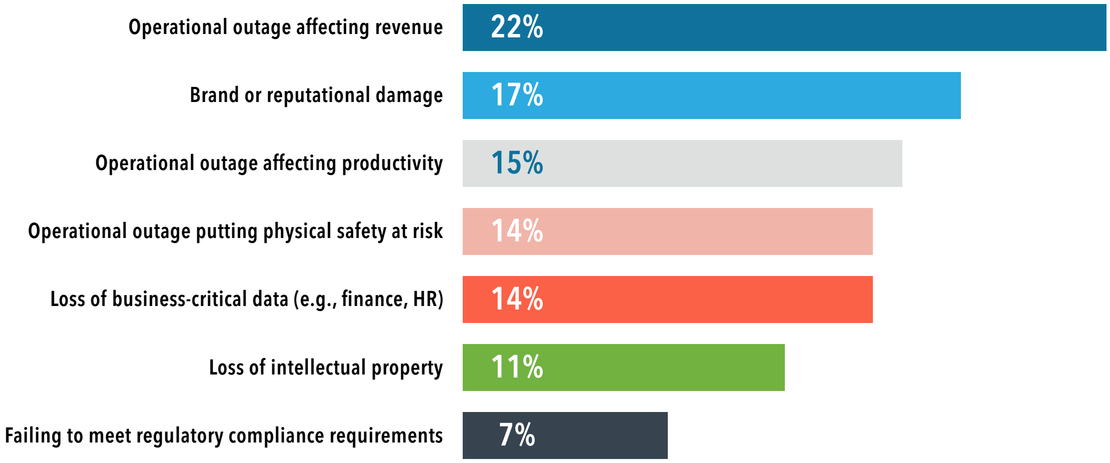
From a business perspective, how do OT cybersecurity risks compare to other business risks for your company? (n=149)



> "We are an old-school, traditional manufacturing company and don't have a lot of technology. It's not been on the network, but that is changing, especially over the last couple years and with where we're looking to go. Everyone agrees that one of the biggest risks is going to be any type of connectivity related to our manufacturing process."
>
> *– Information Security Lead*

At first glance, manufacturing leaders are split on what constitutes the single-greatest concern in securing the OT environment. However, these concerns are interrelated and difficult to tease apart. Overall, financial stability is the common denominator: taken together, operational outages that affect revenue and productivity narrowly edge out concern for reputation and safety.

In general, what is your company most concerned about when securing its OT environment? (n=149)



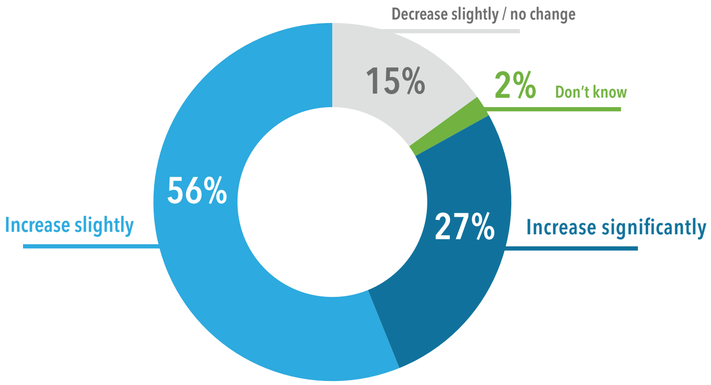
> "We've had incidents that required us to shut systems down, which directly impacted products that we needed to deliver and be able to produce. Then there were also safety issues that happened because of control of devices that were on the shop floor."
>
> *– VP, Technology Operations*

Budget for OT Security Expanding

Budget expectations appear to be rising along with the perception of business risk and concern for impact, which reflects an improvement in the past five years, according to MAPI research.[10]

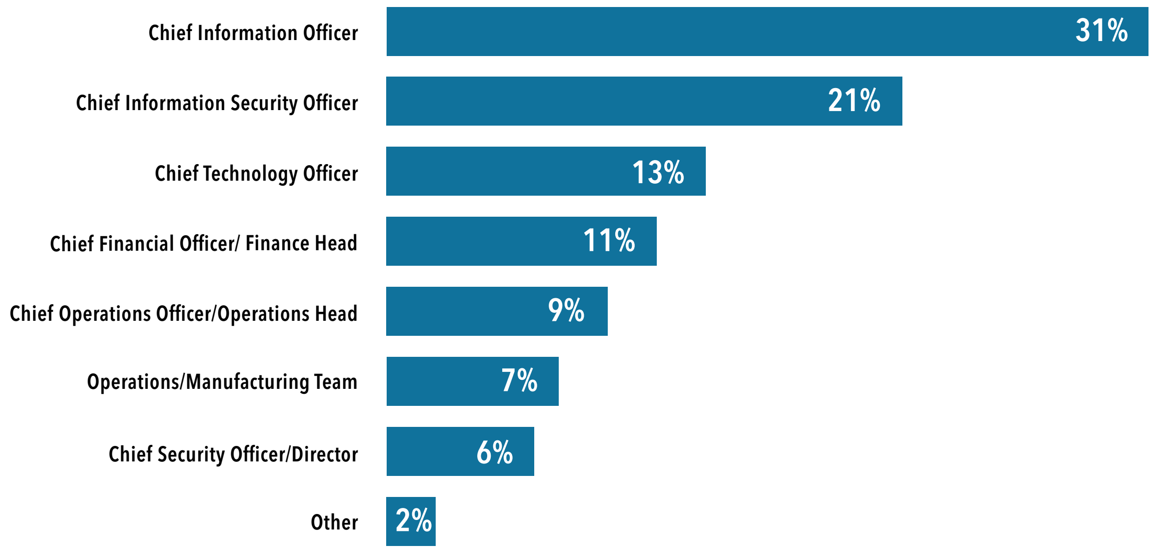
More than 80% of manufacturing leaders expect that their company's budget for OT security will increase in the next fiscal year, projecting confidence in enterprise resourcing to rise with the risk challenge. However, the fact that only 27% expect a "significant increase" signals that this resourcing may not be sufficient.

How do you expect your company's budget allocated to securing OT infrastructure will change in the next fiscal year? (n=150)



Despite relative uniformity in budget expectations, the primary budget "owner" is highly variable across responding companies. CIOs are considered primary owners over budget for OT infrastructure in a plurality of companies surveyed (31%), but there is a significantly longer tail of other C-suite owners, as well as more localized operations and manufacturing teams. Reporting remains far from uniform – or settled.

Who is the primary "owner" of company budget allocated to securing OT infrastructure today? (n=150)



Extensive Management Challenges

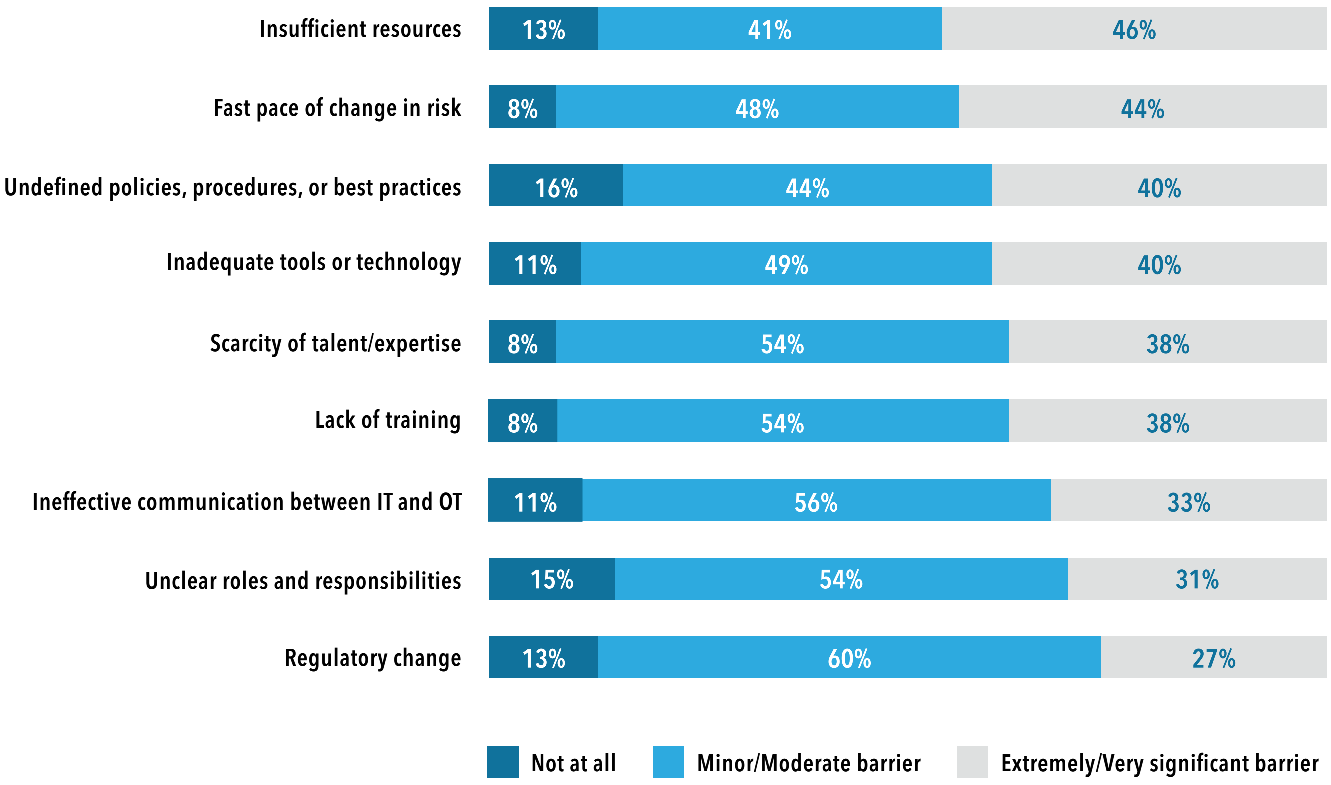
OT security budget owners may be in flux with many "cooks in the kitchen," as one industry executive shared with us, but respondents report strikingly consistent barriers to effective OT cybersecurity initiatives. Consistent with recent related research, barriers span people, processes, and external factors (i.e., change in risk and regulation).[11]

