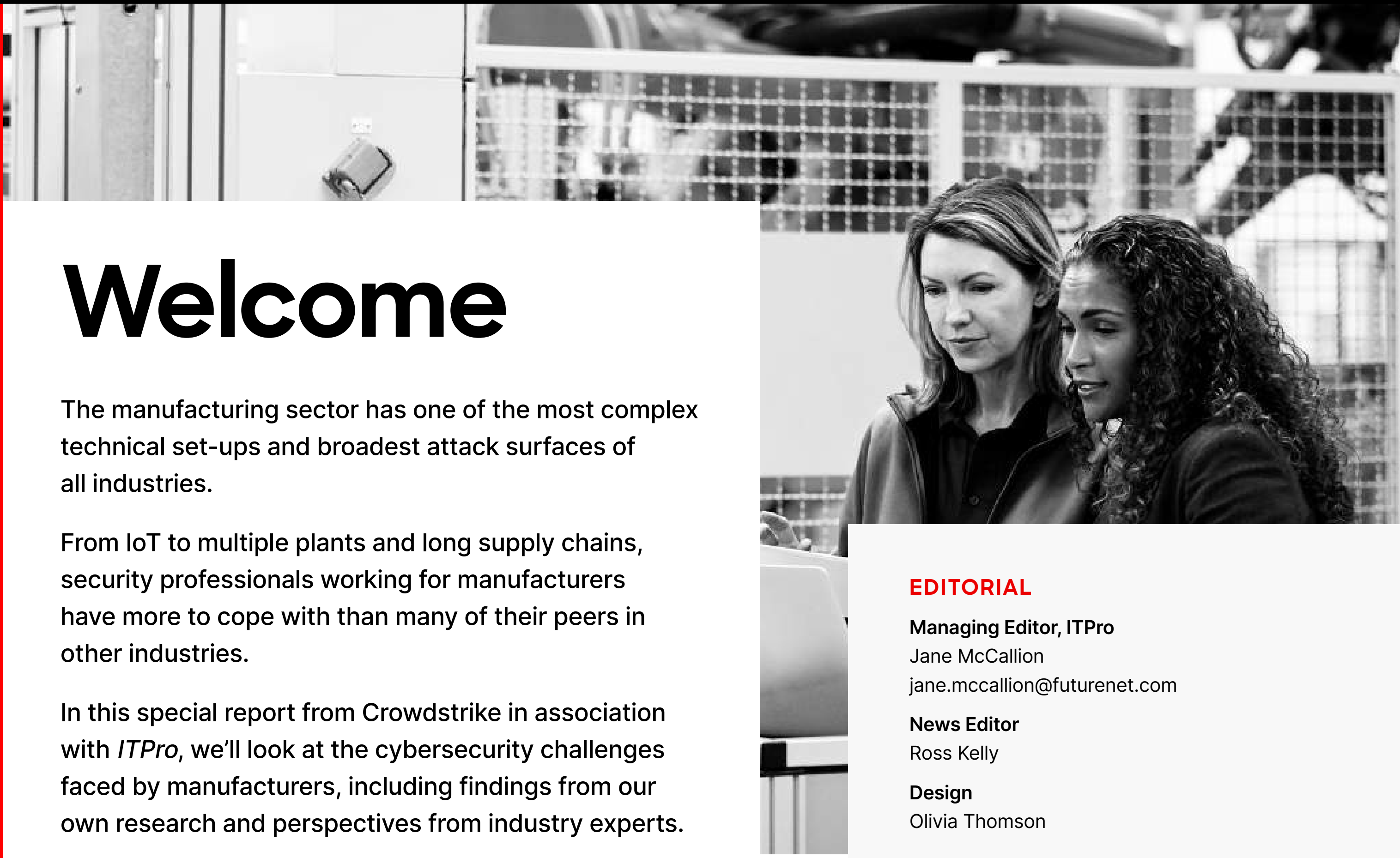
Manufacturing under siege

Navigating the complex cyber threat landscape

ITPro.
BY FUTURE B2B

in association with

CROWDSTRIKE



Welcome

The manufacturing sector has one of the most complex technical set-ups and broadest attack surfaces of all industries.

