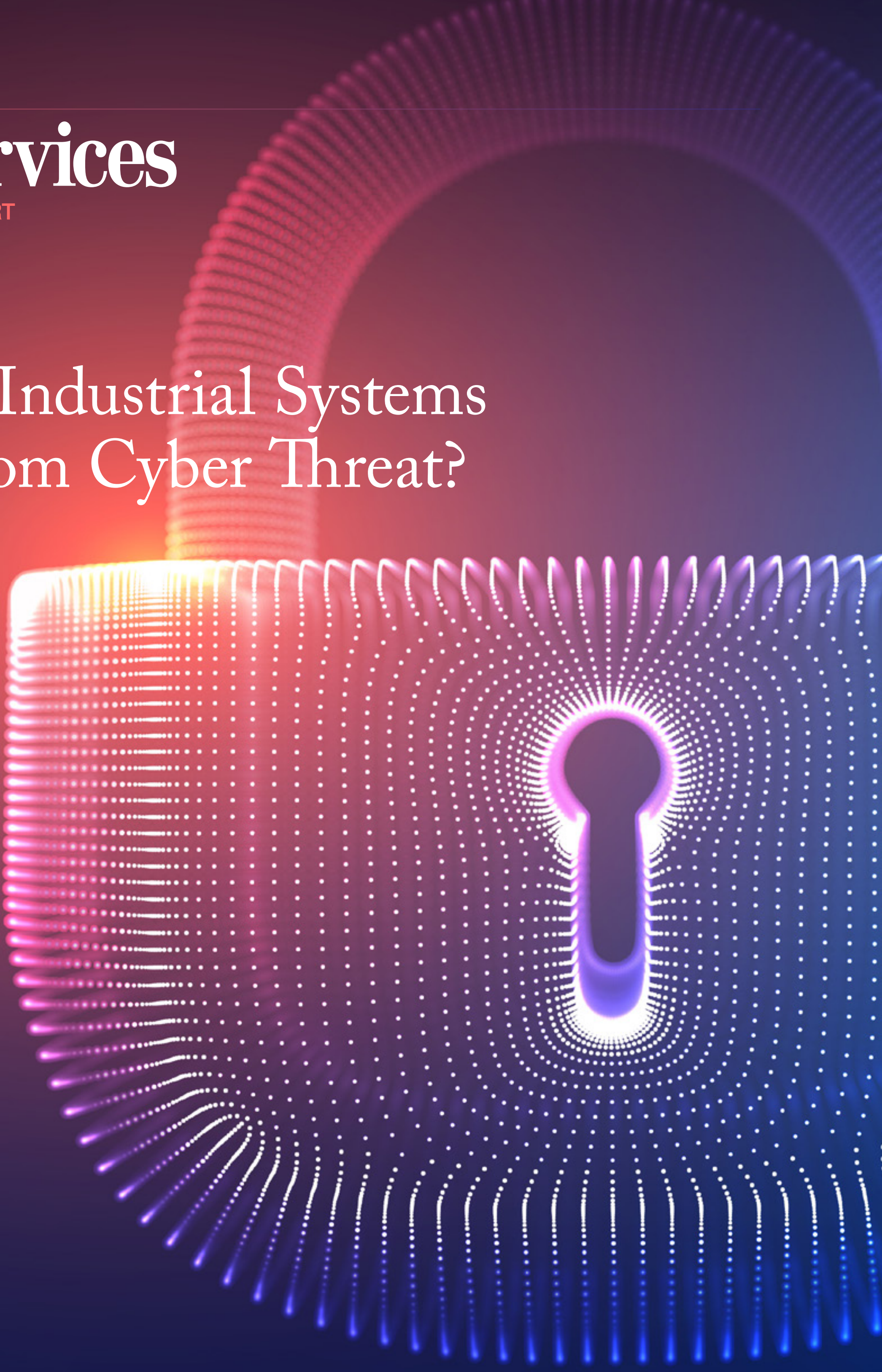
Plant Services
MARKET INSIGHT REPORT

Are Your Industrial Systems Secure From Cyber Threat?



