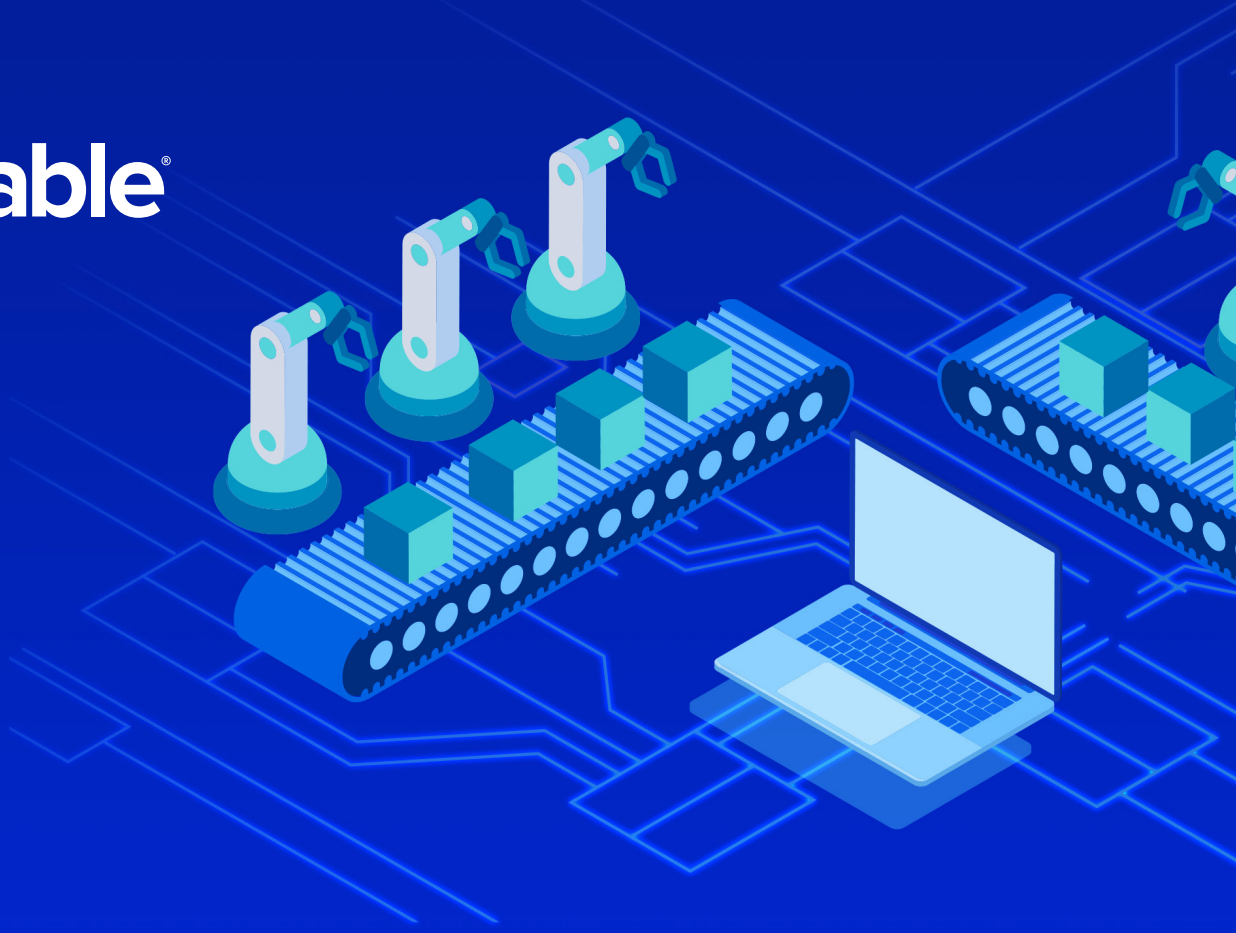


Cybersecurity in Operational Technology: 7 Insights You Need to Know

SPONSORED BY TENABLE

Independently conducted by Ponemon Institute LLC

March 2019

Cybersecurity in Operational Technology: 7 Insights You Need to Know

EXECUTIVE SUMMARY

Cybersecurity in Operational Technology: 7 Insights You Need to Know, which was sponsored by Tenable® and conducted by Ponemon Institute, reveals that a lack of visibility into the attack surface, inadequate security staffing and reliance on manual processes undermine operational technology (OT) sector organizations' stated requirements to protect OT and IoT infrastructure from downtime.

This report is based on our analysis of a subset of 701 respondents from ***Measuring & Managing the Cyber Risks to Business Operations***[1] whose organizations fall into the OT sector[2] – defined as industries dependent upon industrial control systems (ICSs) and other operational technology. All respondents are involved in their organizations' evaluation and/or management of investments in IT and/or OT cybersecurity solutions. Because today's operational systems rely on both OT and IT assets, we have investigated IT, OT and IoT.

The following summarizes the key findings:

1. **Cyberattacks are relentless and continuous against OT environments.** Most organizations in the OT sector have experienced multiple cyberattacks causing data breaches and/or significant disruption and downtime to business operations, plants and operational equipment. Many have suffered from nation-state attacks.

2. **The C-level is heavily involved in the evaluation of cyber risk.** C-level technology, security and risk officers are most involved in the evaluation of cyber risk as part of their organization's business risk management.

3. **Nearly half of organizations attempt to quantify risk from cyber events.** 48% of organizations in the OT sector (vs 38% in the non-OT sector) attempt to quantify the damage a cyber event could have on their business – and they're most likely to quantify the impact based on downtime of OT systems.