Concern with the fast pace of change underscores the evolving nature of OT risks. Executive interviews also highlight the entrenched challenges in the scarcity of talent and expertise, particularly for IT/OT collaboration. Whereas IT professionals may have more cybersecurity specialization and training today, OT professionals more commonly ramp up and add these responsibilities to their day jobs.

"One of our biggest challenges is people and time. We don't have the skills and we don't have the time to learn the skills. It would be nice to have resources to bring on more people, especially someone more experienced in manufacturing security."

– Information Security Lead

To what extent were each of the following a *barrier* to effective response management for cybersecurity incidents in your company's OT environment in the past 12 months? (n=149)



Within this set of management challenges, opportunity areas include available solutions for unclear roles/responsibilities given ample training offerings and roles defined by leadership. By comparison, scarcity of talent and experience is more difficult and complex in light of available talent pools.

However, manufacturers do not face challenges in isolation. Across sectors, thought leaders, third-party providers, public-private partnerships, and federal sources – including the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology (NIST) ICS-CERT – comprise part of the ecosystem supporting manufacturers with information and resources to address OT cybersecurity.[12]

Operational Technology Security Alliance (OTSCA)[13]

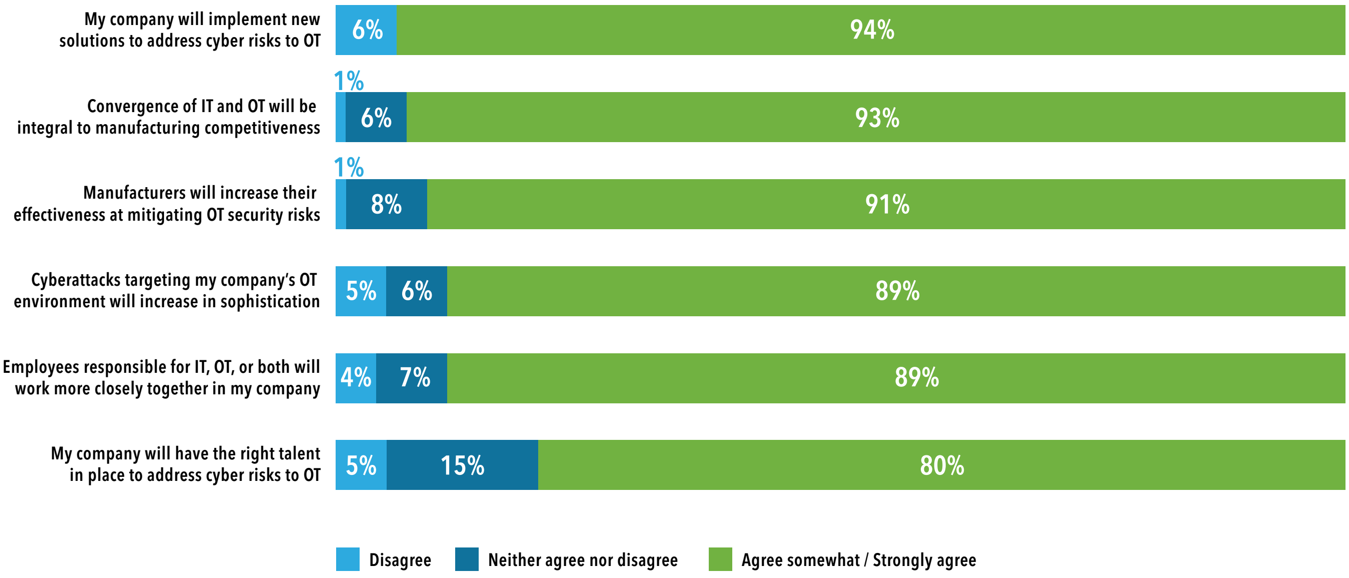
The launch of the industry organization OTSCA is one recent initiative for overcoming common barriers by "helping to strengthen cyber-physical risk posture in OT environments and for interfaces enabling OT/IT interconnectivity.[14] Its mission includes:

- Guide OT operators on how to protect their OT infrastructure based on a risk management process and reference architectures/designs which are demonstrably compliant with regulations and international standards, such as IEC 62443, NERC CIP, and NIST 800-53.
- Guide OT suppliers on secure OT system architectures, relevant interfaces, and security functionalities.
- Support the procurement, development, installation, operation, maintenance, and implementation of a safer, more secure critical infrastructure.
- Accelerate the time to adoption of safer, more secure critical infrastructures.

Outlook Positive

As manufacturing leaders overcome barriers to effective response management, outlooks are favorable for the medium-term. IT/OT convergence will be integral to manufacturing competitiveness and manufacturers will meet increasingly sophisticated OT cyber risks with new solutions and IT and OT collaboration, according to the respondents. Securing the talent required to address cyber risks still remains the least rosy among a set of propositions for a three-year time horizon.

To what extent do you agree or disagree with the following statements about how OT security will change during the next 3 years? (n=149)

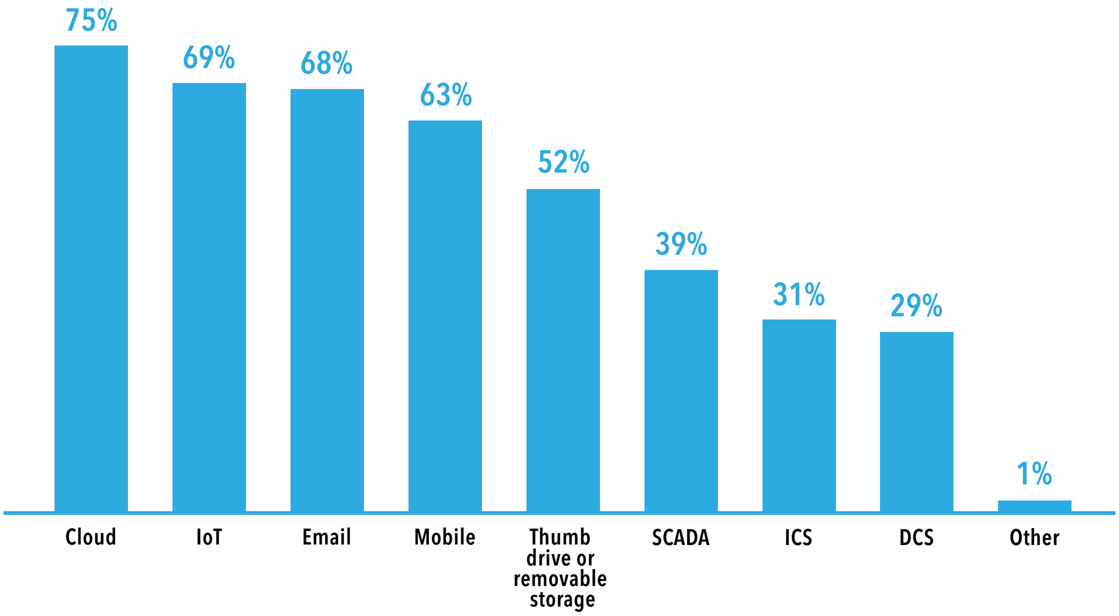


Assessing Security Incidents and Readiness

Consensus on Exposures

As IT/OT converge and the attack surface expands, cloud, IoT, email, mobile devices, and thumb drives rank highest among OT exposures to cyber risk recognized as falling outside of the firewall. Far from immune to attack, SCADA, ICS, and DCS might simply be less associated with the beyond-firewall attack surface. Another study finds that across industries 56% of SCADA or ICS operators reported a breach in the past year.[15]

