KnowBe4

SECURING MANUFACTURING'S DIGITAL FUTURE

How Cyber Threats Could Disrupt Europe's Digitalised Production Lines in an Era of Smart Manufacturing

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

0625US

Table of Contents

CONNECTED. COMPLEX. VULNERABLE.

These three words now define the evolving cyber threat landscape facing Europe's manufacturing sector—where legacy infrastructure is colliding with modern connectivity.

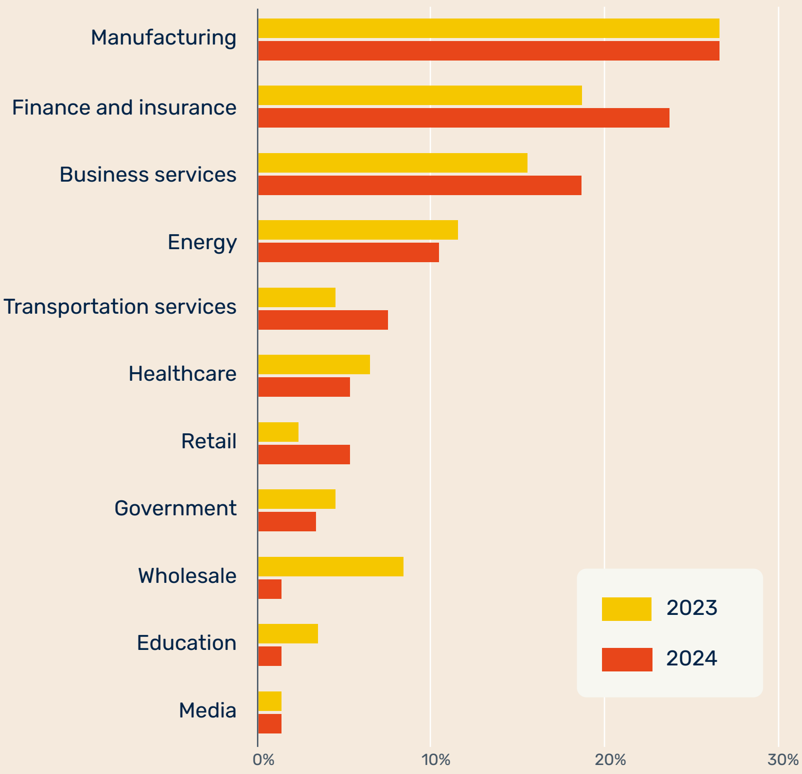
In the race to drive efficiency, speed, and innovation, manufacturers have embraced digital tools at scale. From automated production lines to cloud-based analytics, the sector is being reshaped by digital connectivity. But every advancement brings new exposure—expanding the attack surface and opening more pathways for cyber threats.

The result: manufacturing has remained the most targeted industry for cyberattacks for four consecutive years, accounting for 26% of all reported incidents across sectors.[1] And the threat is only growing. According to Verizon's 2025 Data Breach Investigations Report (DBIR), the industry saw an 89.2% increase in confirmed data breaches in 2024 compared to the previous year.[2]

The threats are not just more frequent—they're more costly. As reliance on digital infrastructure grows, so too does the price of disruption. Over the past year, the cost of attacks in manufacturing rose by 125%,[3] driven by prolonged downtime, supply chain ripple effects, and the rising value of stolen intellectual property.

Yet despite the escalating threat, many manufacturers continue to deprioritise cybersecurity—constrained by legacy systems, talent shortages, operational pressures, and years of underinvestment in digital risk. But that mindset is no longer sustainable. In an era focused on technological advances, cyber resilience and awareness is a core requirement for long-term competitiveness, operational continuity, and trust across the supply chain.

Share of Attacks By Industry, 2023-2024[1]



[1] "IBM X-Force 2025 Threat Intelligence Index," IBM.
[2] "2025 Data Breach Investigations Report," Verizon.
[3] "Building a Culture of Cyber Resilience in Manufacturing," World Economic Forum.

An Expanding Risk Surface in the Manufacturing Sector

Referred to as Industry 4.0, the past decade has seen the manufacturing sector reshaped by a widespread digital transformation. This shift has led to the adoption of modern technologies in an effort to build smart factories—facilities with enhanced automation, efficiency, and quality control. This trend continued in 2024, with technological investment in manufacturing organisations up 30% compared to the previous year.[4] And while this transformation has brought optimisation advances, it has also expanded the attack surface, exposing manufacturers to increased threats.