4. **OT sector organizations expect significant threats in 2019.** Concerns about third parties misusing or sharing confidential information and OT attacks resulting in downtime to plant and/or operational equipment increase when looking at 2019. Worries about nation-state attacks continue at a significant level.

5. **2019 governance priorities vary.** Increasing communication with the C-suite and board of directors about cybersecurity threats facing the organization and ensuring third parties have appropriate security practices to protect sensitive and confidential data are top priorities for 2019.

6. **2019 security priorities address sophisticated threats.** The top 2019 security priority is to improve the ability to keep up with the sophistication and stealth of attackers. This isn't surprising given the significant number of OT sector organizations that have suffered a nation-state attack in the past 24 months.

7. **Organizations are challenged to improve cybersecurity.** Few organizations have sufficient visibility into their attack surface. Gaining required visibility will continue to be a challenge due to a combination of staff shortages and heavy reliance on manual processes.

1 We surveyed 2,410 IT and IT security practitioners in the United States, United Kingdom, Germany, Australia, Mexico and Japan and the findings were presented in a previously released report, ***Measuring & Managing the Cyber Risks to Business Operations***.
2 The OT sector in this study includes respondents in energy & utilities, health & pharma, industrial & manufacturing and transportation.

KEY INSIGHTS

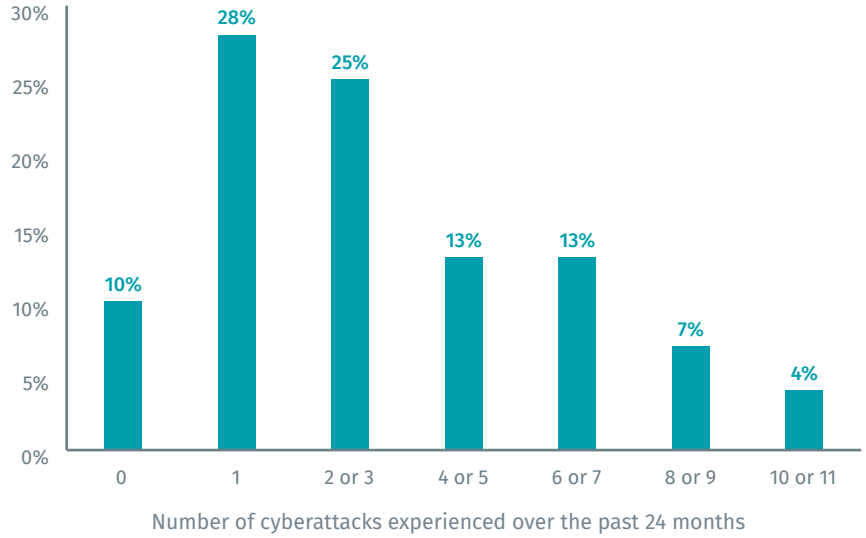
Let's take a closer look at each of the findings.

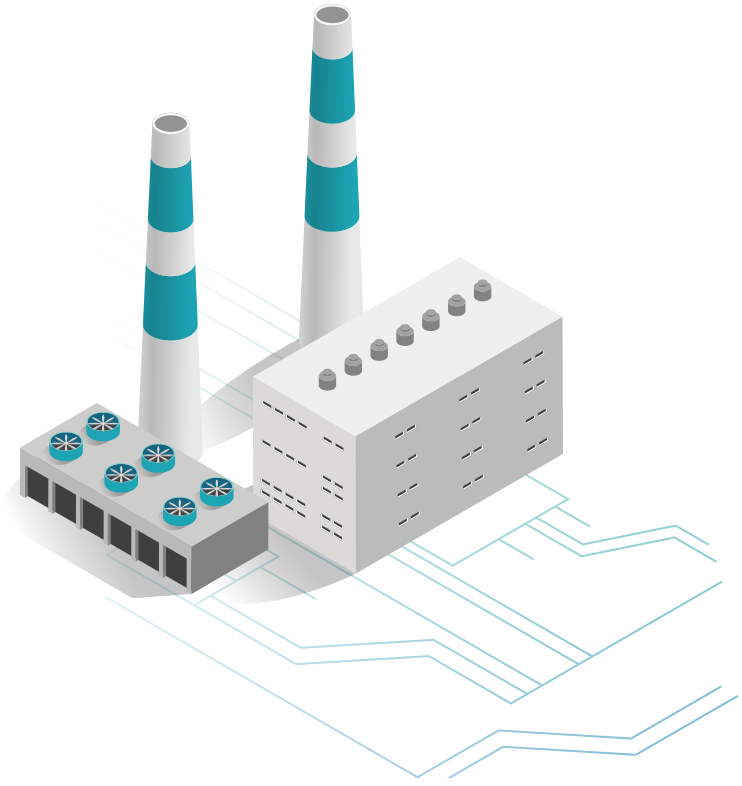
Finding #1: Cyberattacks are relentless and continuous.

As shown in Figure 1, 90% of OT organizations represented in this study have experienced at least one damaging cyberattack over the past two years and 62% have had two or more. These attacks have resulted in data breaches and/or significant disruption and downtime to business operations, plants and operational equipment.