Sponsored by

FORTINET

Are Your Industrial Systems Secure From Cyber Threat?

New survey on OT security preparedness reveals that plants understand most common cyber threat vectors, despite little agreement across industry on which department should lead these initiatives

In recent years, cyberattacks can do more than disrupt operations and compromise sensitive data — they can put lives at risk. However, when attacks occur, often there's no obligation for plant owners and operators to disclose the incident. Embarrassment and the potential for reputational damage and/or legal exposure continues to prevent the industry from sharing knowledge and developing a full portrait of efforts being taken to mitigate and respond to these attacks.

> **It was somewhat surprising that only 20.6% of respondents signaled that they had experienced ransomware attacks.**

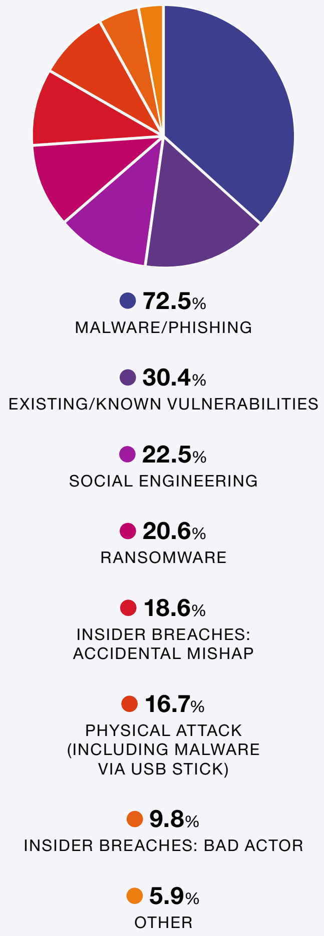
In April and May 2022, Plant Services set out to remedy this incomplete picture by deploying its new Operational Technology (OT) Security Risk Survey. The goal of the survey was to uncover the types and levels of commitment that exist among plant teams to manage cyber safety over OT networks and devices, and how organizations are putting it into action. The survey was conducted in partnership with Fortinet (www.fortinet.com), and more than 150 respondents took part, with all respondents kept anonymous to ensure that they could answer openly on this sensitive topic.

More than 80% of respondents are involved in manufacturing, both process (53%) and discrete (29%), with the remainder working in utilities, metals and mining, and transportation/aerospace. A majority of respondents also work for small or medium-sized organizations, with 78% reporting $1 billion or less in sales in the previous year.

When asked about their daily job responsibilities, more than 50% of respondents reported that their job function includes maintenance/reliability engineering and/or management, as one might expect of a survey targeted at Plant

FIGURE 1

OVERALL, WHAT TYPES OF CYBERSECURITY INCIDENTS DID YOUR COMPANY'S OT ENVIRONMENT EXPERIENCE IN THE PAST 12 MONTHS?

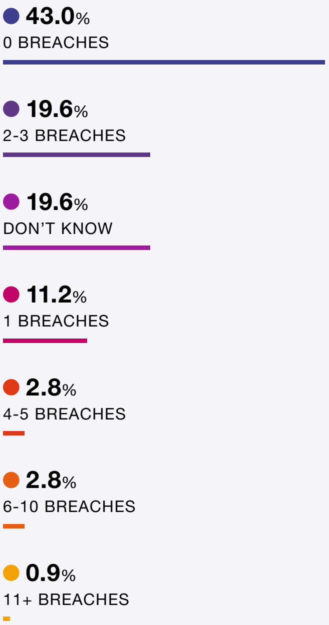


Services readers. However, about a third of respondents also reported that they are responsible for quality control (35%) environmental, safety, and health (31%) and/or plant floor operations (31%). Only 19% reported being responsible for digital transformation, and 18% said they worked on automated workflows.

The survey explored three key areas of cybersecurity: What incidents have occurred? What detection and mitigation strategies are plant teams engaged in? And who on these teams plays the lead role when implementing cybersafety initiatives?

FIGURE 2

HOW MANY DATA BREACHES DID YOUR ORGANIZATION EXPERIENCE IN THE OT ENVIRONMENT IN THE PAST 12 MONTHS?