From IoT to multiple plants and long supply chains, security professionals working for manufacturers have more to cope with than many of their peers in other industries.

In this special report from Crowdstrike in association with *ITPro*, we'll look at the cybersecurity challenges faced by manufacturers, including findings from our own research and perspectives from industry experts.

Jane McCallion

Managing Editor, ITPro

Contents

EDITORIAL

Managing Editor, ITPro
Jane McCallion
jane.mccallion@futurenet.com

News Editor
Ross Kelly

Design
Olivia Thomson

ADVERTISING & REPRINTS

Global VP B2B, Tech
Amardeep Mangat
amardeep.mangat@futurenet.com

LICENSING & SYNDICATION

Licensing Team
licensing@futurenet.com

MANAGEMENT

Chief Executive
Jon Steinberg

SVP, MD, B2B
Amanda Darman-Allen

VP, Global Head of Content, B2B
Carmel King

Global Content Director, B2B IT
Maggie Holland

VP, Global Head of Strategy & Ops, B2B
Allison Markert

Head of Design, B2B
Nicole Cobban

Liability
While every care has been taken in the preparation of this magazine, the publishers cannot be held responsible for the accuracy of the information herein, or any consequence arising from it.

Does complexity have to mean insecurity?

With digital transformation projects continuing at pace in the manufacturing industry, there has never been a better time to invest in cybersecurity

A period of widespread digital transformation across the global manufacturing industry has enabled organisations to deliver marked improvements in operational efficiency and streamline production capabilities.

Over the last decade, manufacturers have increasingly shifted to the cloud, and this process was further fueled by the pandemic-era shift to remote operations, according to InfoSys' April 2024 *Cloud Radar* report.

Across 2023, two out of three respondents to InfoSys' survey said they had increased cloud spending, and a further four-in-five revealed plans to increase spending in 2024 and beyond.

This shift has precipitated rapid advancements across the manufacturing lifecycle, allowing operators to introduce automation and robotics within processes and adopt technologies such as the Internet of Things (IoT), operational technologies (OT), and artificial intelligence (AI) at scale.

The results of this shift have been profound, helping to deliver tangible business benefits. However, while widespread digital transformation has delivered positive results for manufacturers, it has also given rise to critical new considerations within a cybersecurity context.

Statistics from the World Economic Forum's (WEF) *Building a Culture of Cyber Resilience in Manufacturing* report show the sector was the most-targeted industry for three consecutive years, accounting for 25.7% of all cyber attacks globally.

The rapid digitalisation of the industry was specifically highlighted by the WEF as a key contributory factor to this increased threat level.

"Over the past decade, digital transformation has accelerated within the sector, with continuous investments in innovation and emerging technologies such as digital twins, robotics, generative artificial intelligence, cloud computing, and the Industrial Internet of Things (IIoT)," the report states.

"While this progressive digitalisation fosters growth, efficiency, and profitability, it also connects industrial and operational technologies to the digital world, exposing the sector to cyber threats."

These figures align with similar findings in CrowdStrike's 2024 *Threat Hunting Report*, which ranked the manufacturing sector as the sixth-most targeted industry globally for cyber intrusions. Notably, between July 2022 and June 2024, the number of intrusions increased by 57%.

In particular, cyber attacks against cloud infrastructure have become a leading concern for security practitioners in the manufacturing space.

CrowdStrike's 2024 *Global Threat Report*, for example, identified a growing trend of 'cloud-consciousness' among threat actors, with many now deliberately targeting cloud environments.

Cloud-consciousness, according to CrowdStrike, refers to threat actors who are aware of the lucrative opportunities that vulnerable cloud environments represent. Consequently, they abuse features and specifically target these environments.