Figure 1.
OT sector organizations are experiencing multiple damaging cyberattacks

90%
experienced at least one damaging cyberattack over the past two years

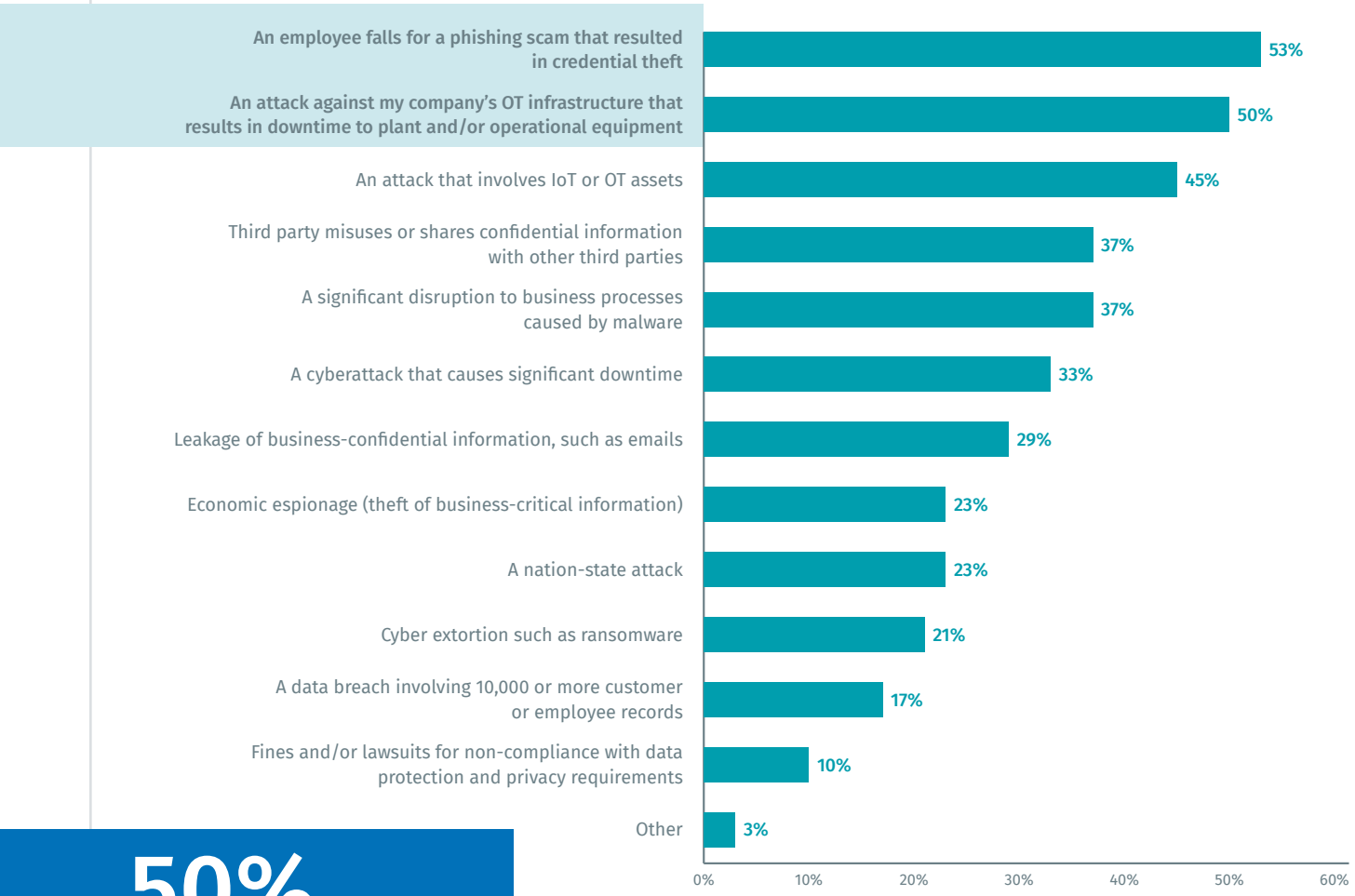




Virtually all organizations in the OT sector rely on converged OT and IT systems. Therefore, the OT sector is concerned with weaknesses and attacks relating to OT and IT systems, including phishing scams. 53% of OT sector organizations report that in the past 24 months an employee fell for a phishing scam resulting in credential theft (see Figure 2).

OT attackers often use credentials gained in IT environments to pivot into and attack OT infrastructure. Half of OT sector organizations say they've had at least one attack against OT infrastructure in the past 24 months that resulted in downtime to plant and/or operational equipment. Furthermore, 23% report at least one nation-state attack in the past 24 months.

Figure 2. Cyber events experienced in the past 24 months



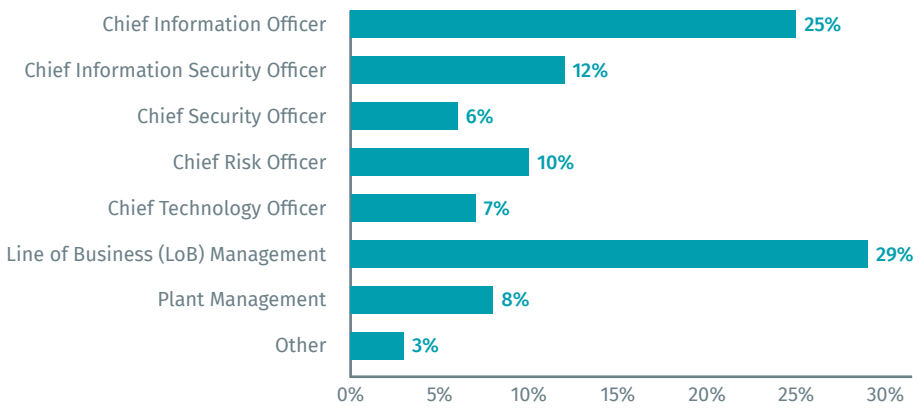
50%

have experienced at least one attack against OT infrastructure that resulted in downtime in past 24 months

