Understanding how manufacturing enterprises navigate threat landscapes

a CXO Priorities report in partnership with Quest®

CONTENTS

INTRODUCTION

SURVEY OVERVIEW

PART 1
Challenges with cybersecurity in the manufacturing industry

PART 2
Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

CONCLUSION

ⓘ INTRODUCTION

The rapid expansion of attack surfaces and continuously evolving threat landscape has almost tripled the chances that every manufacturing enterprise will experience a cybersecurity event significant enough to disrupt their production process. The pandemic played a pivotal role in exposing cyberattack surface areas and limited cybersecurity tools, which in turn has put the spotlight on disaster recovery policies in the manufacturing industry.

As a growing threat to the manufacturing industry, cyberattacks continue to advance in quantity and sophistication. We are witnessing disruptive attacks impacting industrial processes and supply chain disruptions, with ransomware, intrusions enabling information theft and new activity from industrial control systems targeting adversaries.

The effect of these advancements and enterprise systems lacking inherent security controls required to protect themselves, is leading to production downtime, financial losses in the millions, supply chain disruptions and reputational damage to businesses.

Manufacturing ranks among the top five industries for cyberattacks. The way to start, experts suggest, is for every manufacturing organisation to invest in holistic cyber management programmes that extend across the enterprise to identify, protect, respond to and recover from cyberattacks.
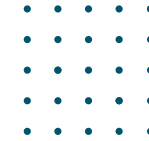
SURVEY OVERVIEW

To find out more, we surveyed C-level executives about their challenges with cybersecurity in the UK, Germany and France across the manufacturing sector. This report explored the challenges manufacturing companies face with bolstering their security and disaster recovery policies.

Through this survey, we aimed to discover:

- How manufacturing enterprises navigate threat landscapes, both currently and in the future
- The major threat challenges and security gaps within the manufacturing industry
- Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

Key Findings:

- Over 38% of manufacturing organisations will incur a US$20 to US$50 million revenue loss if their Active Directory environment was compromised for 24 hours and 32% will experience between US$50M and US$100 million loss
- Industrial espionage (21%) and ransomware (22%) are the greatest security threats within the manufacturing industry
- Thirty-three percent of manufacturing enterprises consider cybersecurity important but rely only on existing security without additional review when adopting new technology
- Eighty percent of respondents say their organisation's cybersecurity has been negatively affected by the shortage of skills
- Over half of the respondents (54%) consider cybersecurity as important when adopting new technology
- Two-thirds of the respondents (66%) believe that the potential of cybersecurity risks will negatively affect the speed of adopting new technology in their organisation
- The overwhelming majority (87%) state their cybersecurity measures do align with the NIST framework
- Over two-thirds of respondents (67%) cite aligning with a cybersecurity framework for their organisation as a medium to high priority
- When evaluating if an organisations's cybersecurity has been negatively affected by a skills shortage four-fifths of the respondents cited being negatively affected (80%)
- The fast pace of new technology being adopted (33%) was cited as the biggest cybersecurity skills gap challenge for organisations, closely followed by reliance of legacy technology (27%) and budget restrictions (27%)
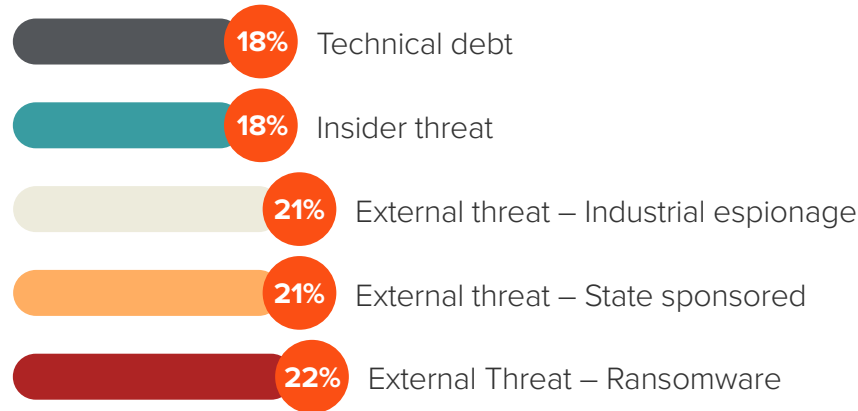
Challenges with cybersecurity in the manufacturing industry

Managing rising cyberattacks and aligning cybersecurity measures with organisational frameworks is a key concern to many manufacturing enterprises. In this section, we explore the industry's threat landscape and the major challenges for respondents in protecting their attack path.