What areas does your company consider to be part of its OT exposure to cyber risk outside of the firewall (i.e., part of the cyber-attack surface)? (n=150)

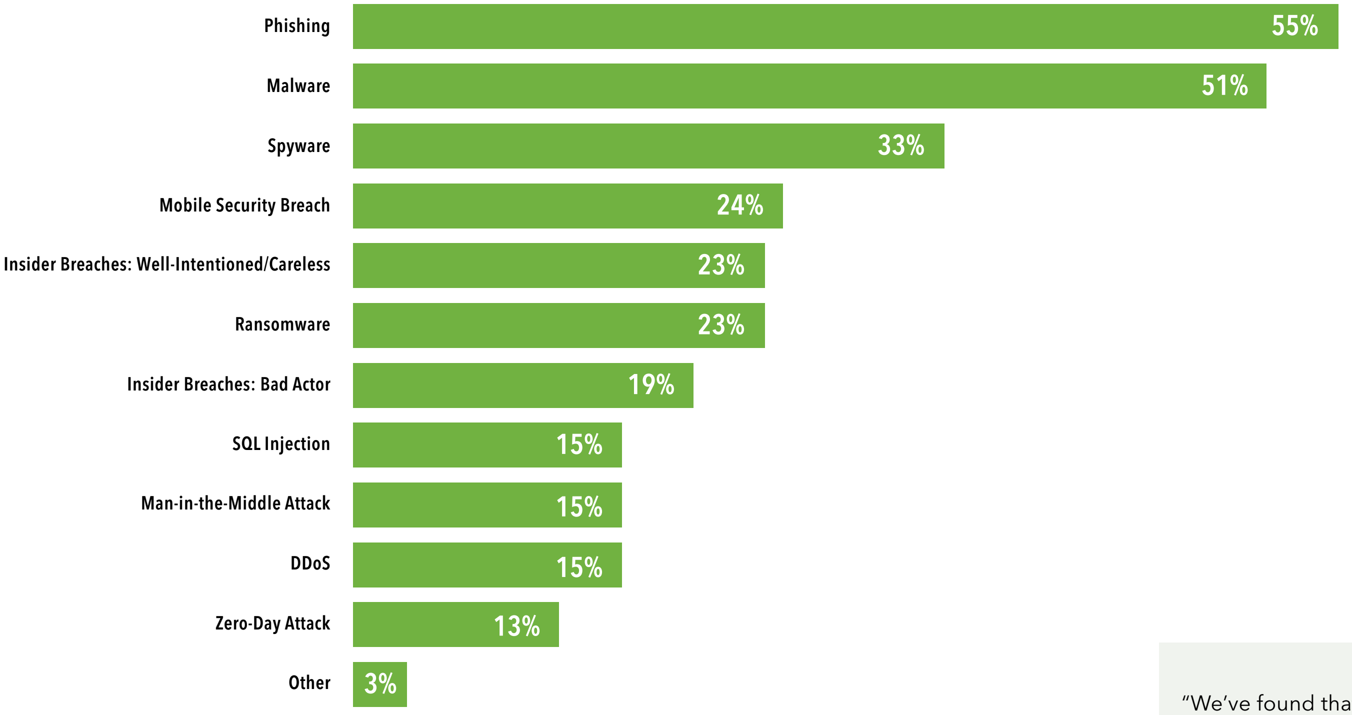


Although there are increasing emerging threats in cloud and IoT, the predominant attacks still begin with email. The biggest impact for security is found in focusing on email and phishing, as email is the largest vector for attack.

Breaches not Uncommon

Phishing incidents are occurring at over half of responding companies, and anecdotally this figure may be underreported. Verizon research similarly identifies privilege misuse from external and insider threats as "the top threat vector for manufacturers, with most cases following a successful phishing attack." Manufacturers are duped by around 3% of phishing emails that make it into their inboxes.[16] Such IT-based attacks are increasingly affecting OT systems, as threat actors "recycle" malware for IT.[17] Ransomware remains common too.[18]

Overall, what type(s) of cybersecurity incidents did your company's OT environment experience in the past 12 months? (n=150)

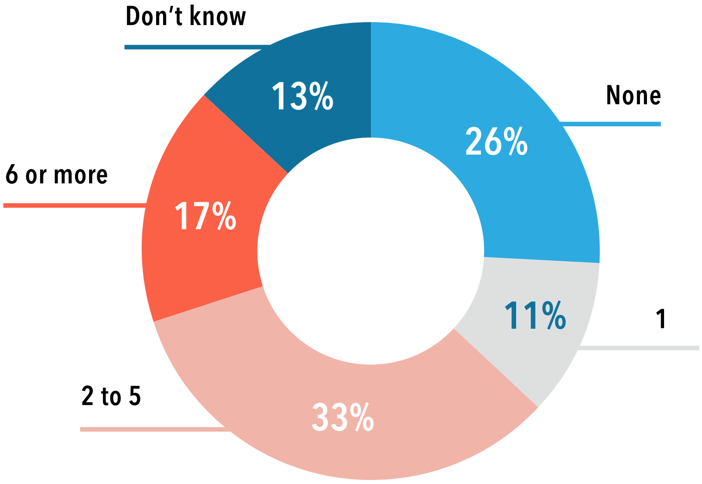


Phishing and malware are not new methods of attack but they are becoming more sophisticated. Both are delivered through email and represent the persistent use of legacy techniques.

Beyond the total number of incidents, a majority of responding companies faced at least one breach in the past 12 months, which is distinguished as a specific security incident that resulted in unauthorized access to data. This is an escalation over MAPI findings from 2016.[19] The finding is alarming but also consistent with other recent research corroborating that the rates of data breaches are rising, with half of companies reported being a victim of at least one data breach during the past year.[20]

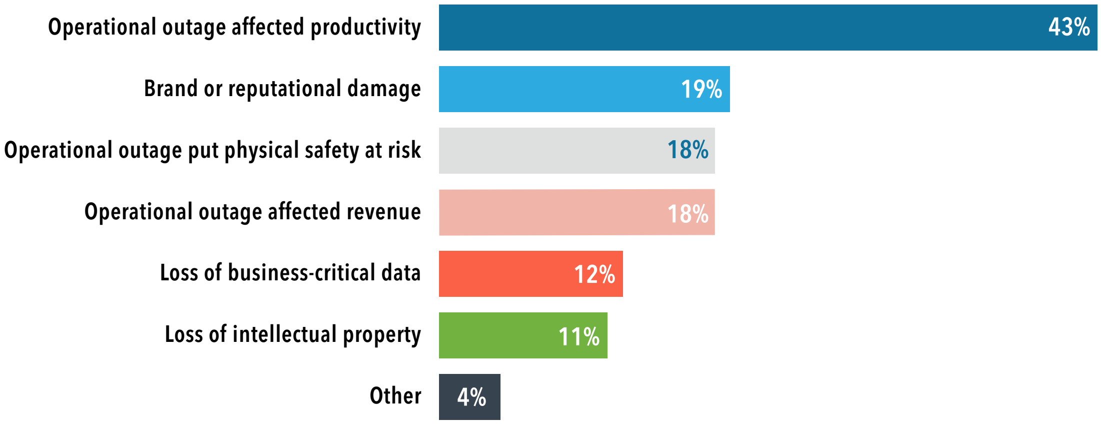
> "We've found that it's still the old kind of legacy threats – phishing, malware – that are that are the most common sources of incidents. Despite the education trainings for employees, they seem to still be the source of so many of these breaches."
>
> *– VP, Operational Technology*

How many data breaches did your organization experience in the OT environment in the past 12 months? A breach is a specific security incident that resulted in unauthorized access to data. (n=150)



Even more concerning, companies that faced a breach most commonly report operational outages affecting productivity. A large subset saw direct revenue impact. Harm to safety and hits to reputation are unacceptably high. Although operational outages affecting productivity are out front, the overall profile of the actual impact from breaches looks similar to respondent concerns in securing the OT environment in the first place. Productivity is often first causality in breaches because a shutdown is required to determine its impact.[21]

What impact did the OT security breach(es) have on your company? (n=150)