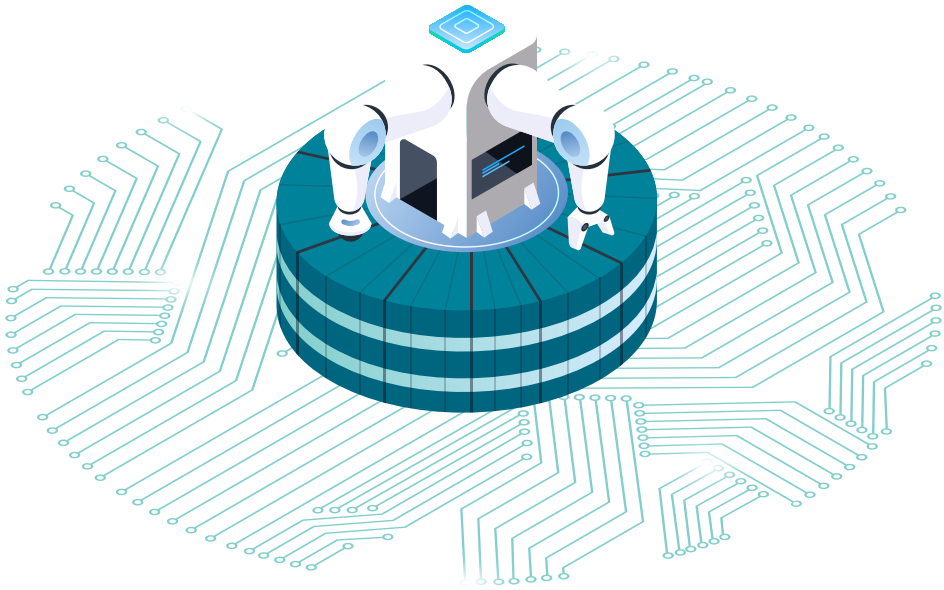
Finding #2: The C-level is heavily involved in the evaluation of cyber risk.

Not surprisingly, more than half (60%) of respondents report that C-level executives are most involved in the evaluation of cyber risk as part of their organization's business risk management. Line-of-business and plant managers are most involved only about one-third (37%) of the time.

Figure 3.
Who is most involved in the evaluation of cyber risk as part or your organization's business risk management?



60%
report that C-level is most involved in the evaluation of cyber risk

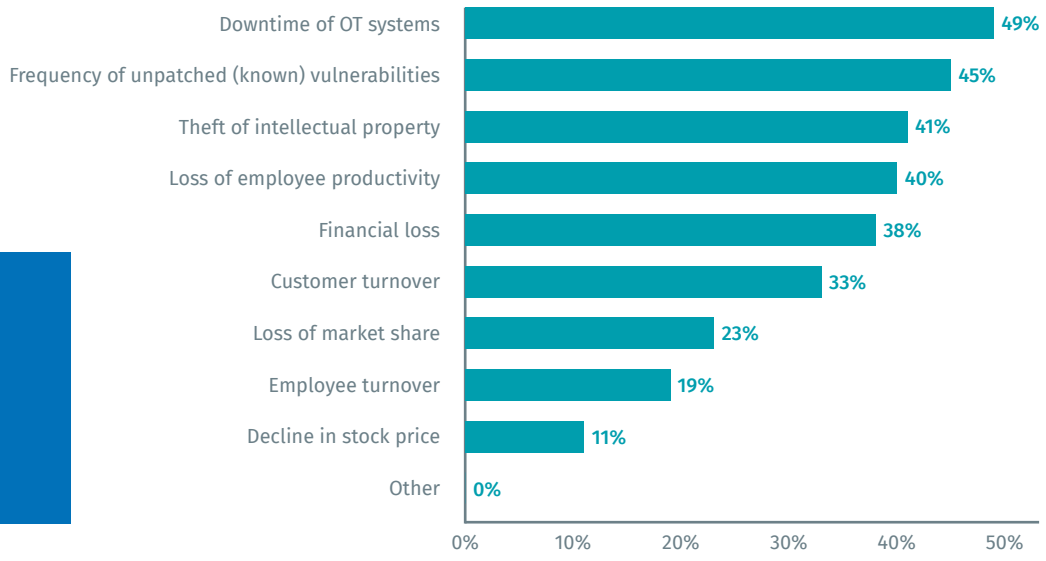


Finding #3: Nearly half of OT sector organizations attempt to quantify damage from cyber events.

Nearly half of OT sector respondents (48%) say their organization attempts to quantify the damage to the business from the threats listed in Figure 4. In fact, quantifying the damage from downtime of OT systems is rated as the highest factor when quantifying overall cyber risk (see Figure 4).

OT downtime can result in millions of dollars of lost revenue, productivity, etc. For example, the Taiwan Semiconductor Manufacturing Company Ltd. reported that the WannaCry infection which crippled multiple factories would reduce quarterly revenues by 3%[3] – estimated at more than $150 million.