This evolution has resulted in a 75% increase in cloud-related intrusions between 2022 and 2023, underlining the significant threats faced by manufacturers operating in the cloud.

However, cloud-based attacks aren't the only threat facing manufacturers at present. With digital transformation efforts still ongoing in the sector, operators are forced to contend with a wide array of attack vectors.

Ransomware remains a pervasive threat

As with other industries, the manufacturing sector faces surging rates of ransomware. Attacks of this kind against industrial organisations increased by nearly 50% in 2023, according to the WEF, and 71% of these were directed specifically at manufacturers.

The WEF notes that ransomware remains the "top-of-mind concern" for manufacturers, with 40% of respondents to its *Cyber Resilience in Manufacturing survey* ranking it as their leading threat.

50%

increase in ransomware attacks against industrial organisations in 2023

Indeed, industry stakeholder sentiment on manufacturing-related threats was also reflected in a survey conducted by *ITPro* on behalf of CrowdStrike.

The survey, which sought the views of 400 EMEA-based IT decision-makers in the industry in June 2024, found that nearly two-thirds (64%) of respondents believe the manufacturing sector is at “somewhat more” risk than other industries. Similarly, five per cent of respondents said the sector is at far more risk than other industries.

A slew of manufacturing organisations have been impacted by ransomware attacks in recent years, with threat actors targeting a wide range of operators including chemical production companies and car manufacturers.

The root cause of these attacks has also evolved significantly, but a common recurring theme has emerged - social engineering and phishing.

The growing threat of phishing

Social engineering and phishing attacks are often a precursor to ransomware attacks, and remain a favoured method among threat actors seeking to compromise corporate systems by preying on unwitting staff.

Manufacturing industry stakeholders are acutely aware of the threats posed by social engineering and phishing. More than one-third (34%) of respondents to the WEF’s *Cyber Resilience in Manufacturing survey* identified these techniques as their second-most prominent cyber threat, for example.

ITPro’s research also found 42% of IT leaders in the sector viewed phishing as their single greatest risk.

This trend shows no sign of slowing down either, with attackers now accelerating attempts to target workers across a wide range of industries.

42%

of IT leaders in the sector viewed phishing as their single greatest risk

With this in mind, security experts forecast that phishing will remain a potent and pervasive threat in 2024 and beyond - and the use of emerging technologies such as generative AI will play a key role in this trend.

Over the past 18 months, security researchers have issued repeated warnings about the potential to use AI tools to create more convincing email scams.

Analysis from CrowdStrike pinpointed this as a key threat for organisations moving forward, noting that AI could be used to “automate real-time communication” between the attacker and victim.

IoT attacks are mounting

The use of IoT in the manufacturing industry has grown significantly in recent years. In 2021, for example, the IoT in the manufacturing market was valued at $50 billion (€45.7 billion), and this market is forecast to continue growing in 2024 and beyond.

By 2030, it is expected to grow more than double to $129.42 billion (€118.4 billion)

The deployment of IoT within manufacturing allows organisations to gather vital data, which can then be disseminated by workers to provide detailed insights on operational efficiency and thereby optimise processes.

But although this technology has delivered benefits, it has been repeatedly identified as a potential weak spot within an organisations' broader security apparatus.

> **"One compromised organisation can lead to hundreds or thousands of follow-on targets."**
>
> — CrowdStrike's Global Threat Report

According to the WEF, IoT has created "new points of entry" and has expanded the attack surface for threat actors.

Forrester Research's *Top Trends in IoT Security 2024* report notes that a major contributory factor behind IoT vulnerability is due to the fact that the design of these products is aimed at ensuring low latency for real-time data analysis.

Concerns about the potential security risks associated with IoT were highlighted in *ITPro*'s survey of manufacturers, with one-third (37.16%) of respondents noting that IoT-related attacks represent the biggest single attack vector at their organisation.