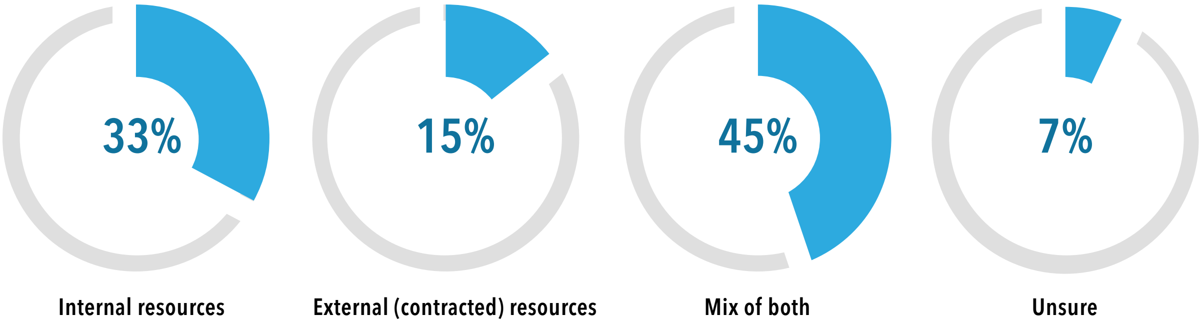


Effective Detection and Response

To detect cybersecurity incidents in the OT environment, nearly half of companies use a mix of internal and external capabilities. A plurality of companies rely on both internal and external resources in their response as well—only 15% have outsourced responding to security breaches.

Given the pace of total security incidents and breaches, it is reassuring that manufacturing leaders are confident in capabilities and their effectiveness at responding to OT security breaches.

How did your company respond to the OT security breach(es)? (n=109)



Overall, how would you rate the effectiveness of your company's response to the OT security breach(es)? (n=108)

Exceptional	Very Good	Good	Fair	Poor
20%	42%	31%	6%	1%

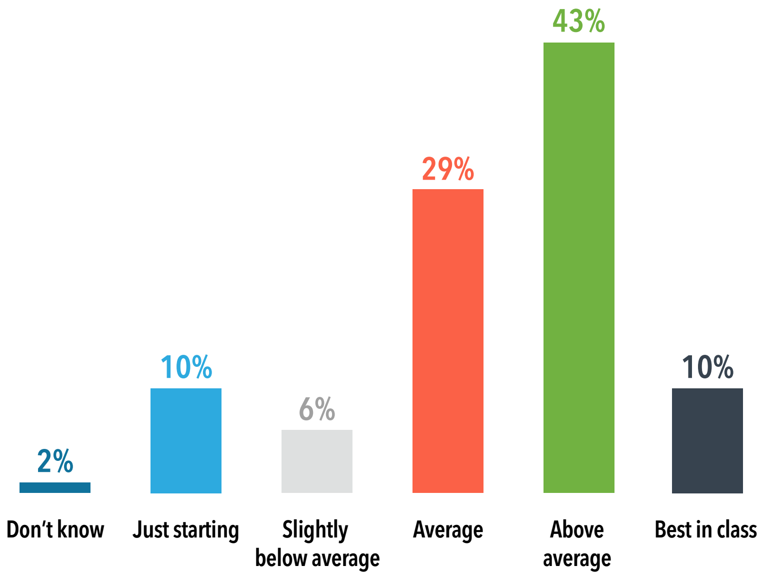
Positive self-assessment on response may reflect organizational resilience in the face of breaches. Effectiveness of response should be measured by the ability to neutralize the event without causing operational downtime, which includes both the process and outcome together.

Confidence in Readiness at Lake Wobegon

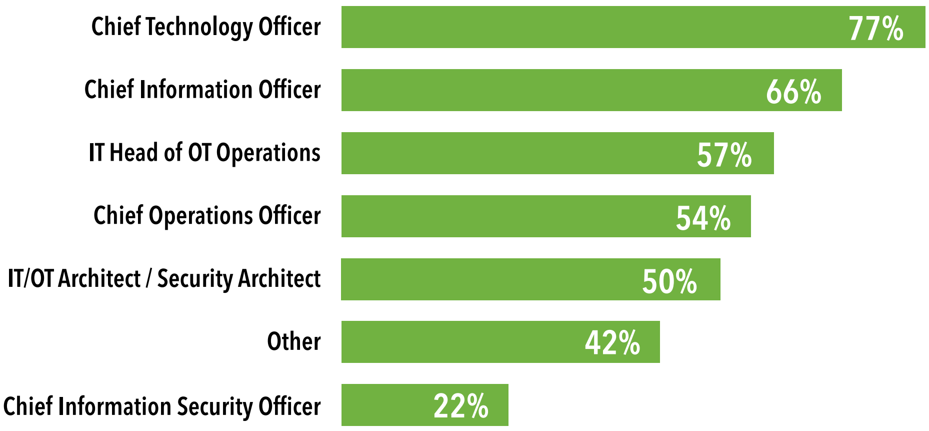
Garrison Keeler wrote of a town where “all the children are above average.” Similarly, more than half of leaders self-assess their company’s readiness to manage OT security risks as above average or best-in-class. Confidence in security maturity relative to peers is highest among the cohort of CTOs and CIOs. By comparison, CISOs are least likely to self-assess in the top echelon.

> “We’re kind of our own worst enemy at times. So much effort goes into doing the things to keep us safe. Because we haven’t had any breach in a in a few years, it’s not taken as seriously. I’d like to find that middle ground.”
>
> *– OT Security Manager*

Overall, how would you rate your company’s level of readiness to manage OT security risks today in comparison to your peers in the industry? (n=150)



Respondent Job Title/Category “Above average” or “Best in class” (n=80)

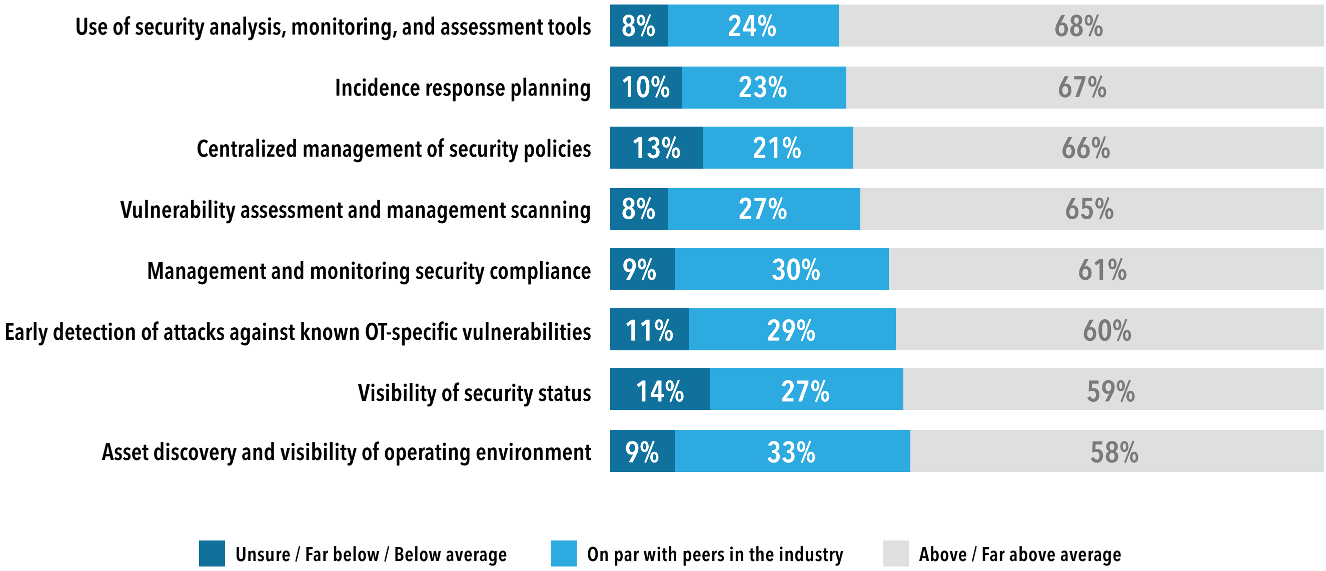


Executive Confidence May Belie Blind Spots

Confidence in readiness relative to peers aligns with high self-assessment on execution of activities to secure the OT environment. These span critical, leading practices including centralized policies, visibility, tools, assessments, early detection, and incidence response planning. In reality, how many companies can truly be above average in the face of such costly breaches?

Are there blind spots?

