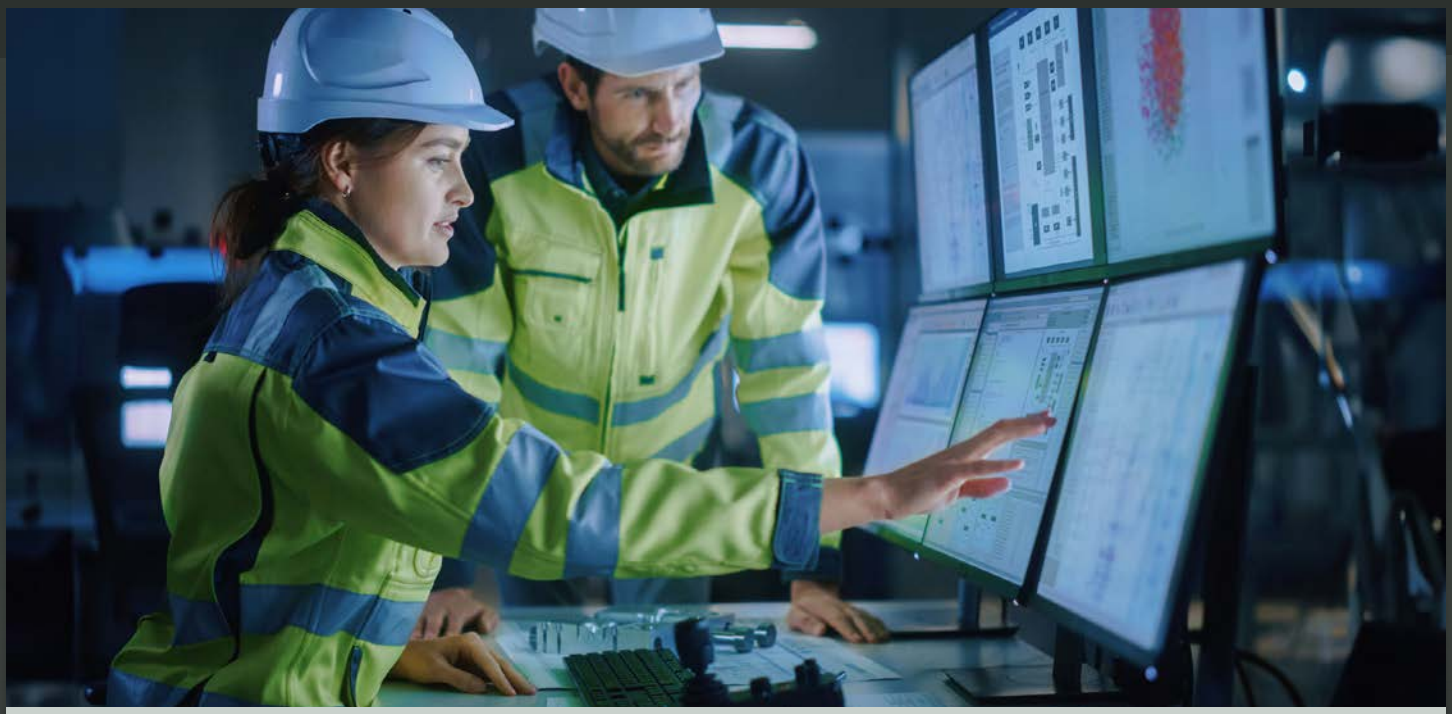


SPONSORED CONTENT | WHITE PAPER

Market Pulse

Manufacturing OT cybersecurity: increasingly concerning and costly

Amid growing awareness of cybersecurity risks to manufacturing operational technology (OT) systems, senior decision-makers increasingly are grappling with the potential impacts of downtime, missed shipments, and reputational damage, along with the growing costs of cybersecurity insurance or inability to comply with provider requirements for coverage.