Supply chain vulnerabilities

Supply chain vulnerabilities have been the root cause of some of the most devastating cyber attacks in recent memory.

Modern supply chains are highly complex and interconnected, meaning that threat actors who successfully compromise a third-party - or even fourth-party - vendor can wreak havoc across downstream ecosystems.

Targeting supply chain vendors essentially enables a threat actor to maximise their return on investment, CrowdStrike's *Global Threat Report* notes, as the compounding effect of an attack can be enormous.

"One compromised organisation can lead to hundreds or thousands of follow-on targets," the report states.

"These stealthy attacks can also more effectively provide an opportunity for attackers seeking to exploit a hardened end target."

Supply chain visibility is a key concern for manufacturing leaders at present, according to the WEF's *Global Cybersecurity Outlook* study. More than half (54%) of organisations "lack adequate visibility into the vulnerabilities of their supply chain", the report states.

Notably, 41% of organisations that suffered what the WEF described as a "material impact" from a cyber attack reported the breach originated from a third-party.

54%

of organisations lack adequate visibility into the vulnerabilities of their supply chain

Distributed workforce risks

Distributed workforces have become commonplace in the post-COVID era, with organisations now using a combination of remote and hybrid working practices and employing staff in a range of geographical locations.

The continuation of these practices since the waning of the pandemic has been beneficial for staff and employers alike. However, considerable risks still remain, and many organisations continue to lack the technical capabilities required to adequately protect distributed workforces.

Remote staff typically work on home Wi-Fi networks, which if left unprotected can pose a significant risk for staff and their organisations. During the widespread global shift to remote working during the onset of the COVID pandemic, remote workers faced a surge in attacks, according to 2021 analysis from EY.

Outdated work devices and vulnerable software solutions are among the key dangers for remote workforces. As such, organisations are strongly advised to maintain robust patching processes.

Best practice advice from the UK's National cybersecurity Centre (NCSC) recommends updating obsolete products on a regular basis alongside maintaining a consistent patching regime in line with vendor guidance.

How manufacturers can combat cyber threats

With this confluence of threats in mind, there are a number of ways in which organisations can protect themselves against growing cyber risks.

This typically involves a combination of harnessing emerging technologies while supporting workforce awareness. Critically, however, implementing change within an organisation to more deeply embed security awareness starts with leadership, according to the WEF.

"Effective culture change always originates from the top, which is why it is imperative for manufacturing and supply chain leaders to personally champion the necessary mindset shift and serve as exemplary role models," the *Building a Culture of Cyber Resilience in Manufacturing* report states.

So where do security leaders start?

Security culture and workforce training

Starting at a grassroots level and embedding a culture of resilience and awareness among staff will be critical for any organisation.

Staff training is vital in combating the threats posed by phishing and social engineering attacks, for example. Educating staff on how to spot the telltale signs of phishing can go a long way to bolstering basic cyber resilience.

This is critical for organisations, as CrowdStrike's 2024 *Global Threat Report* notes that while technology is crucial in the fight to detect and prevent intrusions, the "end user remains a crucial link in the chain to stop breaches."

To improve awareness, frequent training exercises should be conducted with staff across all business functions to inform them of the latest threats and techniques being employed by attackers.

"User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques," the *Global Threat Report* states.

62 minutes

average time adversaries take to compromise networks

> **"Effective culture change always originates from the top, which is why it is imperative for manufacturing and supply chain leaders to personally champion the necessary mindset shift and serve as exemplary role models."**
>
> — World Economic Forum's (WEF) Building a Culture of Cyber Resilience in Manufacturing report

Identity protection

Identity protection tools also play a key role in the fight against threat actors, according to CrowdStrike. Identity-based social engineering attacks have taken "centre stage", according to CrowdStrike, meaning organisations are strongly advised to invest in phishing-resistant multi-factor authentication (MFA) tools.