Overall, how would you assess your company's effectiveness in executing on the following activities to secure its OT environment? (n=150)



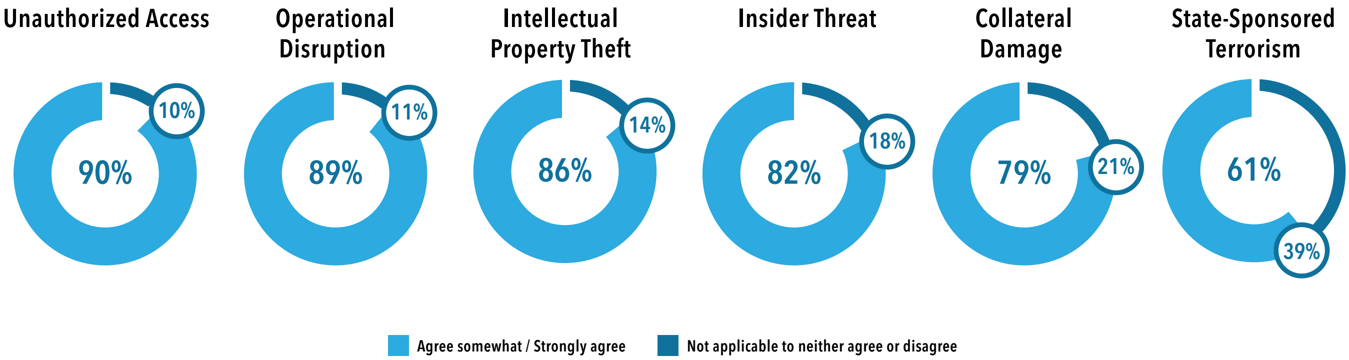
Alternatively, there may be reason for confidence. Given relatively low talent mobility within manufacturing, leaders are witnessing first-hand the advances in protection of OT environments in the industry. Companies are stepping up OT cybersecurity with investment in this area, which translates to leaders more confident in their ability to protect critical infrastructure.

Reducing Risk to an Expanding Attack Surface

Efforts Focus on Prevention

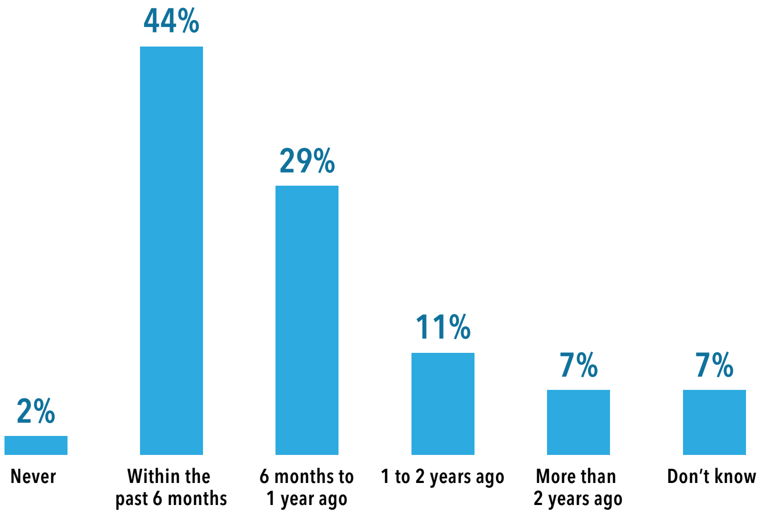
As threats multiply and expand, manufacturing leaders are doubling-down on a proactive posture to reduce OT risks, foremost among them unauthorized access, operational disruption, and intellectual property theft.

To what extent do you agree or disagree your company is *taking action proactively* to reduce the following risks to the OT environment? (n=150)



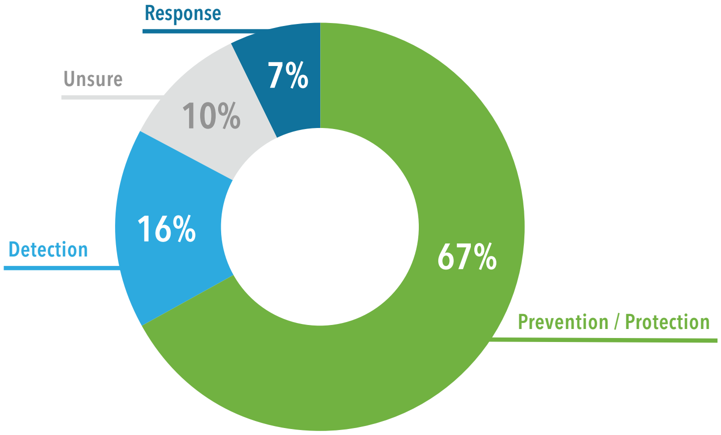
As part of proactive action, nearly three-quarters report performing a cyber-risk audit or assessment related to OT cybersecurity. This again reflects something of a split in those who self-assess as above average or best in class versus all other respondents (84% incidence versus 60%). MAPI's finding is similar to another recent study in which 69% of security professionals polled worldwide audited their OT/control systems or networks in the past year.[22]

How recently has your company performed a cyber risk audit and/or assessment related to OT cybersecurity? (n=150)



Looking further out, companies are continuing to focus efforts primarily on prevention/protection over the next 12 months for SCADA/ICS security, as compared to detection and response.

In what areas will your company focus efforts on improving SCADA/ICS security in the next 12 months? (n=150)



Given the frequency of breaches, prevention should be considered first, but all areas are important. As breaches occur, it is key is to be proactive to detect and neutralize them versus having to turn out the lights due to significant attack. Responding to the breach demands equal attention.

Preventive Measures Paramount

Manufacturing leaders place high importance on each of the preventive measures on which they self-assess favorably, suggesting little daylight when it comes to attitudes on importance and effectiveness.

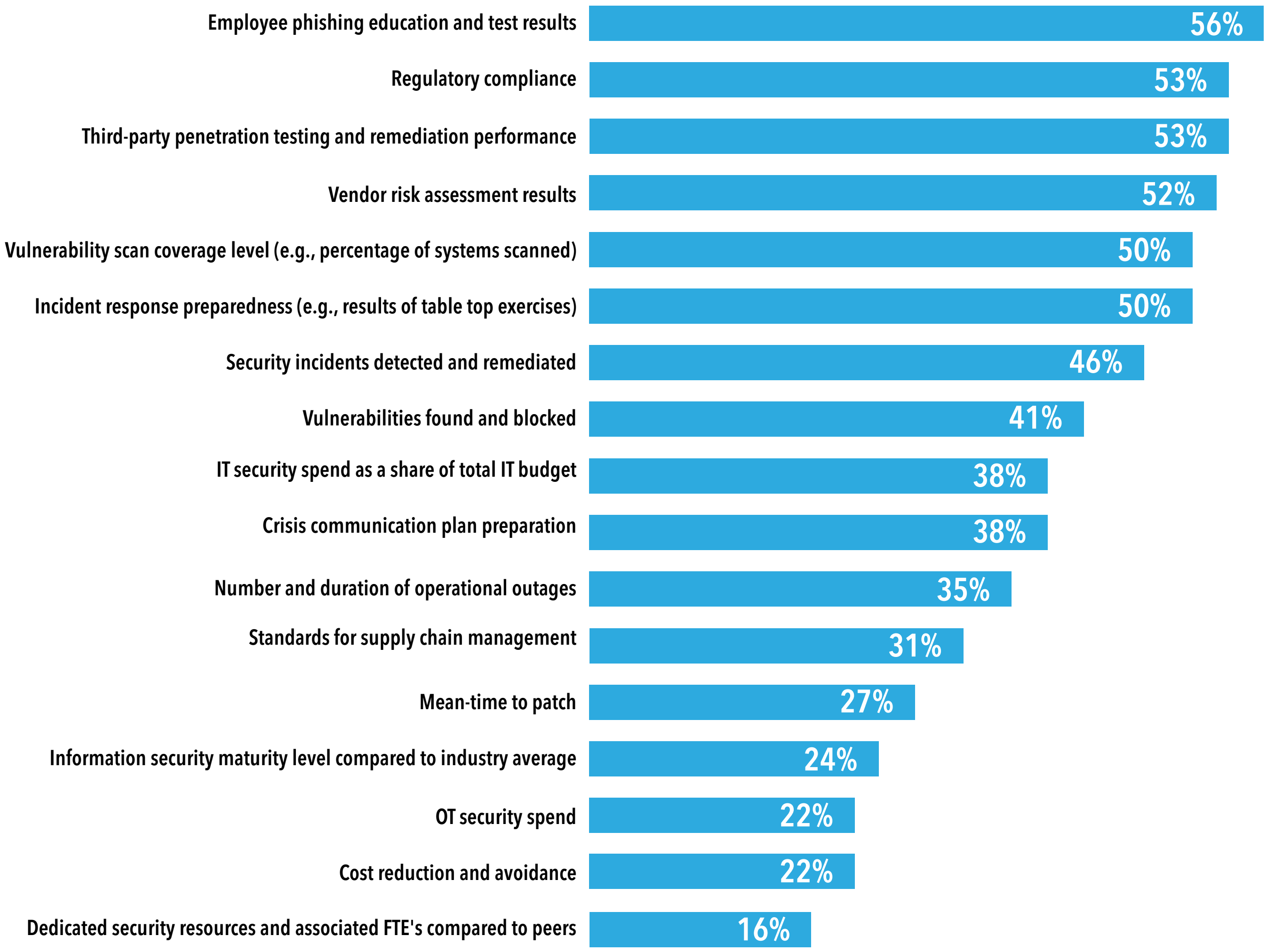
Overall, how important are each of the following activities to securing the OT environment in your company? (n=150)