CSO

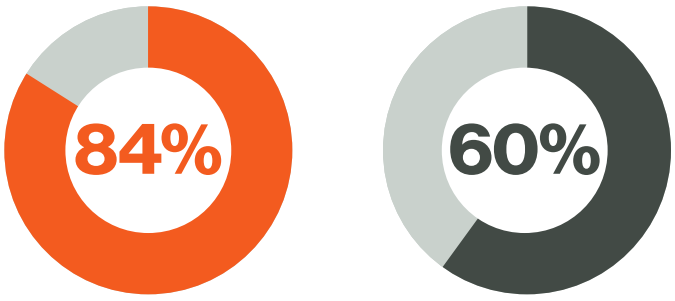
SPONSORED BY Connection® we solve IT®

Market Pulse

A recent Connections/Foundry survey of senior decision-makers employed in IT, operations, production, and executive management roles reveals a disturbing increase in the number of successful cybersecurity attacks or events since a previous survey.

An alarming number – 84% of respondents – report their organizations have experienced one or more successful cybersecurity incidents in the past 12 months, compared to 60% in 2022. Almost one-in-four have experienced multiple incidents – about double that reported in a similar survey two years ago. The number who have not been impacted has halved over the same period to just 15%.

Organizations reported to have experienced one or more successful cybersecurity incidents



Over the past 12 months **In 2022**

Future attacks deemed likely

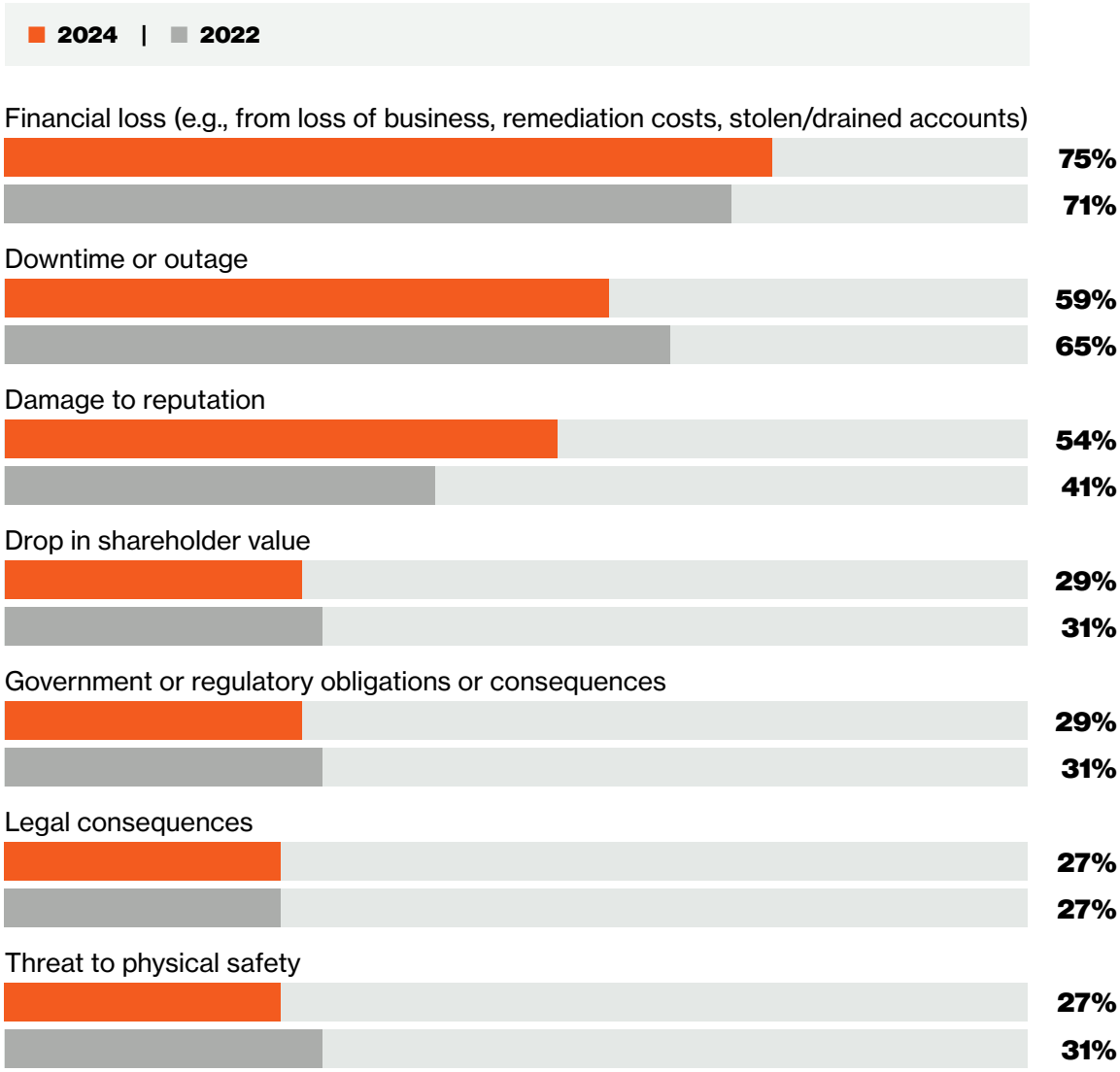
Overall, 90% perceive the degree of active cybersecurity risk currently experienced from OT cybersecurity incidents to be moderate to severe. The broadest shift over the past two years is a decline in those who believe an incident is likely in the coming 12 months, from 18% in 2022 to 8% in 2024, and correspondent increase from 30% to 42% among those who believe one is possible.