The tension between embracing innovation and managing security sits at the heart of today's manufacturing cybersecurity challenges.

Common Challenges Across the Manufacturing Sector

Against the backdrop of digitalisation, key themes emerge across most manufacturing sub-sectors that help explain why it remains one of the most targeted industries.

Technological Challenges

One of the most critical shifts in recent years has been the convergence of operational technology (OT) with information technology (IT). While this integration is a key step toward realising smart factories, it also introduces significant challenges. OT systems prioritise availability, reliability, and safety, whereas IT systems focus on data confidentiality, integrity, and availability. These differing priorities can lead to misalignments—and often, security becomes the casualty.

Compounding the challenge is that many manufacturers continue to depend on legacy OT, not built with cybersecurity considerations. These systems often lack fundamental security measures such as encryption, user authentication, and regular software updates that are common in modern IT environments. Although they remain critical to daily manufacturing processes, they struggle to meet cybersecurity requirements or defend against increasingly sophisticated threats. Replacing them is often avoided due to the high costs and the complexity of their integration within existing networks.

Supply Chain Vulnerabilities

Manufacturing does not operate in isolation. It is embedded within a web of global supply chains—many of which intersect with entirely different sectors such as energy, transportation and technology. This significantly broadens the sector's attack surface, meaning a single weak link, whether it's a third-party vendor or a logistics partner, can serve as an entry point for attackers.

While not exclusive to manufacturing, many manufacturers identify supply chain vulnerabilities as a significant concern. In the UK, the National Cyber Security Centre (NCSC) has historically issued repeated warnings about the rising threat posed by nation-state actors targeting weak links within the supply chains of engineering and industrial firms—many of which are tied directly to the manufacturing sector.[5] Supporting this, the World Economic Forum's survey ranked supply chain attacks as the third most significant cyber risk facing manufacturing organisations in both 2023 and 2024, underscoring the persistent nature of the threat.[6]

High Value Data

From proprietary vehicle designs in the automotive industry to sensitive research and development data in pharmaceuticals, manufacturers store a trove of high-value intellectual property. These assets are prime targets for cybercriminals and nation-state actors looking to steal, ransom, or gain a competitive edge.

[4] "State of Smart Manufacturing Report," Rockwell Automation.
[5] "Hostile state actors compromising UK organisations with focus on engineering and industrial control companies," NCSC
[6] "Building a Culture of Cyber Resilience in Manufacturing," World Economic Forum.

Automotive Manufacturing

As vehicles grow more connected and autonomous, the cybersecurity focus in the automotive sector has shifted toward protecting the car itself, with new components like onboard systems, AI-driven navigation, and external communication protocols. However, this concentrated focus on the end product often diverts critical attention from a more foundational vulnerability: the manufacturing environment.

As with other sectors, many automotive manufacturing environments still rely heavily on legacy equipment designed for 100% uptime—machinery that was never built with cybersecurity in mind.[7] In an industry where precision, speed, and just-in-time delivery are paramount, shutting down production lines for routine updates or patching is often viewed as commercially untenable. Yet, as these legacy systems are increasingly integrated into modern networks—supporting capabilities like predictive maintenance, real-time analytics, and robotic assembly—they introduce critical vulnerabilities. Without proper segmentation, continuous monitoring, and strict access controls, even a single outdated machine or unpatched robot across the assembly line can serve as an attack vector.

In this context, the cybersecurity posture on the automotive factory floor tends to be reactive rather than proactive—leaving many organisations exposed at a foundational level, despite sophisticated protections being developed for the vehicles themselves.

Food and Beverage Manufacturing

In line with the digitalisation trend, the food and beverage manufacturing sector is increasingly focused on automated equipment and networked processing facilities. This shift often brings a greater emphasis on productivity and profitability. However, according to a BSI poll, 78% of food-sector respondents said their organisation was not adequately prepared for a cyberattack, highlighting a common trade-off where security takes a back seat to operational efficiency in digitally evolving environments.[8]

According to Sue Newton, GB food and drink practice leader at WTW, "The issue with the food and drink industry is that they are considered more vulnerable because the operational technology underpinning production has increased but cybersecurity measures for businesses in the sector haven't been sufficiently considered, so many companies are now having to play catch up."[9]

In fact, cybersecurity concerns in food manufacturing environments often fall down to other critical priorities, such as food safety, contamination prevention, and public health. Ironically, while these priorities can divert attention away from cybersecurity, they are the very factors that could be directly compromised in the event of an attack.