What do you believe are the greatest security threats within the manufacturing industry? (Please select two)

18%	Technical debt
18%	Insider threat
21%	External threat – Industrial espionage
21%	External threat – State sponsored
22%	External Threat – Ransomware

Key Takeaway

Ransomware (22%), industrial espionage (21%) and state-sponsored threats (21%) are considered the greatest security threats within the manufacturing industry. This is a clear representation of the current state of attack surfaces and the need for manufacturing enterprises to consider OT security as early as possible.

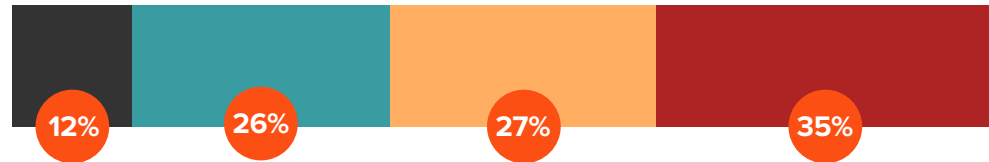# Challenges with cybersecurity in the manufacturing industry

Which of the following incidents have you experienced in your organisation? (Please select two)

12% **26%** **27%** **35%**

- ⬛ Unintentional data leak (laptop sent to the wrong person etc)
- 🟦 Credential theft/account compromise
- 🟧 Phishing/social engineering
- 🟥 Ransomware/Malware

Key Takeaway

Respondents attest that ransomware/malware (35%) and phishing/social engineering (27%) are their most experienced forms of attacks. This highlights a strong need to build multilayered security against targeted and fileless attacks that can stop viruses, spyware, malware and ransomware. Concerningly, manufacturing ranks among the top five industries for cyberattacks which calls for the need for several powerful layers of protection.
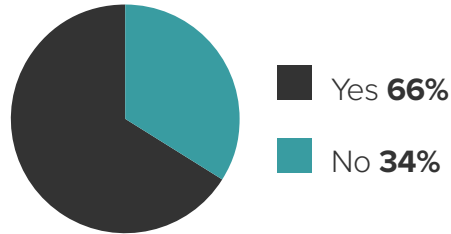
Quest

CXO priorities

A Lynchpin Media BRAND

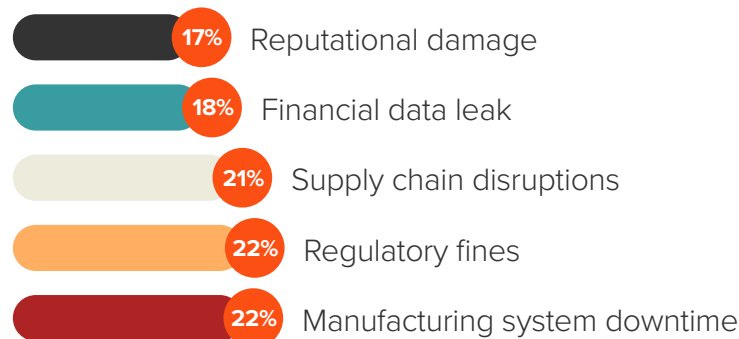# Challenges with cybersecurity in the manufacturing industry

Do you believe your organisation will be the target of a cyberattack within the next 12 months?

■ Yes **66%**

■ No **34%**

Key Takeaway

More than half of respondents (66%) believe their manufacturing enterprise will be the target of a cyberattack within the next 12 months. This highlights the reality that as long as digitalisation continues, attackers will always find new ways to target industrial control systems, so security should either be a high or medium priority for organisations moving forward.