Figure 4.
Factors used to quantify risk



1/2
say downtime of OT systems is biggest factor used to quantify risk

3 **TSMS Details Impact of Computer Virus Incident**

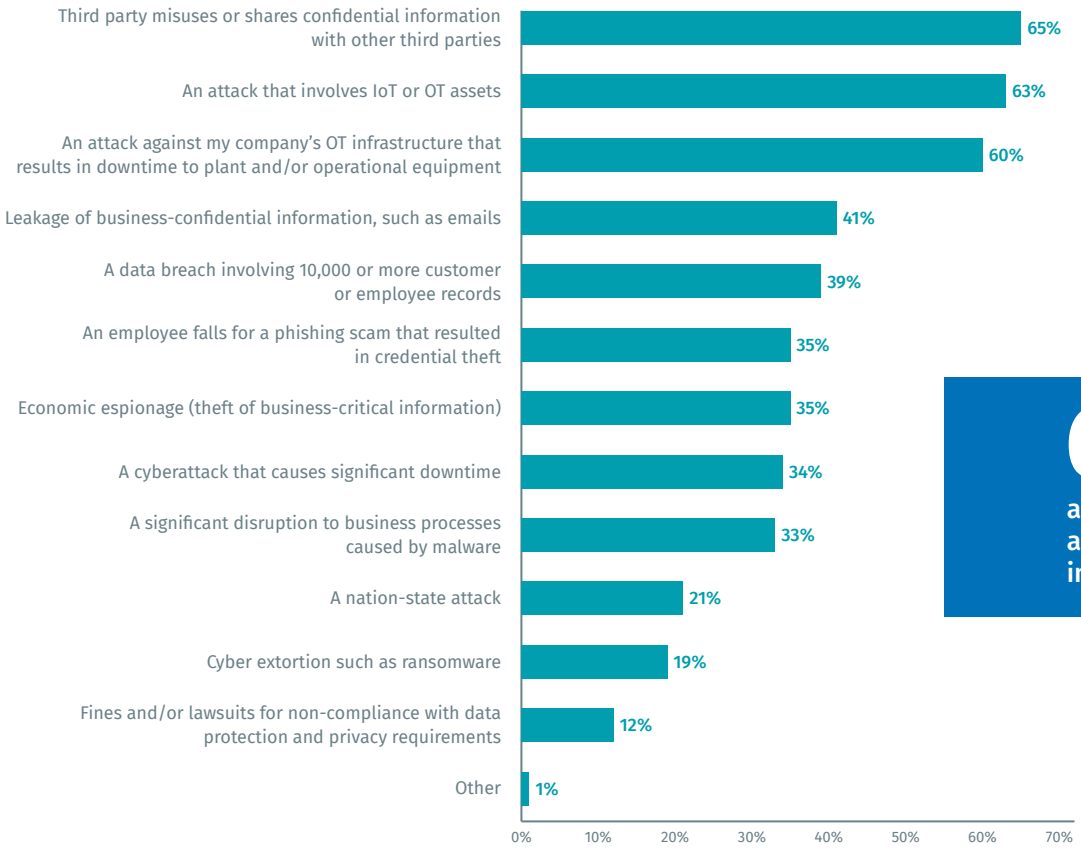
Finding #4: OT sector organizations expect significant threats in 2019.

- **Third parties misusing or sharing confidential information:** Although only 37% of OT sector respondents report that in the past 24 months a third party misused or shared confidential information with other third parties (see Figure 2), 65% list the threat as one of the top five they worry about in 2019 (see Figure 5) – making it the biggest expected threat this year. This isn't surprising given many organizations in the OT sector rely on third parties to help them manage and maintain their OT infrastructure.

- **OT attacks resulting in downtime are an increasing threat:** While 50% of organizations experienced an attack in the past 24 months against OT infrastructure that resulted in downtime to plant and/or operational equipment (see Figure 2), 60% list it as one of the threats they're most worried about in 2019 (see Figure 5).

- **Nation-state attack threats continue:** More than one-fifth (21%) of OT sector organizations list a nation-state attack as one of the threats they're most worried about (see Figure 5). Nation-state attacks are especially concerning in the OT sector because they're typically conducted by well-funded, highly capable cybercriminals and are aimed at critical infrastructure.[4]

Figure 5. Most worrisome threats in 2019



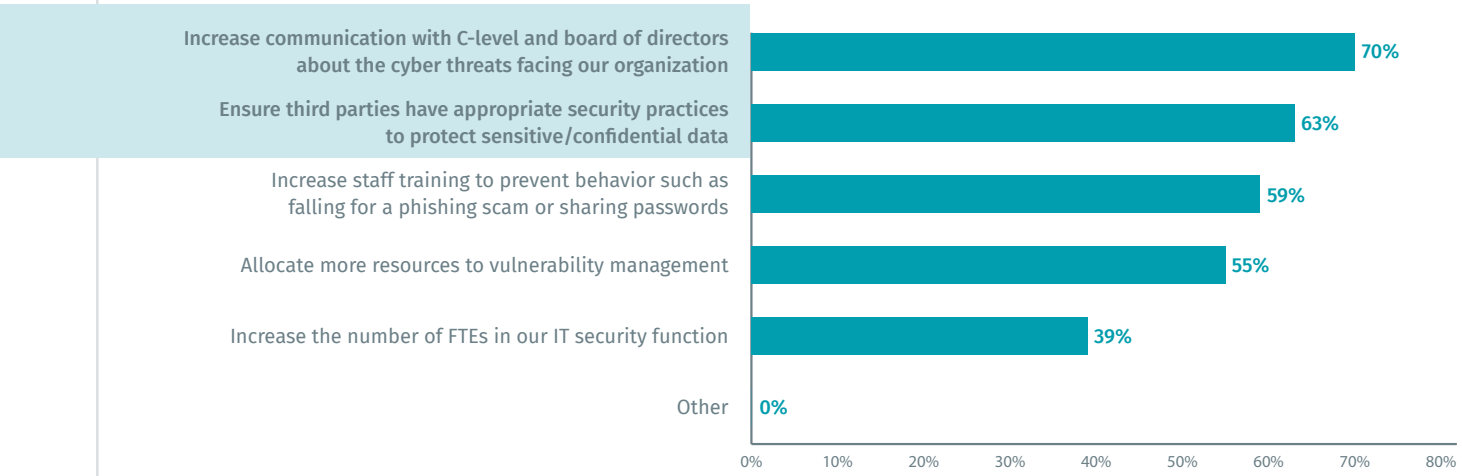
60%
are worried about an attack against OT infrastructure

4 Refer to the **US-CERT Technical Alert, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors"**

Finding #5: 2019 governance priorities vary.