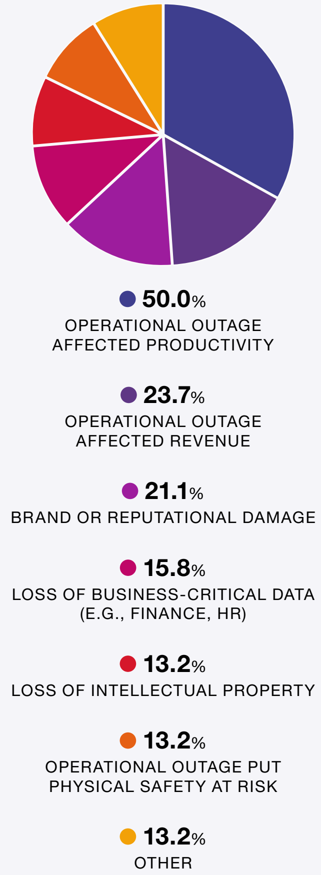
INCIDENTS: TYPE, FREQUENCY, IMPACT

One of the key questions on the survey asked about the types of cybersecurity incidents experienced in the company's OT environment in the past 12 months. By far, the most common type of incidents reported were malware/ phishing attacks (72.5%) and existing or known vulnerabilities (30.4%), with social engineering attacks rounding out the top three (22.5%). These data map well onto another survey question, in which many more respondents said their companies consider email, USB drives, and mobile devices to be part of OT exposure to cyber risk than ICS, DCS, and SCADA systems.

It was somewhat surprising that only 20.6% of respondents signaled that they had experienced ransomware attacks, given how common and lucrative those attacks can be (see Figure 1). However, in many cases, the initial compromise can be from phishing incidents, which may or may not lead to full-blown ransomware demands. Also, when it comes to insider breaches, almost double the number of incidents reported by respondents were attributed to accidental mishaps (18.6%) than to bad or malicious actors (9.8%). This result echoes reliability data uncovered by researchers such as Winston Ledet and John Moubray, who found that many physical asset failures could be traced to human error.

FIGURE 3

WHAT IMPACT DID THE OT SECURITY BREACH(ES) HAVE ON YOUR COMPANY?



In a follow-up question, respondents were asked about the number of OT data breaches experienced in the past 12 months. (A breach was defined as a specific security incident that resulted in unauthorized access to data.) A whopping 30.8% admitted that they had experienced up to three incidents in the past year, a surprisingly high number. The good news is that

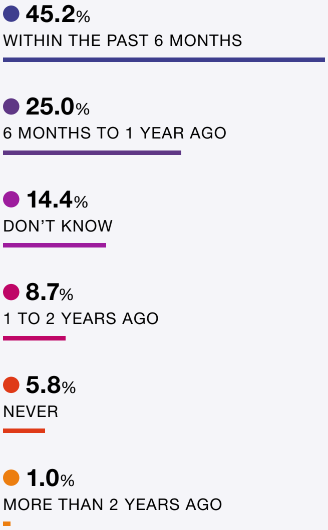
The data suggest that responsibility for cyber-strategy is not yet considered an essential job responsibility for maintenance and reliability managers.

43.0% reported no data breaches (see Figure 2). Also, close to 20% reported that they did not know the number, and most of those respondents identified as maintenance/reliability managers, which suggests that responsibility for cyber-strategy is not yet considered an essential job responsibility for these managers.

Finally, when asked about the impact of these OT data breaches on their company, the top two responses were impacts to operational productivity (50.0%) and brand or reputational damage (21.1%). Figure 3 shows the full range of impacts identified by survey respondents.

FIGURE 4

HOW RECENTLY HAS YOUR FACILITY PERFORMED A CYBER-RISK AUDIT AND/OR ASSESSMENT RELATED TO OT CYBERSECURITY?