Pharmaceutical Manufacturing

Pharmaceutical companies are rapidly shifting toward continuous manufacturing models, with interconnected environments designed to optimise production, ensure regulatory compliance, and maintain product quality.

These transformations bring both operational advantages and critical risks, as pharmaceutical organisations manage a wide range of sensitive assets. This includes intellectual property related to drug formulas and production methods, research and development data for future treatments, sensitive health records from clinical trials, and patient data—all of which are subject to strict regulatory protections.

This data is a prime target for ransomware, espionage, and intellectual property theft, especially by nation-state actors and organised cybercriminal groups. However, external actors are not the only concern. According to a survey carried out by the World Economic Forum, respondents from the healthcare manufacturing sector ranked insider threats as their second most concerning cyber threat, reflecting growing awareness of the risks posed by internal actors—whether through negligence, misuse, or malicious intent.[10]

[7] "Cyber readiness: are auto companies prepared to counter the risk of an attack?" PWC.
[8] "The Potential Risk of Cyberattacks in the Food Sector," BSI.
[9] "Tech leaves food industry more exposed to cybersecurity threat," JustFood.
[10] "Building a Culture of Cyber Resilience in Manufacturing," World Economic Forum.

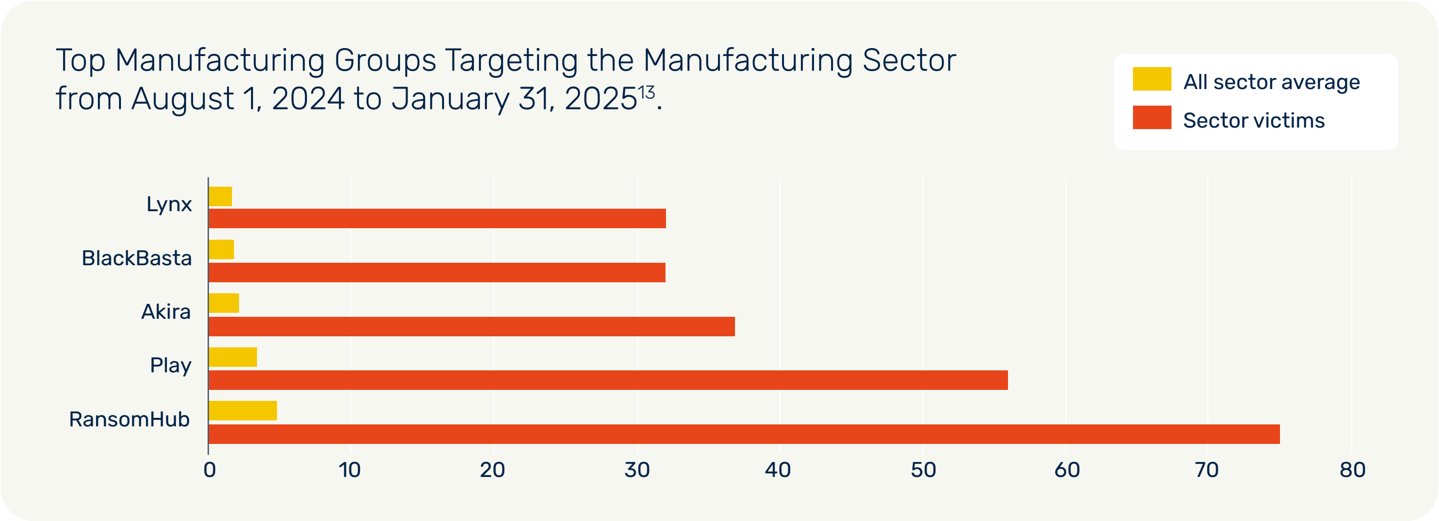
Inside the Breach: How Attackers Are Targeting the Manufacturing Sector

Ransomware: A Persistent Threat to Manufacturing

Ransomware remains one of the most pressing cybersecurity challenges facing the manufacturing sector in 2025. According to the 2025 Verizon DBIR, ransomware accounted for 47% of all breaches in manufacturing—underscoring its dominance as the attack method of choice.[11] This trend is echoed in the IBM X-Force Threat Intelligence Index, which reported that manufacturing led all industry ransomware cases in 2024.[12]

While the ransomware epidemic spans nearly every industry, it has taken a particularly aggressive hold in manufacturing due to the sector's unique vulnerabilities.