Increasing communication with the C-suite and board of directors about cybersecurity threats facing the organization is the number-one priority for 2019 (see Figure 6). The second priority is ensuring third parties have appropriate security practices to protect sensitive and confidential data. This objective aligns directly with the most worrisome threat for 2019: third-party misuse or sharing of confidential information with other third parties (see Figure 5).

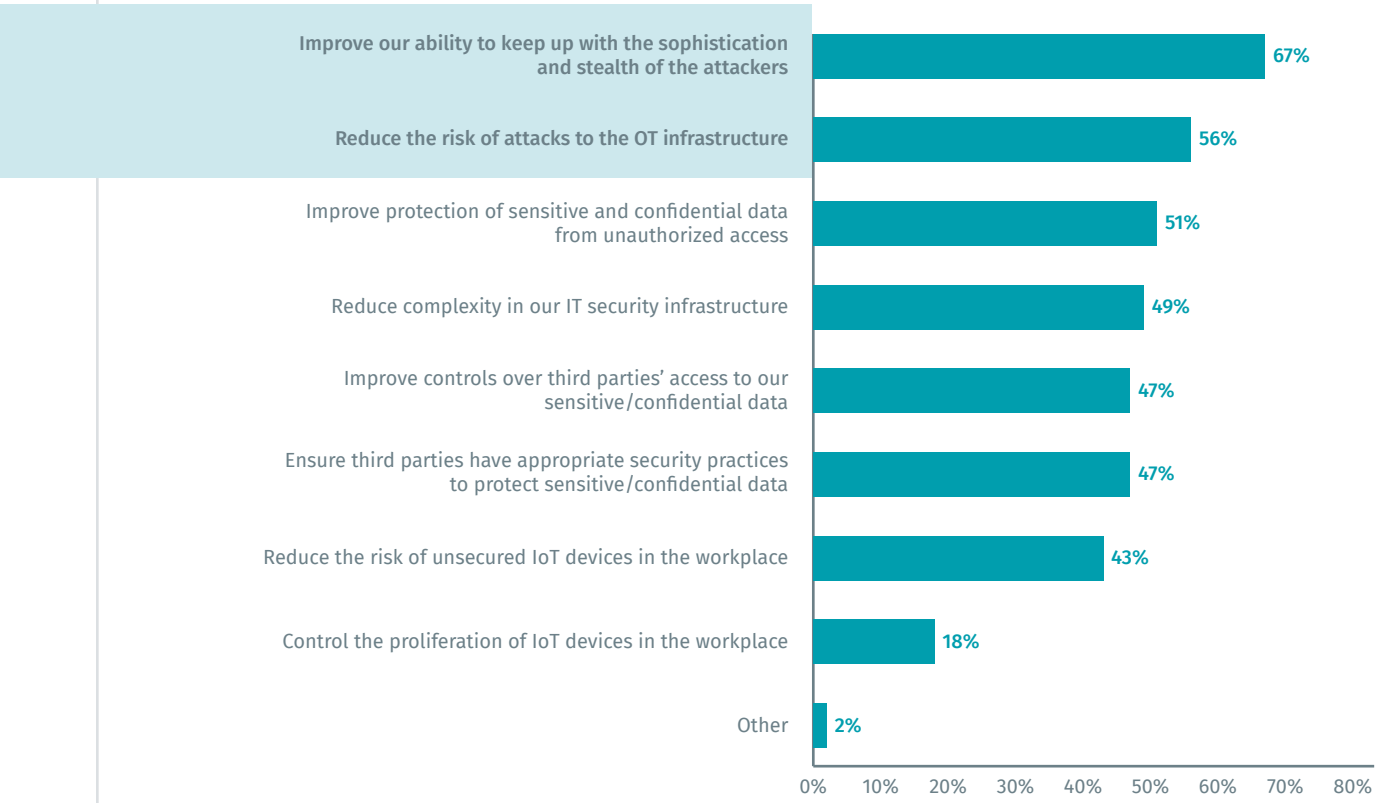
Figure 6. 2019 governance priorities



Finding #6: 2019 security priorities address sophisticated OT threats.

As shown in Figure 7, the top two priorities, "Improve our ability to keep up with the sophistication and stealth of the attackers" and "Reduce the risk of attacks to the OT infrastructure," align well with the previously discussed risk of nation-state attacks against OT infrastructure (see Figure 2).

Figure 7. 2019 security priorities



Finding #7: Organizations are challenged to improve cybersecurity.