CrowdStrike's Falcon Identity Protection platform, for example, provides users with increased visibility across an organisation's hybrid identity landscape and provides "hyper-accurate" detection of identity-based threats.

In the event of an identity-based attack, Falcon works by enforcing MFA requirements for users if suspicious activity is detected.

Invest in modern SIEM solutions

With cyber attacks becoming far quicker, the need to invest in next-generation tools is critical. Adversaries take an average of 62 minutes to compromise networks and begin moving laterally through an organisation's environments, according to CrowdStrike's *Global Threat Report*.

> **"User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques."**
>
> — CrowdStrike's Global Threat Report

What's more, the report noted, that the fastest observed breakout time was just two minutes and seven seconds.

With cyber attacks now unfolding at breakneck speeds, traditional Security Information and Event Management (SIEM) solutions can prove both ineffective in combating threat actors and add needless complexity for practitioners.

These solutions were designed for an era when the volume of data organisations used was far lower, according to the *Global Threat Report*.

More modern options, such as CrowdStrike's Falcon Next-Gen SIEM, allow organisations to unify threat detection, investigation, and response within a single platform, however. This improves speed and efficiency, enabling security practitioners to keep pace with adversaries.

Generative AI

Generative AI tools have surged in popularity over the last 18 months, and now play an important role for organisations seeking to bolster their cybersecurity capabilities.

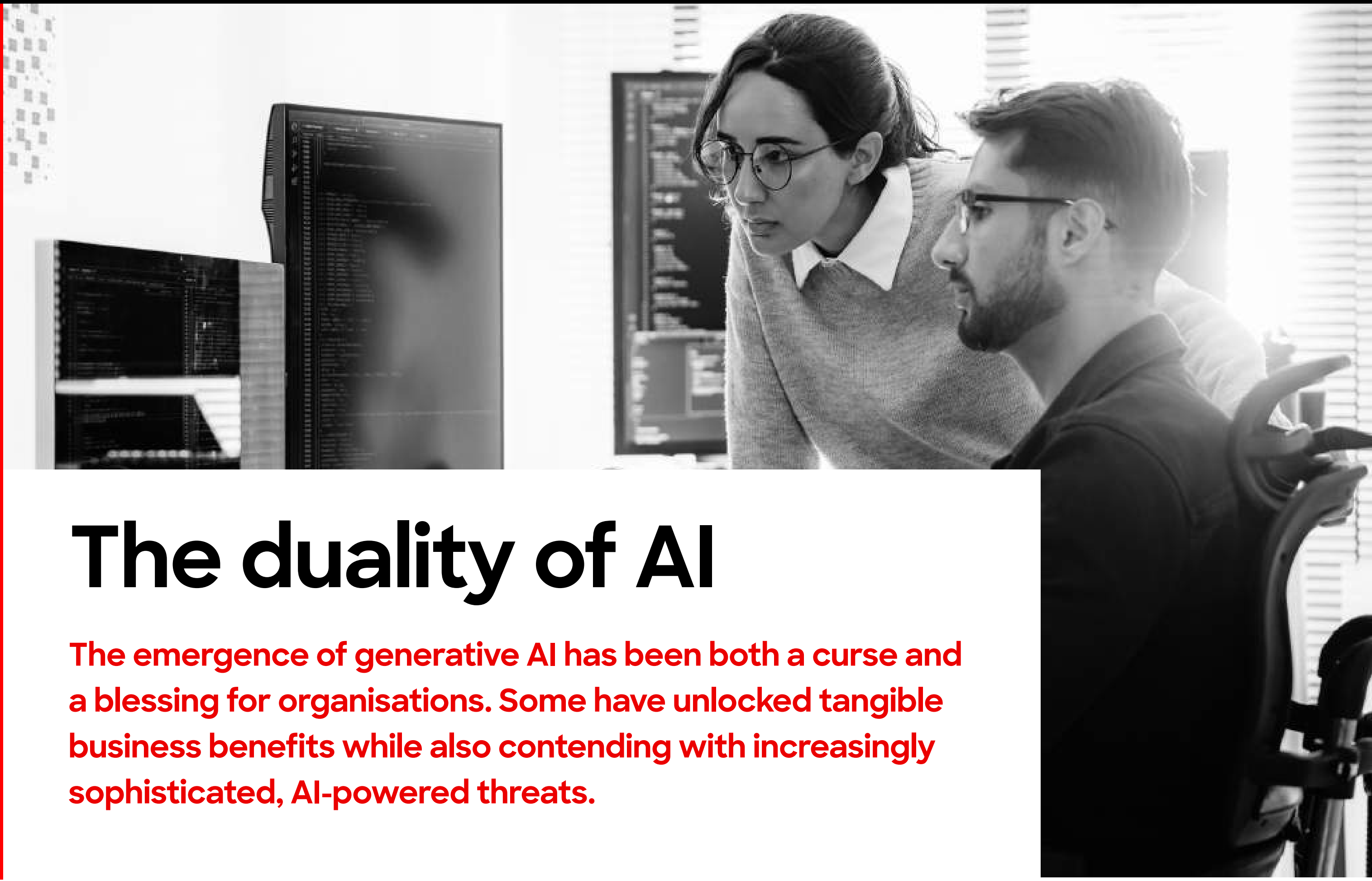
Businesses globally can now draw upon an ever-growing variety of AI-powered assistant tools specifically catered for security operations.