Despite broad awareness of the risk, there is a notable disparity in the perceived threat across functional areas. Among those in an IT role, for example, 79% believe a cybersecurity attack is likely in the coming year, compared to 40% in other roles. Still, an overwhelming 89% of all respondents agree that such an attack is possible, likely, or very likely.

Market Pulse

Decision-makers are also concerned about their ability to address the threat with internal resources, with 68% indicating that cybersecurity workforce shortages and lack of skillsets to address OT cybersecurity poses a significant or severe degree of risk.

Figure 1 | What are your top concerns around the impact of cybersecurity on your business?



SOURCE: FOUNDRY

98%

Plan moderate to significant investment in **modernizing IT or industrial networking solutions over the next 12 months.**

Market Pulse

Financial impacts go beyond bottom line

Just as in 2022, financial losses, downtime/outages, and reputational damage are the top three concerns among survey respondents, but the latter accounts for the biggest change, with an uptick from 41% to 54%.

The results indicate a growing awareness that not only could their companies lose money from a successful attack, but it also may deter customers and partners from doing business with them.

Another growing negative impact is the cost and even ability to qualify for cybersecurity insurance, with 84% in 2024 reporting their organizations have experienced challenges with finding or qualifying for coverage. That's up from 65% in 2022.

Specifically, 43% say their cybersecurity posture is limiting the availability of cybersecurity insurance; 27% say they are struggling to comply with insurer requirements for coverage, both up from 2022, while 14% report having been dropped by their providers, the one area that has declined over the past two years, from 18% in 2022.

Market Pulse

Regardless, costs are going up, with 59% saying the cost of insurance premiums is high or increasing due to their cybersecurity posture. That's a substantial increase over the 2022 survey. Across the industry, insurers expect their customers to shore up their cybersecurity posture, skilled resources, and security-minded culture.

Figure 2 | What challenges does your organization face with respect to cybersecurity insurance?