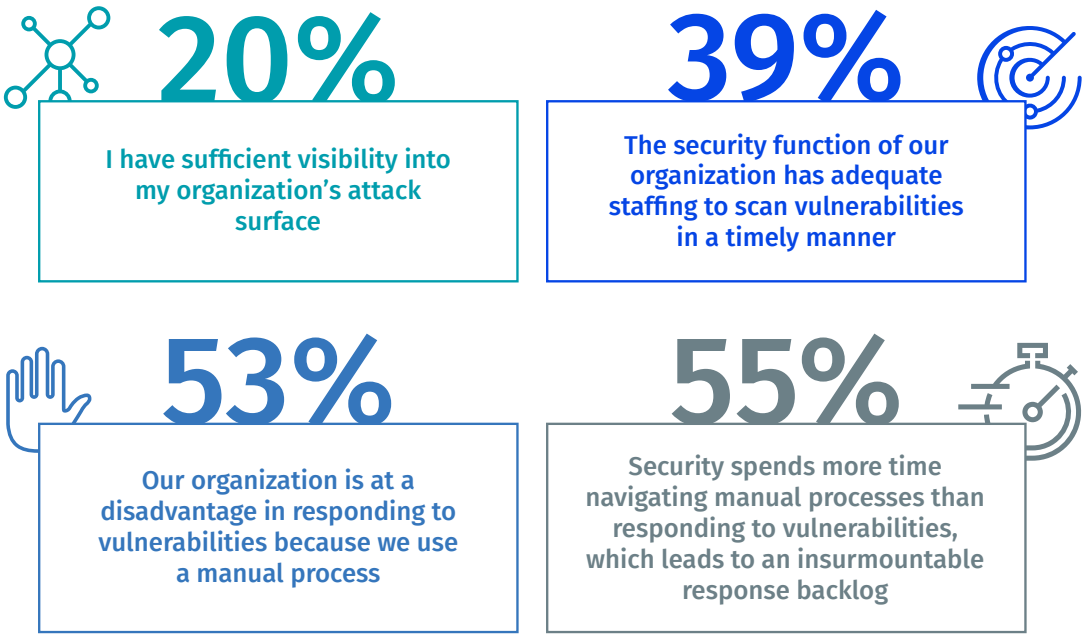
Visibility into the attack surface is insufficient

Using a five-point scale of strongly agree to strongly disagree, only 20% of OT sector respondents agree or strongly agree they have sufficient visibility into their organization's attack surface (see Figure 8). This is concerning because all security controls and processes depend on the visibility provided by comprehensive asset inventories. A complete hardware and software inventory is fundamental to all security frameworks and compliance requirements, including the CIS Controls, NIST Framework for Improving Critical Infrastructure Cybersecurity and NERC CIP.

Inadequate staffing and manual processes limit vulnerability management

The cybersecurity skills shortage has exacerbated the issues created by reliance on manual processes. This skills shortage is especially evident in vulnerability management because organizations often lack sufficient vulnerability management staff to execute the manual processes.

Figure 8. Perceptions about the challenges security teams face



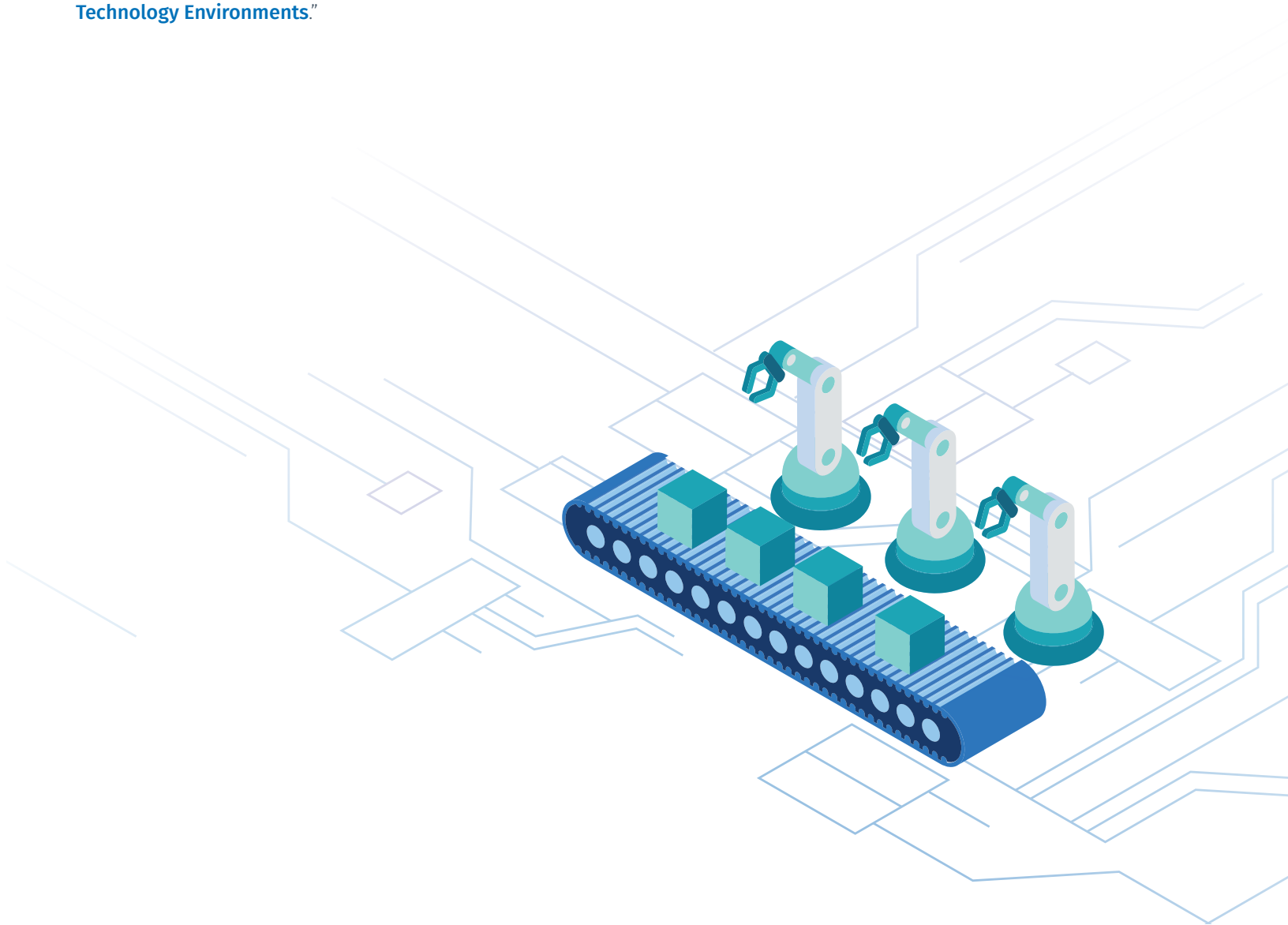
Percentages represent combined Strongly Agree and Agree responses