Which of the following issues are you most concerned about mitigating with cybersecurity measures? (Please select two)

- **17%** Reputational damage
- **18%** Financial data leak
- **21%** Supply chain disruptions
- **22%** Regulatory fines
- **22%** Manufacturing system downtime

Key Takeaway

Manufacturing system downtime (22%) and regulatory fines (22%) are the most concerning areas for manufacturing enterprises when mitigating cybersecurity risks. As these organisations monitor projects and associated risks, resilient security tools will be critical to shore up defences. This also implies that security budgets will likely be adjusted to accommodate these areas of concern.
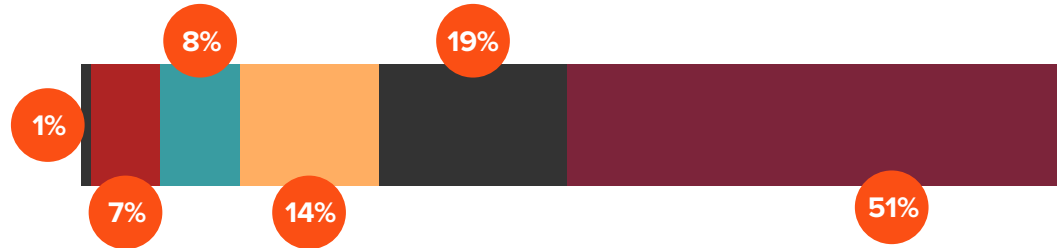
Quest

CXO priorities

A Lynchpin Media
BRAND

Challenges with cybersecurity in the manufacturing industry

How often do you review the vulnerabilities and potential attack paths that currently exist within your Active Directory environment?

1%
8%
19%
7%
14%
51%

- ⬛ We do not do this
- 🟦 I don't know
- 🟥 Weekly
- 🟧 Yearly
- ⬛ Monthly
- 🟪 Every 6 months

Key Takeaway

More than half of respondents (51%) state the routine for reviewing vulnerabilities and potential attack paths within their Active Directory environment occurs only twice a year. Only 19% conduct monthly reviews and 7% on a weekly basis. Considering the rapid expansion of the threat landscape and how reviews expose exploitable paths, it is strongly advised that organisations introduce more security hires who can constantly review and safeguard high-impact assets.

Quest

CXO priorities

A Lynchpin Media BRAND

If you answered "We do not do this" in the previous question – why do you not currently conduct a review?


- ■ Lack of expertise **50%**
- ■ Lack of adequate tools/solutions **50%**

Key Takeaway

Lack of expertise (50%) and lack of adequate tools and solutions (50%) are the main reasons why some manufacturing organisations do not review vulnerabilities and potential attack paths that currently exist within their Active Directory environment. If the global shortage of cyber-skilled professionals and adequate tools continues, organisations will find it increasingly difficult to be on the winning side of the security battle. This will clearly hold back progress in achieving adequate and effective protection in the production process.

What would be your organisation's estimated revenue loss if your Active Directory environment was compromised for 24 hours in US$?

1–10M 11%	<1M 19%	50–100M 32%	20–50M 38%
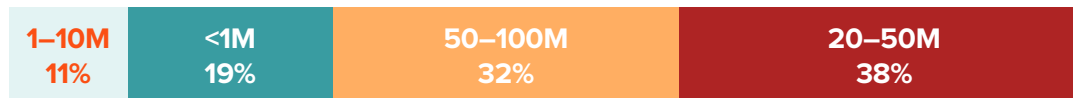
Key Takeaway

If a manufacturing organisation's Active Directory environment was to be compromised for 24 hours, 38% of these enterprises will lose an estimated revenue of US$20–50M while 32% will incur a US$50–$100M loss. Conversely, companies which would be willing to take a more proactive investment approach to their security posture would save millions. It is also unlikely to predict that a compromised Active Directory environment will last only 24 hours. This means investing in security is only an upward spiral and a strategic move in the right direction for organisations to save more.

Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

Investment and adapting to new technologies are critical in facing the current rise in attacks. In this section, we look at the top considerations for organisations in the coming year and what their key priorities look like.

How important is cybersecurity when adopting new technology?