Manufacturers are especially attractive targets for ransomware actors due to the combined pressure of managing high-value data, relying on legacy systems, and the severe operational consequences of downtime. Unlike other sectors, disruptions in manufacturing can cascade through entire supply chains, affecting product quality, delivery timelines, and overall profitability. ReliaQuest noted a 24% increase in ransomware groups specifically targeting the sector over the past year, with particular focus on the group 'PlayCrypt' who they coined one of the "most dangerous ransomware groups targeting manufacturing".[13]


Top Manufacturing Groups Targeting the Manufacturing Sector from August 1, 2024 to January 31, 2025[13].

In Europe, manufacturing was the most targeted sector by ransomware between July 2023 and June 2024, according to the ENISA Threat Landscape 2024.[14] Prominent ransomware groups such as LockBit and 8Base were observed to display a large focus on European manufacturers, leveraging both commodity malware and custom-built tools to infiltrate supply chains and disrupt operations.

[11] "2025 Data Breach Investigations Report," Verizon.
[12] "IBM X-Force 2025 Threat Intelligence Index," IBM.
[13] "Threat Landscape Report: Uncovering Critical Cyber Threats to Manufacturing Sector," ReliaQuest.
[14] "ENISA Threat Landscape 2024," European Union Agency for Cybersecurity.

Social Engineering and Phishing

Unsurprisingly, social engineering—particularly phishing—plays a significant role in manufacturing-related cyberattacks. The Verizon DBIR revealed social engineering as the second most common attack type in the sector, accounting for 22% of breaches behind system intrusion. Notably, phishing was responsible for 19% of incidents, highlighting the persistent vulnerability of human users within manufacturing environments.[15]

However, the influence of social engineering extends beyond its own category. Many breaches listed under headings like stolen credentials, privilege misuse, or malware installation often begin with social engineering tactics such as phishing. Even incidents like business email compromise (BEC), sometimes categorized separately, rely on human manipulation. The DBIR ultimately attributes 60% of breaches to the human element, illustrating how deeply embedded social engineering is across the threat landscape—not as a standalone tactic, but as a foundational enabler of many attack types.

From August to November 2024, CYFIRMA reported a surge in advanced persistent threat (APT) activity, with 69% of observed APT campaigns recording manufacturing industry victims. Notable actors for these attacks included Chinese-linked threat actors such as Stone Panda (APT10), Emissary Panda (APT27), and Volt Typhoon.[16]

This spike in APT activity reflects the sector's relatively low cyber maturity. Known for favouring scale over sophistication, many APT groups exploit this gap by overwhelming manufacturing organisations with high volumes of phishing and social engineering attempts—methods that remain highly effective in industrial environments with limited user training and fragmented security defences across technology.

[15] "2025 Data Breach Investigations Report," Verizon.
[16] "Manufacturing Industry 2025" CYFIRMA.

The State of Cyberattacks Across Europe

The regulatory environment across Europe is shaping cybersecurity practices within the manufacturing industry, but due to the number of different sectors that make up manufacturing, and their differing levels of digital maturity, this has not been a unified process. The EU's NIS2 Directive,[17] for example, mandates stricter cybersecurity measures and incident reporting for operators of essential services, including key manufacturing industries like automotive, pharmaceuticals, and critical infrastructure. This has driven many organisations in these sectors to bolster their cybersecurity posture, invest in risk management frameworks, and enhance supply chain security.

Similarly, the upcoming Cyber Resilience Act, set to regulate security requirements for connected products, will further push manufacturers to adopt cybersecurity-by-design approaches, particularly impacting companies producing smart, connected equipment and IoT devices.[18]

In contrast, the food and drink manufacturing sector has historically operated under relatively relaxed cybersecurity regulations. While food safety regulations emphasise hygiene and traceability, they do not specifically mandate comprehensive cybersecurity controls. As a result, many food manufacturers have not prioritised cybersecurity investment to the same degree as sectors facing more rigorous compliance demands.

[17] European Union, Directive (EU) 2022/2555, Official Journal of the European Union, L 333 (2022).
[18] European Commission. (2022). Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). COM(2022) 454 final.

Notable Cyberattacks by Region

UNITED KINGDOM

A 2022 report revealed that 42% of UK manufacturers experienced cyberattacks, with 26% suffering significant financial losses—some up to £250,000.[23] This ongoing threat was underscored in early 2025 when two FTSE 100 engineering firms, Smiths Group and IMI, were hit by major cyber incidents.[24] Both companies were forced to engage external cybersecurity experts to investigate and contain the breaches, and following the announcement shares in Smiths Group dropped by 2.3% in early trading.