CONCLUSION

Organizations in the OT sector are aligning their 2019 security priorities to address their most significant worries in 2019. The survey results suggest multiple recommendations for improving security in 2019 and beyond:

- **Improve communication with the C-suite and board of directors** about the cyber threats facing the organization. This will help identify and address gaps among the organization's risk appetite and actual risk exposure.
- **Improve visibility into the attack surface.** Blind spots can result in unmanaged and unsecured IT and OT systems. Complete visibility is required for organizations to assess their risk.
- **Increase the use of automated processes** to compensate for the security staff shortage.
- **Continue to recognize the security impact of interdependencies between IT and OT systems.** Vulnerabilities and other weaknesses in IT systems can put interconnected OT systems at risk, and vice versa.

Need help getting visibility into your OT infrastructure? Check out the blog post, "**Gaining Greater Insight into Operational Technology Environments**."



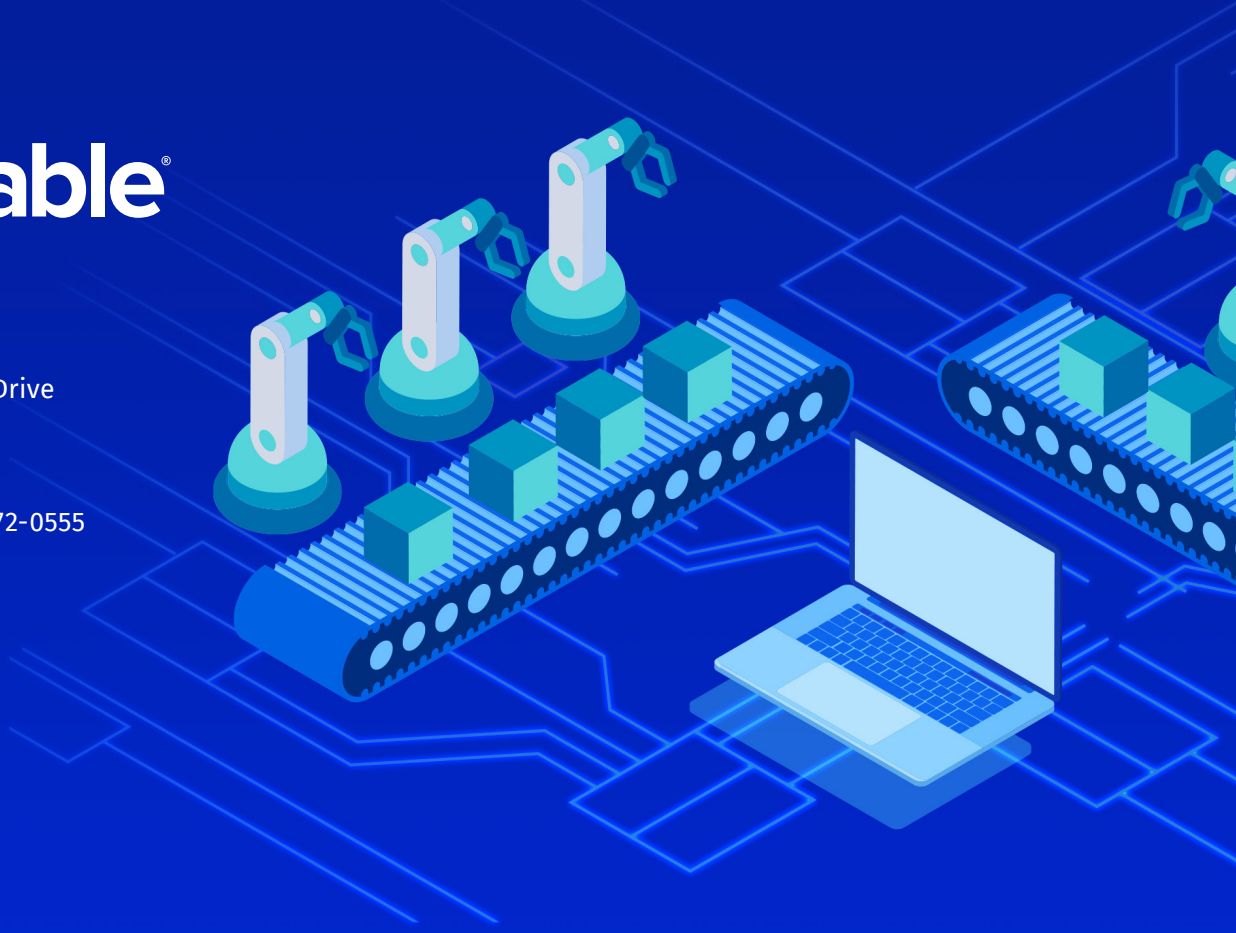
Please write to **research@ponemon.org** or call **800.887.3118** if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advance responsible information and privacy-management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com