21%	22%	24%	33%
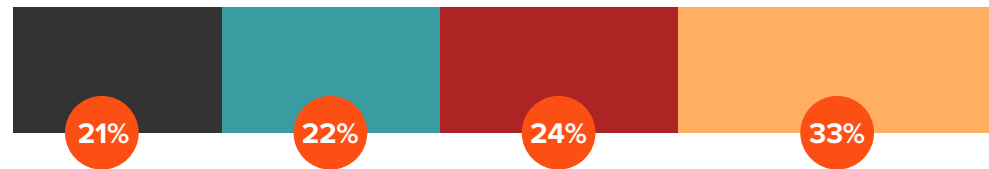
■ We may consider cybersecurity, but view it as optional in most scenarios

■ We don't consider it important

■ We always conduct a dedicated cybersecurity review each time new technology is adopted

■ We consider it important, but in most cases just trust our existing cybersecurity without additional review

Key Takeaway

Over half of the respondents (57%) consider cybersecurity as important when adopting recent technology. Nearly a quarter of respondents (24%) state they always conduct a dedicated cybersecurity review each time new technology is adopted. This clearly highlights that adopting innovative technology is and will always be a critical component in enabling organisations to strengthen their security posture. We are still witnessing a large fraction of enterprises trusting their existing cybersecurity without additional reviews, and with this presents opportunities for vendors which specialise in securing larger attack surfaces from digital technology adoption.

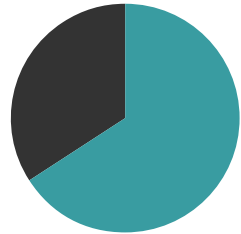# Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

Do you believe that the potential of cybersecurity risks will negatively affect the speed of adopting new technology in your organisation?
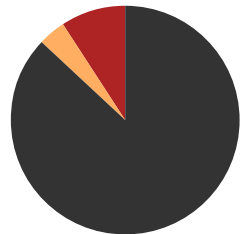
Key Takeaway

Two-thirds of the respondents (66%) believe that the potential of cybersecurity risks will negatively affect the speed of adopting recent technology in their organisation. Organisations must invest in these areas to safeguard their networks and be adequately prepared for disaster recovery situations. This highlights the need for security partners to execute these security plans and to help these businesses adopt new technologies at a faster rate.

■ Yes **66%**　■ No **34%**

Do your cybersecurity measures align with the NIST framework?

■ Yes **87%**　■ We haven't heard of NIST **9%**

■ No **4%**

Key Takeaway

The overwhelming majority (87%) state their cybersecurity measures do align with the NIST framework. From an IT and cybersecurity perspective, adhering to NIST framework should be a top priority for companies which understand the value of regulatory compliance. Organisations will therefore need security partners which can lead the proper implementation of the NIST framework approach.

Quest

CXO priorities

A
Lynchpin
Media
BRAND

Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

Looking ahead over the next 12 months, how much of a priority will aligning with a cybersecurity framework be for your organisation?

| 33% | 33% | 34% |

■ **Low priority.** We are not prioritising OT aligning with a cybersecurity framework

■ **Medium priority.** We need to take steps to become better aligned, but we must balance this against other security objectives.

■ **High priority.** We now have many more connected devices and therefore many more risks – achieving a high level of alignment has become a strategic objective

Key Takeaway

Over two-thirds of respondents (67%) cite aligning with a cybersecurity framework for their organisation as a medium to high priority. This suggests that enterprises must invest in critical infrastructure to support an ever-growing ecosystem of connected devices and achieve a balance between strategic and security objectives. It shows that companies are seeking unbiased, superior cybersecurity solutions and taking a long-term risk management strategy that supports their security posture.

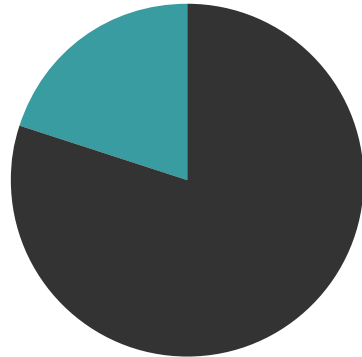# Priorities and plans for adopting new technology, aligning with frameworks and addressing skills gaps