A host of major industry providers, including CrowdStrike, have launched powerful, intuitive AI security applications to support organisations and cyber practitioners during this period.

CrowdStrike unveiled its 'Charlotte AI' security assistant in May 2023, for example, which can be used by security personnel to support everyday tasks such as identifying and mitigating emerging threats.

But while generative AI tools are growing in popularity - especially within a security context - there are aspects of this technology that some organisations may have not considered.

Generative AI offers many opportunities, but brings with it novel risks.



The duality of AI

The emergence of generative AI has been both a curse and a blessing for organisations. Some have unlocked tangible business benefits while also contending with increasingly sophisticated, AI-powered threats.

Global interest in AI has skyrocketed in recent years, with organisations across a range of industries adopting the technology to supercharge operational efficiency and equip workers with powerful tools to boost productivity.

In the manufacturing sector, the situation is no different. With rapid technological shifts ongoing in the industry, AI represents a prime opportunity to further enhance long-running digital transformation efforts.

Research from McKinsey in 2020, for example, found that AI could markedly improve both efficiency and production quality. But with the emergence of generative AI in late 2022, a new wave of activity has flourished.

Statistics from IDC's 2023 *GenAI Awareness, Readiness, and Commitment (ARC) Survey* showed manufacturing organisations across Europe were actively evaluating or implementing generative AI solutions.

Around 30% of respondents said they had already invested heavily in the technology and were in the process of allocating budgets for training, the acquisition of generative AI tools, and potential consultancy work.

> **The rise of generative AI "has the potential to lower the barrier of entry for low-skilled adversaries."**
>
> — CrowdStrike's Global Threat Report

Moreover, around 20% said they had already begun initial testing of AI models to support operations and were building proofs of concept.

In the UK, meanwhile, the appetite for generative AI solutions is fierce. According to the *2024 State of Smart Manufacturing* report from Rockwell Automation, more than three-quarters (79%) of UK manufacturers expect to use generative AI in their operations in the coming year.

Notably, 88% of respondents said they have already invested in AI initiatives, or plan to do so within the next 12 months.

AI in manufacturing brings risks as well as opportunities

As with any emerging technology, heightened expectations are being tempered by the additional risks it may bring - and there are notable security concerns related to generative AI. Security experts have flagged repeated warnings over the potential misuse of the technology by threat actors in recent months.