SOURCE: FOUNDRY

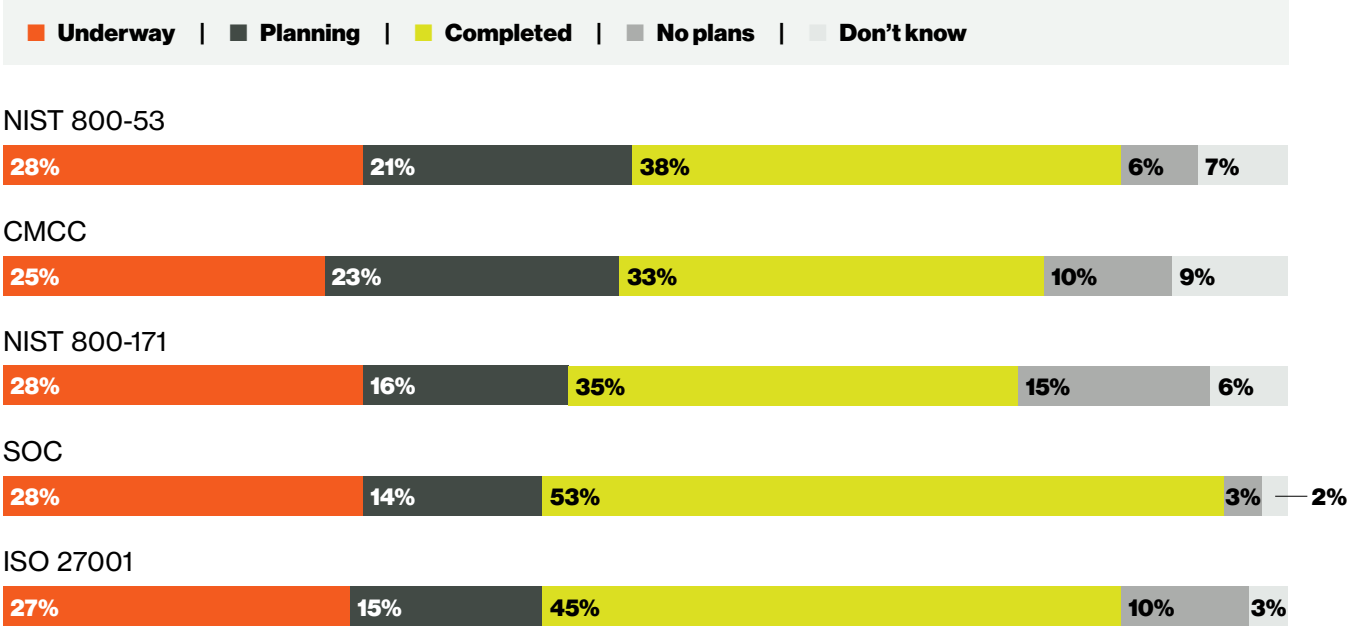
Market Pulse

Security a factor, but not foremost, in modernization wave

Many manufacturers are understandably concerned over vulnerabilities as they pursue competitive advantage through modern convergence and infrastructure that will enable future investments into smart manufacturing technologies, effective data orchestration, and exchange of information across functions.

Modernization is underway at 98% of surveyed companies, with 56% allocating significant investments to upgrade and enhance OT or industrial networking infrastructure, and 42% planning moderate investments to improve existing OT or networking systems. Foremost among investment drivers are improving operational efficiency (69%), scalability for future growth (63%), and security trailing somewhat at 54%.

Figure 3 | What are your organization's plans to invest in managed compliance services?



SOURCE: FOUNDRY

Market Pulse

There is a demonstrable shift toward managed compliance services investments, with more than half saying they have completed a move to managed security operations centers, but many are still in the planning or implementation stages in key areas such as the ISO 27001 and NIST 800-53 information security management standards or the US Department of Defense Cybersecurity Maturity Model Certification program.

The move to managed compliance services provides a faster path to enhanced compliance and improved cybersecurity posture, as well as improved access to cybersecurity resources, including advanced tools and domain experts who understand how best to mitigate and can assist with remediation in the face of a cybersecurity event. ◆

Increasing resiliency | **Manufacturing is the most targeted industry for cybersecurity incidents, with a high rate of successful attacks.** An improved cybersecurity posture, driven by a robust and resilient infrastructure that complies with industry standards and regulations, will help to control the growing cost of cybersecurity insurance and minimize the likelihood of downtime. That's vital to decreasing the risks of financial loss and brand and partner reputation impacts.

Learn more on how manufacturers can create a cybersecurity framework for success here.

Contact your Connection Account Team for more information.

Business Solutions 1.800.800.0014

Enterprise Solutions 1.800.369.1047

www.connection.com/manufacturing

CSO

SPONSORED BY Connection we solve IT®

C2772771-0824