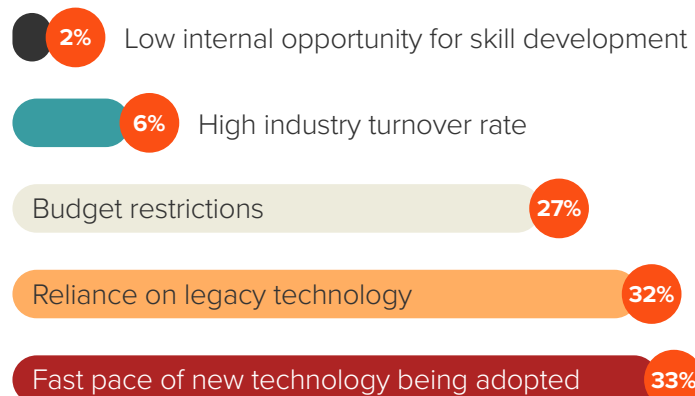## Has your organisation's cybersecurity been negatively affected by a skills shortage?

■ Yes **80%** ■ No **20%**

Key Takeaway

When evaluating if an organisation's cybersecurity has been negatively affected by a skills shortage, four-fifths of the respondents cited being negatively affected (80%). There is a case here for a trusted security provider which can implement gap analysis to identify growth opportunities and prioritise resources. A failure to address this skills gap will exacerbate workplace inefficiencies with staff struggling to handle their responsibilities and perform assigned tasks. With productivity being at the heart of manufacturing processes a skills gap analysis would help to evaluate its overall efficiency and be better placed to handle cyberattacks.

What is the biggest cybersecurity skills gap challenge your organisation faces?

2% Low internal opportunity for skill development

6% High industry turnover rate

Budget restrictions **27%**

Reliance on legacy technology **32%**

Fast pace of new technology being adopted **33%**

Key Takeaway

The fast pace of new technology being adopted (33%) was cited as the biggest cybersecurity skills gap challenge for organisations, closely followed by reliance on legacy technology (32%) and budget restrictions (27%). This suggests that organisations should work with vendors which can help transmit a security culture that optimises technology adoption and has offerings at comfortable price points. Organisations should consider investing in cybersecurity training and updating legacy technology so that everyone is aware of potential red flags when keeping their data and colleagues safe.
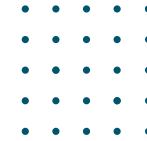
CONCLUSION

With the majority of respondents citing that aligning with a cybersecurity framework is of a medium to a high priority for their organisations for the next year, there is no better time to invest in cybersecurity partners that are focused on long-term resilience and have expertise in limiting regulatory fines. The consequences of a cybersecurity skills shortage can be harmful to an organisation, and given how threats missed is the main consequence, investing in training is imperative.

Furthermore, as organisations are keen on reducing their attack surface due to digital technology adoption, it is an excellent opportunity for providers to offer a comprehensive approach to modernising Active Directory environments and innovation. However, as a higher percentage of respondents believe the potential of cybersecurity risks will negatively affect the speed of adopting new technology, providers need to provide a comfortable price point that enables organisations to derive maximum benefits.

Another area of concern was ensuring that companies have the appropriate safeguards in place to combat system downtime and supply chain disruptions. The findings highlight that ransomware, malware, phishing and social engineering are top areas of concern for companies. By taking a long-term approach and securing a trusted partner to help obtain a proactive strategy for technology and innovation, organisations can put themselves on the path to improved cyber-resilience. The manufacturing industry is subject to much uncertainty and having a partner which has expertise in disaster recovery would provide a significant advantage to building a security-wide ethos.

> **AS ORGANISATIONS ARE KEEN ON REDUCING THEIR ATTACK SURFACE DUE TO DIGITAL TECHNOLOGY ADOPTION, IT IS AN EXCELLENT OPPORTUNITY FOR PROVIDERS TO OFFER A COMPREHENSIVE APPROACH TO MODERNISING ACTIVE DIRECTORY ENVIRONMENTS AND INNOVATION.**

Lynchpin Media is a global technology media, data and marketing services company. We help to increase awareness, develop and target key accounts and capture vital information on regional trends. Visit **lynchpinmedia.com** for more information.

CxO Priorities, a Lynchpin Media Brand

63/66 Hatton Garden
London, EC1N 8LE

Find out more: **www.cxopriorities.com**

Sponsored by

Quest