NORDICS

In August 2024, Swedish clothing and fabric manufacturer Nilörngruppen was hit by the Play ransomware group, disrupting operations and incurring financial losses of approximately 4.4 million SEK (around €354,000).[25] Just months later, in December, Finland’s Peikko Group, a building components manufacturer, suffered a similar fate from the Akira ransomware gang, leading to operational delays in 12 of its factories, limited manufacturing activities and 30GB of allegedly stolen data.[26]

BENELUX

In March 2024, two high-profile ransomware attacks hit the Benelux region. A Dutch semiconductor manufacturer fell victim to ransomware group ‘Dark Angels’, who claimed they had exfiltrated 1 Tb of sensitive data including engineering designs, corporate information and confidential client data.[19] The attack forced a shutdown of IT systems and raised serious concerns about the theft of intellectual property in a sector critical to European innovation and competitiveness.

Meanwhile in Belgium, a beverage manufacturer was hit by the Stormous group, who claimed responsibility for stealing 88 gigabytes of data.[20] The organisation swiftly enacted its incident response plan, shutting down operations—including production—to contain the breach.

DACH

In February 2024, a German battery manufacturer suffered a cyberattack that disrupted operations across five production plants.[21] The organisation proactively shut down its IT systems and disconnected them from the internet to contain the breach, leading to halted production and administrative processes.

In the same period, German industrial conglomerate, ThyssenKrupp, confirmed a cyberattack.[22] The breach involved unauthorised access to IT infrastructure, prompting them to temporarily shut down certain applications and systems. As a key player in the global supply chain for steel-based products, the incident raised concerns about the downstream impact of breaches on interconnected industries, despite reports that the customer supply chain was not affected.

[19] “Ransomware Group Claims Theft of Data From Chipmaker Nexperia,” Security Week.
[20] “Duvel has ‘enough beer’ following ransomware attack,” The Drinks Business.
[21] “German battery maker Varta halts production after cyberattack,” BleepingComputer.
[22] “Steel giant ThyssenKrupp confirms cyberattack on automotive division,” BleepingComputer.
[23] “Cyber Security in Manufacturing,” Make UK.
[24] “Engineering firm IMI hit with cyber attack just days after Smiths group incident,” IT Pro
[25] “Q3 2024 - a brief overview of the main incidents in industrial cybersecurity,” Karpersky ICS CERT.
[26] “A brief overview of the main incidents in industrial cybersecurity. Q4 2024,” Karpersky ICS CERT.

Barriers to Cybersecurity Investment in Manufacturing

Despite widespread cyberattacks on manufacturers across Europe, a general trend of resistance remains among organisations to prioritise cybersecurity investment. Several key factors contribute to this challenge:

Lack of Awareness and Expertise

Manufacturing is typically not an office-centric industry, which often results in lower cybersecurity awareness among employees who don't receive regular training, as well as a shortage of skilled personnel to effectively manage and mitigate cyber risks. This skills gap is highlighted in ENISA's NIS Investments Report 2024, where it was reported that 59% of small and medium size enterprises were finding it challenging to fill cybersecurity roles.[27]

Dependence on Legacy Systems

Manufacturing environments often rely heavily on outdated OT systems. These legacy systems are difficult to secure or replace without incurring significant costs and risking operational disruptions, creating persistent security challenges.

Financial Constraints and Downtime Risks

The financial impact of downtime is particularly acute in manufacturing. For example, every unproductive hour in automotive manufacturing costs approximately $2.3 million (around €2.04 million).[28] This risk discourages investment in cybersecurity updates or system replacements that might interrupt production, further exacerbating vulnerabilities.

Competing Priorities

Manufacturers often face a balancing act between operational demands and cybersecurity investments. With the primary focus on maintaining production uptime, physical safety, and meeting tight delivery schedules, cybersecurity can be deprioritised. This trade-off means that even when risks are understood, limited resources and urgent business needs often delay necessary security upgrades or training initiatives.

[27] "NIS Investments 2024," ENISA.
[28] "The True Cost of Downtime 2024," Siemens.

What Can Organisations Do to Address the Challenge?

Cyberattacks on the manufacturing sector are persistent, damaging, and growing in volume. As digitalisation continues, manufacturers can no longer rely on reactive or piecemeal approaches to cybersecurity. Instead, building long-term resilience requires an integrated strategy that addresses both technical vulnerabilities and human risk.