Activities	Extremely Important	Very Important	Somewhat / Slightly Important	Not at All / Don't Know
Incidence response planning	61%	31%	8%	1%
Early detection of attacks against known OT-specific vulnerabilities	52%	42%	4%	1%
Vulnerability assessment and management scanning	52%	39%	9%	1%
Visibility of security status	49%	38%	12%	1%
Management and monitoring security compliance	47%	43%	9%	0%
Use of security analysis, monitoring, and assessment tools	45%	47%	6%	2%
Asset discovery and visibility of operating environment	45%	42%	12%	1%
Centralized management of security policies	42%	41%	16%	0%

Variability in Tracking

Despite such positive ratings of importance and effectiveness on critical activities, behaviors tell a story with more variable activity levels across industry. For instance, monitoring of employee phishing education appears low (56%), as do security incidents detected and remediated (46%), to call out two.

Which of the following measures and activities does your company track to manage OT cybersecurity? (n=150)



Broad training across an organization is critical because phishing remains the largest vulnerability internally (i.e., malware clicking on bad links, stolen passwords from all levels of employees). The human element is unpredictable. While it is great that training is the top activity listed, the low incidence (only about 50%) is still concerning. Training isn't a one-and-done activity either, but requires a refresh on a regular basis. It only takes one breach to create a bad outcome for a company.

Variable Capabilities

In contrast to the attitudes toward importance and effectiveness, behaviors in the form of capabilities in place at the company again suggest more modest activity and either underreporting or underuse of a critical set of available best practices.[23]

Which of the following cybersecurity capabilities or controls does your company have in place in the OT environment today? (n=150)

Cybersecurity Capabilities and Controls		
Internal security training and education	56%	✓
Scheduled security compliance reviews	51%	✓
Multifactor authentication	51%	✓
Remote management of physical security	47%	✓
Third-party security products	44%	✓
Internal network segmentation	42%	✓
Outsourced third-party security	41%	✓
Protection for cloud-based applications	39%	✓
Role-based access control	38%	✓
Encrypted SSH/TLS	33%	✓
SCADA/ICS security team	31%	✓
Physical audits of SCADA/ICS	31%	✓
"Walling off" of machine data processes	29%	✓
Hardened network	29%	✓
Elimination of proprietary protocols from network	16%	✓
Deception technology	13%	✓
Zero-day protection	9%	✓

In addition to training and education again, internal segmentation and role-based access tied to multi factor authentication are critical areas for prioritization, yet relatively few companies report these are in place.

Building IT/OT Resilience

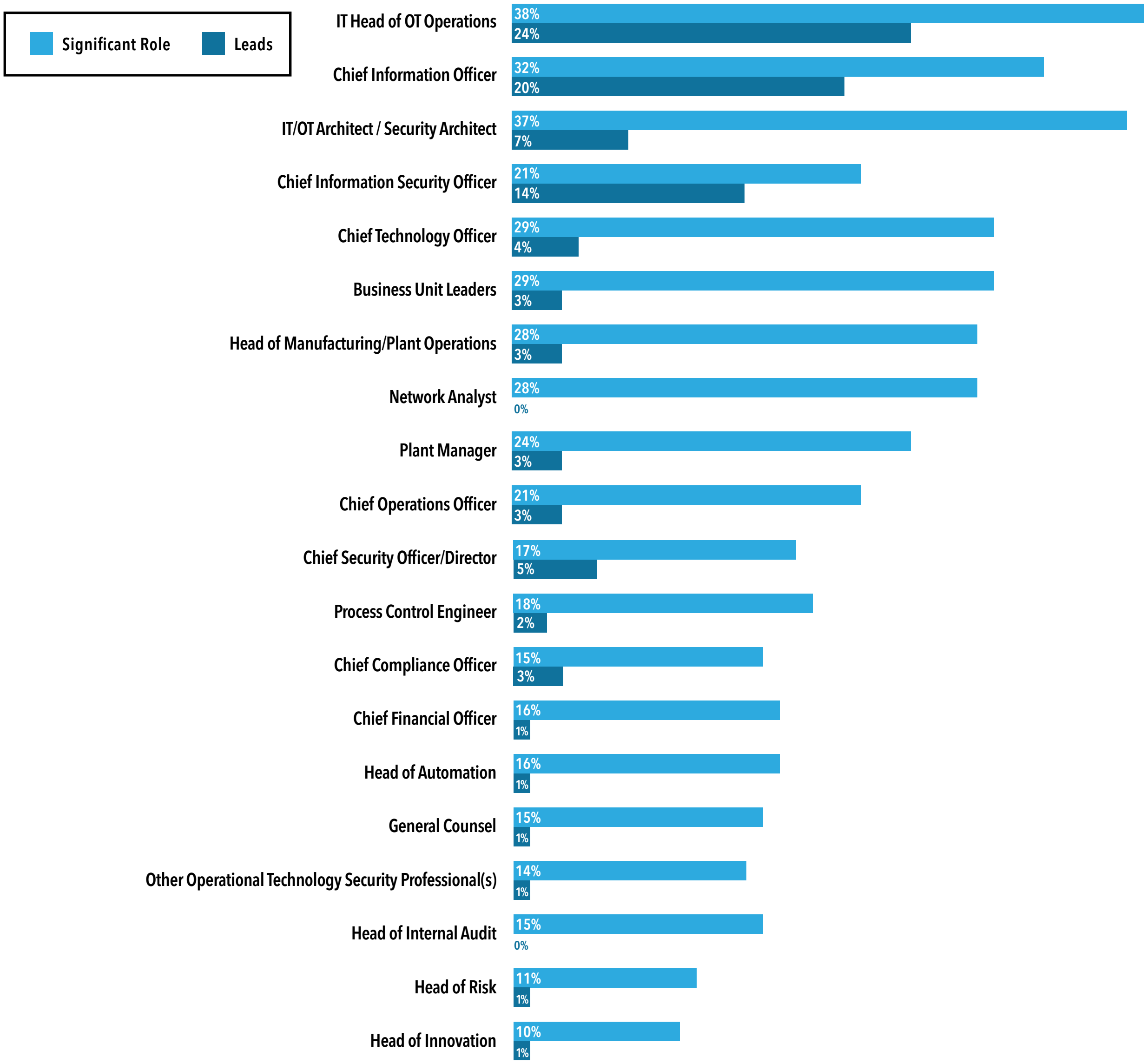
Many Hands in OT Security

The noise in data around activities and behaviors (versus attitudes) may in part reflect the complex web of leaders with significant roles in OT security. A long tail of leaders play a “significant role” while the true lead tends to fit the profile of an IT head of OT operations, CIO, or CISO, and others, too.

On the one hand, high organizational engagement can create strength. But complex reporting relationships can leave ownership unclear or reinforce silos with known cultural challenges for IT/OT collaboration. CISOs may be further down in the organization and navigating the matrix. “Speaking the same language” is foundational to practices for a more resilient future that starts with technology and teams all talking.[24]

> “If you have people involved across the spectrum, then there’s no one owner. Then it gets a little more complicated to control because it’s harder to have consistent policies.”
>
> *– SVP, Manufacturing*

Which of the following individuals play a significant role in managing OT security in your company? Who plays the *lead* role in managing OT security at your company? (n=150)



On the flip side, whereas historically a CIO may not have been included in the security responsibility/lead role for OT security, this data highlights that the CIO has a more significant role in security. This can be viewed as a positive development insofar as it means there may be movement toward single overseer. It is important for security to be given a more holistic view when developing a strategy – clear ownership of the IT and OT security plan. Broad involvement in OT security is likewise encouraging because it is in fact every employee's job to be thinking about company security. The many influencers playing a role in security strategy signals its importance to the business.