Research from the UK's National cybersecurity Centre (NCSC) in January 2024 warned AI will "almost certainly increase the volume and heighten the impact of cyber attacks" and that state-affiliated groups are "already using AI to various degrees" within their operations.

An equally worrying development in this regard is the fact that generative AI is helping enable lower-skilled threat actors. This aligns closely with the findings of CrowdStrike's 2024 *Global Threat Report*, which noted that the rise of generative AI "has the potential to lower the barrier of entry for low-skilled adversaries" and make it easier to wage more state-of-the-art attacks.

This means that lower-level bad actors, in addition to more established and proficient cyber criminals, can use these tools to conduct attacks.

88%

of respondents said they have already invested in AI initiatives, or plan to do so within the next 12 months.

New threats for the manufacturing sector

The manufacturing sector has faced escalating threats for several years now, largely owing to the critical role it plays within the global economy. Research from Netwrix in January 2024, for example, found that nearly two-thirds (64%) of operators in the industry suffered a cyber attack in 2023.

In one incident in February 2024, a German battery manufacturer fell victim to an attack that resulted in production halts at five plants for over two weeks.

These incidents - and the disastrous impact - offer just a snapshot of the dangers manufacturers currently face. Escalating attacks, combined with the growing use of generative AI among threat actors, means the manufacturing sector faces major challenges moving forward with regard to cybersecurity.

Industry stakeholders are frightfully aware of this reality. Indeed, in *ITPro*'s survey of 400 IT leaders from the sector, 40% of respondents noted that generative AI was the single greatest risk to their organisation when it comes to potential vectors of attack.

But where exactly is generative AI having an impact in terms of cyber risks? At present, the landscape varies, but key common themes are emerging.

AI and the rise of phishing

Phishing attacks have long been the bane of organisations globally. Nearly half (43%) of leaders in the manufacturing sector told *ITPro* that phishing and vishing attacks are the greatest risk posed to their organisation.

The goal of any social engineering attack is to dupe the unsuspecting victim in a bid to have them divulge sensitive information that may support a broader attack. This can include login details, for example, which might aid an attacker in gaining access to corporate networks or systems. Similarly, many social engineering attacks aim to trick victims into installing malicious files on work devices, thereby offering another avenue of entry to an organisation's networks.

43%

of leaders in the manufacturing sector said that phishing and vishing attacks are the greatest risk posed to their organisation

With the advent of generative AI, threat actors have identified a prime opportunity to ramp up their efforts. The use of the technology is enabling them to fine-tune their techniques and create more convincing scam emails. The NCSC specifically highlighted this concern in its advisory earlier this year.

"Generative AI and large language models will make it difficult for everyone, regardless of their level of cybersecurity understanding, to assess whether an email or password reset request is genuine, or to identify phishing, spoofing or social engineering attempts," the agency warned.

AI poses significant vishing challenges

Similar to the rise of AI-powered phishing threats, research shows that the technology could also be used to conduct highly sophisticated vishing – or voice-based – attacks.

Generative AI tools have already been used to create highly convincing 'deepfake' content for disinformation campaigns globally, as well as cyber attacks.

A deepfake is a type of AI-generated content, spanning video, images, or audio, that is used to deceive people. In a cybersecurity context, threat actors could use deepfake video footage to manipulate employees.

This form of attack has already been used successfully in the wild by threat actors to devastating consequences. In February 2024, a financial services institution in Hong Kong, for example, was targeted in a social engineering attack in which threat actors mimicked company directors to steal more than $25 million (€22.38 million). While this incident focused on a financial services firm, the lessons learned are just as relevant to the manufacturing industry.

In this particular incident, the worker in question was manipulated into attending a video conference call with individuals they believed to be colleagues. It later transpired that they were threat actors using deepfake recreations.

Using AI for voice cloning has also been highlighted as a major threat by industry experts over the last year. In late 2023, ENISA, the EU's cyber agency, issued a warning about an expected surge in AI-generated content in its *Threat Landscape* report.