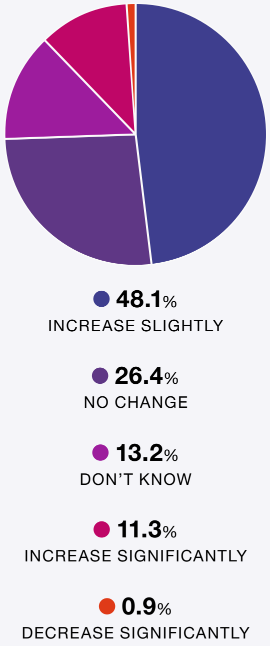


CYBERSECURITY DETECTION AND MITIGATION STRATEGIES

The next focus area of the survey explored the types of strategies that plant teams have in place both before and after the occurrence of OT cyber-incidents. When asked if their facilities had capabilities to accurately detect these incidents, 88% said that they did, whether using internal resources, external resources (i.e., contractors), or a mix of both. This result is encouraging from a critical infrastructure perspective and may even be higher, given that 7.6% of respondents were not sure what capabilities were in place. In an interesting correlation, the vast majority of respondents who said "no" or "don't know" also reported that they work at smaller companies (sales of less than $1 billion).

FIGURE 5

DO YOU EXPECT THAT YOUR FACILITY'S BUDGET ALLOCATED TO OT SECURITY NEEDS WILL CHANGE IN THE NEXT FISCAL YEAR?



When asked about when their last cyber-audit was, responses also were encouraging (see Figure 4), with 70.2% of respondents saying their last audit had come within the last 12 months, and most of those indicated it had come within the last 6 months. Speculating on these results, it could be that insurance carriers and internal finance teams are pushing for audits to be done at least once a year. Also, many plant teams are accustomed to a wide variety of audits and procedural checks, so factoring cyber-security into the procedure mix would be understandable.

FIGURE 6

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?

	NOT AT ALL A BARRIER	SLIGHTLY A BARRIER	SOMEWHAT A BARRIER	VERY MUCH A BARRIER	AN EXTREME BARRIER
Unclear roles and responsibilities	18.9%	16.7%	43.3%	14.4%	6.7%
Unclear on business impact of cybersecurity incidents	16.7%	24.4%	43.3%	14.4%	1.1%
Ineffective communication between IT and OT	23.1%	17.6%	35.2%	18.7%	5.5%
Undefined policies, procedures, or best practices	18.9%	20.0%	43.3%	11.1%	6.7%
Scarcity of talent/expertise	13.3%	24.4%	42.2%	12.2%	7.8%
Lack of training	13.3%	21.1%	43.3%	17.8%	4.4%
Fast pace of change in risk	12.1%	24.2%	40.7%	19.8%	3.3%
Regulatory change	19.3%	27.3%	43.2%	9.1%	1.1%
Insufficient resources (e.g., budgetary constraints)	16.5%	19.8%	40.7%	15.4%	7.7%
Inadequate tools or technology	16.7%	24.4%	42.2%	11.1%	5.6%

The company's financial commitment to cyber-security varied more evenly across respondents, with about half expecting a slight increase in next year's budget and only 11.3% expecting a significant increase (see Figure 5). Finally, when asked about barriers to success in this area (see Figure 6), no particular barriers stood out, as if all unhappy plants are uniquely unhappy. Overall, the top three barriers reported were available budget, available expertise, and ineffective communication between IT and OT teams. One point worth noting is that lack of training was reported as one of many moderate but real concerns and that working with your insurance team may help get cyber training added to the mix if it can be shown to positively impact the financial bottom line.

WHO PLAYS THE LEAD CYBER ROLE?

Given the lack of widely applied standards in managing OT security, you could ask 100 plants who on their staff plays the lead role and is taking the lead on these initiatives, and you'd probably get 100 different answers. Data from this survey was no different, and responsibility was fairly evenly spread across several key executive areas, from COO, CTO, and CIO to Chief Security Officer and Plant Manager (see Figure 7). These results point to a lack of standardization across the industry, which makes it difficult for plants to share best practices. Of the 12% who selected "other," some of the responses included maintenance

When it comes to corporate financial commitment to cyber-security, about half of respondents expect a slight increase in next year's budget, and only 11.3% expect a significant increase.

manager, plant engineer, and one who said, "just me." And again, these respondents reported that they work at smaller companies (sales of less than $1 billion), reflecting how smaller plant teams must take on multiple functional roles to help their company stay competitive.