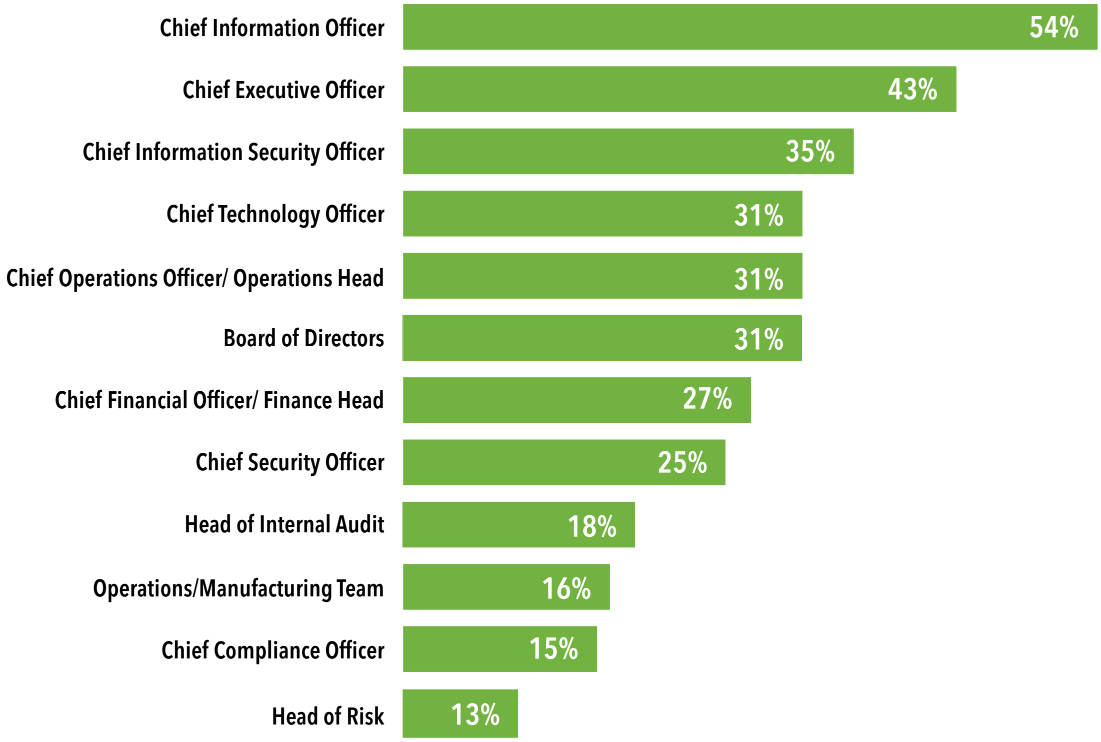
Variable Accountabilities

Compounding the communication challenges with leaders and significant roles is a larger governance question on consistent reporting of OT cybersecurity status. We find the buck stopping with CIOs often, but also with many others. Boards of directors are still less common, although respondents from the C-suite are more likely to report involvement than the group overall, suggesting a challenge with line of sight. Executive and board-level engagement requires careful coordination and help to translate cybersecurity risk into a source of competitive advantage.[25]

Moreover, there is a question about the frequency of response where updates to some parties may be more episodic than consistent. **Governance is integral to resilience in capturing lessons learned and driving investment in improvements.**

> "The OT space historically rolls up to somebody like a CTO or engineering, whereas you have the IT space which really rolls up to the CIO, normally. When you're looking at putting a holistic cybersecurity approach in place across the organization, there's quite a lot of partnership that's needed there – communication and understanding."
>
> *– VP, Technology Operations*

As far as communication protocols, to whom in the organization is OT cybersecurity status and compliance with security standards reported? (n=150)



Conclusion: Risk Beyond the Horizon

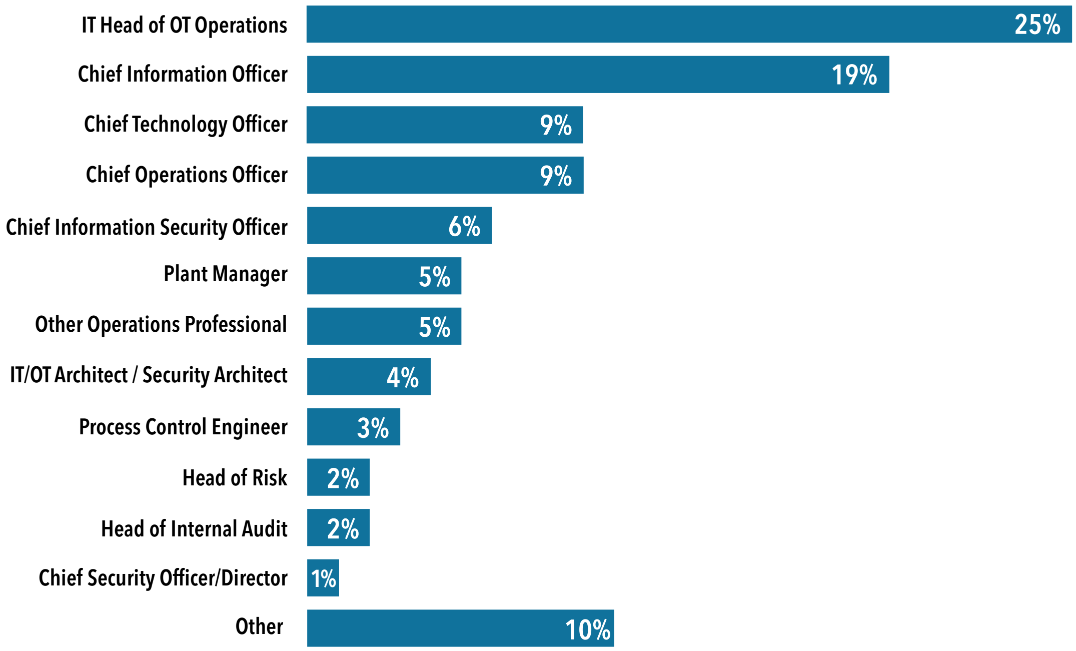
As the integration of new technologies into legacy systems enable efficiencies and value creation in the age of Industry 4.0, manufacturers are managing the cybersecurity implications for the new production environment. Significant direct costs may understate total costs in terms of operational and financial stability, safety and reputation, which are all at risk.

At the root of today's cybersecurity challenges, IT/OT convergence is also the solution. Technologies and network security stand to benefit from practices that promote greater visibility, control and continuous monitoring, as well as clearer roles and responsibilities, resourcing, and reporting for a culture of collaboration. Manufacturers are confident in readiness, but to stay ahead of the fast-changing threat landscape, leaders must continue to evolve, upgrade practices, and prioritize company resilience.

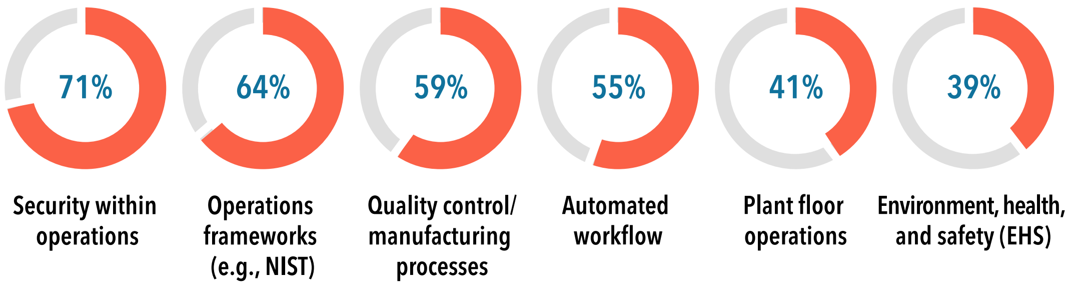
About the Research

Respondent Profile

Which of the following best describes your current role in your company? (n=150)

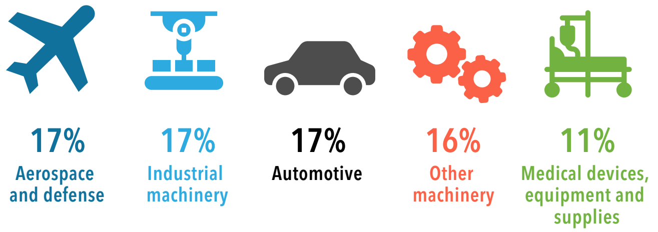


Which of the following management and supervisory activities in the operations/production environment fall within your responsibilities? (n=150)