1 Secure Legacy Systems Without Sacrificing Uptime

While replacing legacy systems may not be immediately feasible, manufacturers should take steps to minimise exposure. This includes:

- Network segmentation to isolate legacy systems from core IT infrastructure.
- Virtual patching through intrusion detection systems and endpoint protection tools.
- Strict access controls and monitoring to limit who can interact with vulnerable assets.
- Establish a robust change management process to ensure that any modifications to legacy systems are properly tested and approved before deployment.

2 Embed Cybersecurity into Digital Transformation

Cybersecurity must be woven into the design and deployment of new technologies—from smart machinery to cloud-based analytics. This includes:

- Adopting a cybersecurity-by-design approach, where security is embedded into the architecture of every new system, device, and process from the outset.
- Conducting regular risk assessments across the IT/OT stack.
- Aligning with frameworks such as NIS2, ISO 27001,[29] or IEC 62443.[30]

3 Strengthen the Supply Chain

With suppliers and third parties often representing a weak link, organisations should:

- Implement vendor risk management programs.
- Require cybersecurity assessments from critical partners.
- Share threat intelligence collaboratively across the supply chain.
- Ensure the incident response plans include supply chain partners. This should outline roles, responsibilities, and communication protocols in the event of an incident.

4 Don't Overlook Human Risk

Despite increasing automation, people remain one of the most common entry points for attackers—particularly through phishing, social engineering, or misconfigured systems. To address this:

- Make it difficult for attacks to reach employees. Use intelligent technology that can filter and block suspicious emails, direct messages, or other channels that can be monitored.
- Roll out relevant and timely security awareness training tailored to the manufacturing environment.
- Simulate phishing campaigns to improve employee response and awareness.
- Provide nudges or just-in-time training to minimise the impact of any risky behaviour an employee may engage in.
- Invest in cyber talent and leadership, creating clear pathways for cybersecurity roles within OT and IT.

[29] ISO/IEC 27001:2013, Information technologys—Security techniques—Information security management systems—Requirements, International Organization for Standardization, 2013.
[30] IEC 62443 series, Industrial communication networkss—Network and system security for industrial-process measurement and control, International Electrotechnical Commission, ongoing updates.

Mitigating Human Risk in the Manufacturing Sector

Each year, KnowBe4 measures an organisation's Phish-prone™ Percentage (PPP)—the proportion of employees likely to fall for phishing or social engineering attacks. In the latest analysis of 67.7 million simulations across 14.5 million users in over 62,000 organisations, the European baseline PPP was 32.5%, meaning nearly one-third of employees interact with phishing simulations before taking part in best-practice security awareness training (SAT).[31]

In the manufacturing sector, the baseline PPP across organisations of all sizes was close to the European average at 31.8%, with large enterprises (10,000+ employees) showing the highest baseline at 43.7%. However, after just three months of consistent and effective SAT, the overall PPP dropped significantly to 19.8%—demonstrating the powerful impact of SAT in reducing human risk. After 12 months, the PPP declined even further to just 3.6%, representing a 89% reduction. Encouragingly, this progress proved sustainable, with general click rates remaining low at 3.3% after two years and 3.0% after three.

With ransomware, phishing and APT campaigns playing a prominent role in cyberattacks targeting the manufacturing sector, it's clear that strengthening employee awareness and response is critical in building a stronger security culture, defending against initial access attempts, and protecting the broader supply chain from compromise. By stopping attacks at the human entry point, organisations not only protect themselves but help prevent a cascade of disruption across interconnected sectors.

Effective Training Lowers Phishing Click Rate in Manufacturing Sector

	Calculated Phish-Prone™ Percentage (PPP) by Organisation Size				Average PPP Across All Organisation Sizes
	1-249 Employees	250-999 Employees	1,000+ Employees	10,000+ Employees	
PPP Baseline	24.8	27.1	31.6	43.7	31.8
PPP 90 days	21.2	21.0	19.9	17.2	19.8
PPP 1 Year	3.6	3.4	3.8	3.6	3.6

The evidence is clear: Cybersecurity in manufacturing is not optional, it's foundational. For Europe's manufacturing sector, the path forward demands action—not hesitation. Recognising the evolving threat landscape, addressing persistent vulnerabilities, and committing to smart, strategic investment in security are essential steps toward a resilient and secure digital future.

[31] "Phishing By Industry Benchmarking Report: Europe 2025," KnowBe4.

About KnowBe4

As the provider of the world’s largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com