In a related question, respondents were asked what percentage of unplanned downtime experienced in 2021 was attributable to OT system breaches or incidents (see Figure 8). Nearly 70% of respondents said that they were not calculating the impact of cyber-breaches on unplanned downtime; even now, with so many plants reporting 1-3 attacks in the last year, the mindset may not be there yet to connect these attacks to production outcomes. Data from a separate question on the survey also support this analysis: when asked how important a wide variety of factors were to securing their OT environment, the top response was "detection of attacks against known OT-specific vulnerabilities," which positions detection as the predominant thought mode over areas such as "incident response planning" or "standardized plan for software patching and upgrades."

Lastly, the survey looked toward the future and asked respondents how they thought OT security would change during the next three years. Two-thirds of respondents agree or strongly agree that cyberattacks targeting OT environments will increase in sophistication, with nearly as many thinking that manufacturers will increase their effectiveness at mitigating these risks (see Figure 9). Given these data points, asset management specialists must work with the CFO and insurance teams to quantify the cost of downtime in order to make a strong financial case to strengthen the prevention of cyberattacks and keep teams trained on the latest mitigation and response best practices.

FIGURE 7

WHO PLAYS THE LEAD ROLE IN MANAGING OT SECURITY AT YOUR FACILITY?

● **26.4**%
CHIEF TECHNOLOGY OFFICER

● **24.5**%
CHIEF INFORMATION OFFICER

● **17.0**%
CHIEF OPERATIONS OFFICER

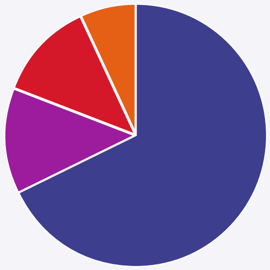
● **12.3**%
OTHER

● **10.4**%
CHIEF SECURITY OFFICER

● **9.4**%
PLANT MANAGER

FIGURE 8

OF ALL THE UNPLANNED DOWNTIME YOUR FACILITY EXPERIENCED IN 2021, WHAT PERCENTAGE WOULD YOU ESTIMATE WAS DUE TO OT/ICS SECURITY BREACHES OR INCIDENTS?



● **67.8**%
UNDEFINED

● **13.3**%
NOT SURE

● **12.2**%
5-10%

● **6.7**%
10-25%

FIGURE 9

TO WHAT EXTENT DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENTS ABOUT HOW OT SECURITY WILL CHANGE DURING THE NEXT 3 YEARS?

	STRONGLY DISAGREE	DISAGREE SOMEWHAT	NEITHER AGREE NOR DISAGREE	AGREE SOMEWHAT	STRONGLY AGREE
Manufacturers will increase their effectiveness at mitigating OT security risks	2.2%	2.2%	30.0%	31.1%	34.4%
Network integration of IT and OT will be integral to manufacturing competitiveness	3.3%	3.3%	32.2%	28.9%	32.2%
Cyberattacks targeting my company's OT environment will increase in sophistication	2.2%	2.2%	29.2%	22.5%	43.8%
Employees responsible for IT, OT, or both will work more closely together in my company	2.2%	4.4%	30.8%	27.5%	35.2%
My company will implement new solutions to address cyber risks to OT	2.2%	6.6%	30.8%	31.9%	28.6%
My company will have the right talent in place to address cyber risks to OT	4.4%	8.8%	38.5%	28.6%	19.8%

IN CONCLUSION

Cybersecurity is the responsibility of everyone working in an industrial facility, from IT staffers who take the lead in preventing cyberattacks to front-line operators and millwrights who are responsible for asset management and care. This new survey indicates that a majority of plant professionals are aware of (and involved with) their company's OT security practices, and consider malware and phishing attacks the most likely attack vector, especially via email. However, there was no single point of agreement among respondents on the barriers that exist to improving OT system security. These data suggest that cyber audits and regular cyber training are an effective step toward identifying the unique opportunities to improve OT security at your individual plant. □