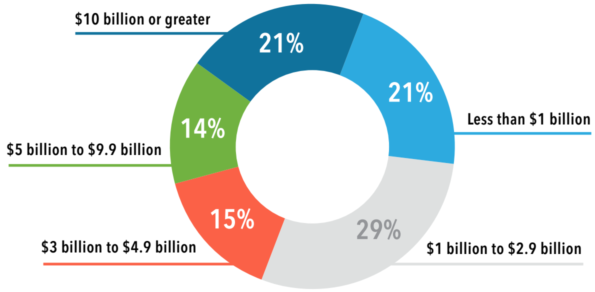


Large Industrial Multinationals

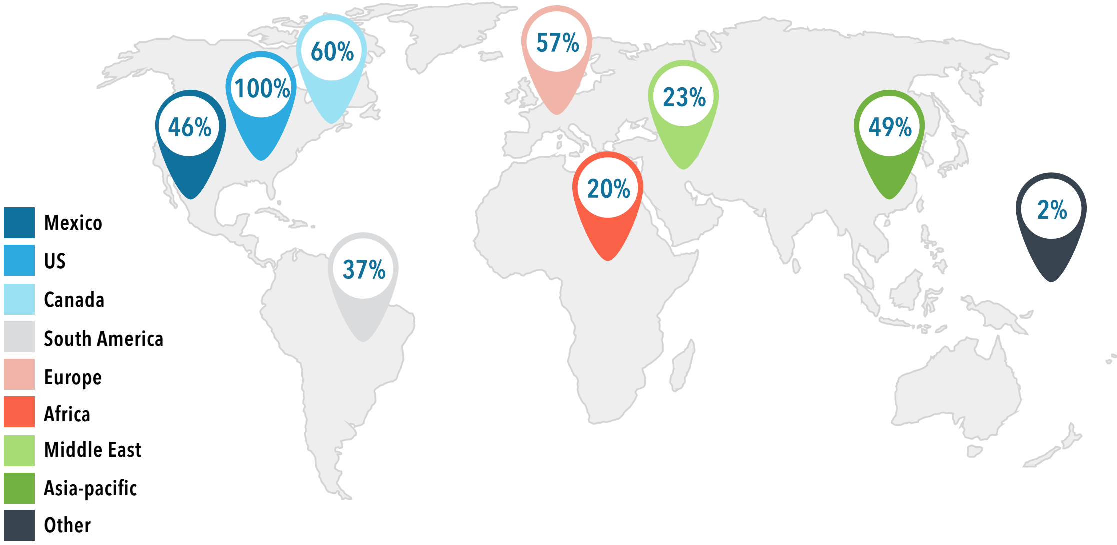
Top 5 industries in which respondents' companies derive most of their revenues. (n=150)



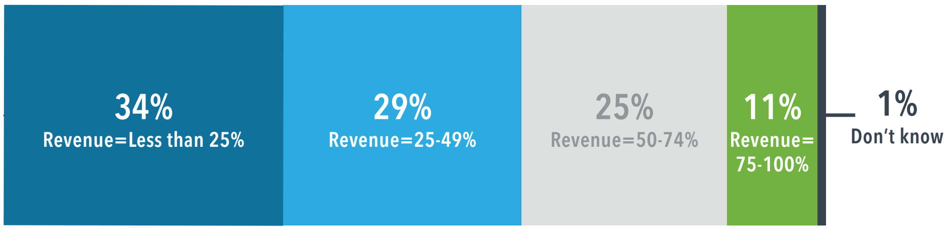
Please estimate your company's sales in the most recent fiscal year. (n=150)



Please indicate the areas in which your company operates currently. (n=150)



Approximately what share of your company's total revenue is generated outside of the United States? (n=150)



Sources

[1] Primarily companies with annual revenues above $1B.

[2] World Economic Forum. "The Global Risks Report 2019."

[3] Rick Peters. "A Cybersecurity Mountain to Climb: Getting IT and OT Tools to Talk to Each Other." *IndustryWeek*. Nov. 19, 2019.

[4] Warwick Ashford. "Operational Technology Security Improving, But Attack Surface Continues to Grow." ComputerWeekly.com. Jun. 12, 2019.

[5] Recorded Future. "Protecting the Manufacturing Industry with Threat Intelligence." Nov. 26, 2019; IBM "2018 Cost of Data Breach Study."; Accenture Security. "Ninth Annual Cost of Cybercrime Study."; Nozomi Networks ."Cost of OT Cybersecurity Incidents."

[6] Fortinet. "2019 Operational Technology Security Trends Report."

[7] GE. "An Executive Guide to Cyber Security for Operational Technology"; Keith B. Belton. "Barriers to Smart Manufacturing." Manufacturing Policy Initiative, Indiana University. Dec. 2018.; Stephen Gold. "Manufacturers are Behind in Industry 4.0 – and for Good Reason." *IndustryWeek*. Nov. 9, 2018.; Glenn Longley. "Security Considerations for the IIoT Challenge." *IndustryWeek*. Feb. 9, 2016.

[8] Fortinet. "What is Operational Security?"

[9] Ibid.

[10] MAPI. "Cyber Risk in Advanced Manufacturing." Nov. 15, 2016.

[11] Ponemon Institute. "Cybersecurity in Operational Technology: 7 Insights You Need to Know." Mar. 2019

[12] MForesight Alliance for Manufacturing Foresight and Computing Resource Association. "Cybersecurity for Manufacturers: Securing Digitized and Connected Factory." Sep. 2017

[13] OTCSA. "Introducing the Operational Technology Cyber Security Alliance."

[14] Peter Fretty. "Alliance Formed to Secure Operational Technology." *IndustryWeek*. Oct. 30, 2019.

[15] Fortinet. "Independent Study Pinpoints Significant SCADA/ICS Security Risks."

[16] Verizon. "2019 Data Breach Investigations Report."

[17] Fortinet. "2019 Operational Technology Security Trends Report."

[18] Yoni Shohet."Ransomware Attacks Hit Manufacturing - Are You Vulnerable?" *IndustryWeek*. Mar. 26, 2019.

[19] MAPI. "Cyber Risk in Advanced Manufacturing." Nov. 15, 2016.

[20] IW Staff. "50% of Manufacturers Experienced Data Breaches in the Past Year." *IndustryWeek*. Jun. 24, 2019.

[21] Cybersecurity and Infrastructure Security Agency. Alert (AA20-049A). "Ransomware Impacting Pipeline Operations." U.S. Department of Homeland Security. Feb. 18, 2020.

[22] Warwick Ashford. "Operational Technology Security Improving, But Attack Surface Continues to Grow." ComputerWeekly.com. Jun. 12, 2019.

[23] Fortinet. "State of Operational Technology and Cybersecurity Report."

[24] Rick Peters. "A Cybersecurity Mountain to Climb: Getting IT and OT Tools to Talk to Each Other." *IndustryWeek*. Nov. 19, 2019.

[25] MAPI. "Cyber Risk in Advanced Manufacturing." Nov. 15, 2016.

About the Authors

David Beckoff

VP, Product Development and Insights, MAPI

David Beckoff is VP, Product Development and Insights at MAPI, where he is responsible for association research, benchmarking programs, and special events for the manufacturing community. Prior to joining MAPI, he served as Research Director at Gartner and led cross-industry studies on topics including data analytics, digital transformation, customer experience, and talent development.

Richard K. Peters (Rick)

CISO, Operational Technology North America, Fortinet

Rick brings the Fortinet OT-CI team more than 37 years of cybersecurity and global partnering experience working across foreign, domestic, and commercial industry sectors at the National Security Agency (NSA). As Fortinet's Operational Technology North American CISO, he delivers cybersecurity defense solutions and insights for the OT/ICS/SCADA critical infrastructure environments.

Prior to Fortinet, Rick led development of cyber capability across Endpoint, Infrastructure, and Industrial Control System technologies at the agency.

Peter Newton

Senior Director of Products and Solutions, Fortinet

Peter Newton is a Senior Director of Products and Solutions at Fortinet, where he oversees the Secure Access, OT and IoT solutions. He brings 20 years of experience with computer networking and security, working at both chip-level and system level solutions for companies including AMD, Netgear, Silver Spring Networks, and Fortinet. Prior work experience includes being an officer in the US Navy. Peter holds a Bachelor's of Science in Electrical Engineering from Rice University and a Master's in Business Administration from the University of Texas at Austin.

FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.

For more information, visit fortinet.com.

MAPI

Founded in 1933, the Manufacturers Alliance for Productivity and Innovation is a nonprofit organization that connects manufacturing leaders with the ideas they need to make smarter decisions. As the manufacturing leadership network, its mission is to build strong leadership within manufacturing to drive the growth, profitability, and stature of global manufacturers.

For more information, visit mapi.net.