While this alert focused predominantly on the use of AI-generated content in election misinformation, it followed a similar advisory from the US Federal Trade Commission (FTC) which warned of an expected rise in AI-generated voice cloning attacks against enterprises.

In these scenarios, an attacker could potentially use audio of a colleague or senior member of staff to create a convincing recreation and instruct an individual to change passwords, grant access to systems, or, as in the Hong Kong incident, transfer funds.

> **"Generative AI and large language models will make it difficult for everyone, regardless of their level of cybersecurity understanding, to assess whether an email or password reset request is genuine, or to identify phishing, spoofing or social engineering attempts."**
>
> — NCSC

Harnessing AI to combat emerging threats

While generative AI can be used by threat actors to wage increasingly sophisticated and devastating attacks, the technology is also being used for good purposes among manufacturers.

Generative AI use cases in the sector vary, however, ITPro's polling shows the technology's use is growing in a wide array of functions.

Some 60% of respondents said they use generative AI to conduct natural language processing for log analysis, for example, while a similar number use the technology in automated response and remediation.

Manufacturers are also using generative AI to bolster predictive analytics for risk assessment, with 51% employing the technology for this purpose.

As previously mentioned, the emergence of generative AI has given rise to a range of AI-powered security tools, with several major providers globally launching their own AI 'assistants'.

These tools offer a helping hand to cybersecurity practitioners when it comes to reducing workloads, streamlining processes, and monitoring and detecting threats.

Reducing repetitive manual tasks in daily workflows has been an area of particular excitement for practitioners and businesses alike, enabling security staff to focus more attention on preventing threats instead of administrative tasks.

Although AI does represent an opportunity for threat actors to capitalise on an emerging technology for nefarious purposes, organisations capable of investing in the technology for security purposes can fight fire with fire.

What next for security in manufacturing?

Poorly aligned business functions and lucrative opportunities for threat actors place manufacturers at risk – but there is light on the horizon

While the manufacturing sector has evolved significantly in recent years from a technology perspective, these advances have been mirrored by an increasingly perilous threat landscape.

Operators in the sector now face an ever-growing array of devastating attack methods waged by highly proficient cyber criminal groups. Ransomware is still pervasive and social engineering-based threats such as phishing and vishing, fuelled by the nefarious use of generative AI tools, pose a serious danger to practitioners globally.

While these threats affect all industries, the risks encountered by operators in manufacturing specifically are rising at pace. As previously mentioned, the manufacturing industry was the most-targeted sector by volume of attacks for three concurrent years, according to the WEF.

Concerns over this reality were made clear by industry stakeholders in *ITPro*'s survey of IT leaders in the space, with nearly two-thirds (64%) of respondents noting the sector faces distinct challenges with regard to security.

Zeki Turedi, CTO for EMEA at CrowdStrike, tells *ITPro* the industry is a "really unique space", making it a prime target. It boasts a plethora of organisations that play a critical role in keeping the world running efficiently, producing goods and components that are central to the global economy.

"They're typically manufacturing goods that need to be delivered pretty efficiently," he says. "Or they're trying to actually dominate a market where they're making sure that the products they're building are able to get to their suppliers, end users, and customers as quickly as possible."

"This is all known to the criminal actor. Basically what it says is, if we disrupt your organisation, we know that it is going to cost your business quite a lot of money," Turedi adds. "And it is probably going to be cheaper and more affordable for you just to pay the ransom and get your business operating again than having loss of profit or having to pay fines for missing contracts and so forth."

Cyber crime is a costly business

The cost of cyber crime has risen by 125% per year, on average, according to the WEF. Successful attacks in industrial settings, for example, now stand at an average cost of $4.73 million (€4.3 million) per attack.

Costs associated with cyber attacks are also expected to rise in the coming years, the WEF study found, and are projected to cost $10.5 trillion (€9.4 trillion) globally by 2025, further underlining the disastrous financial consequences of cyber crime.

125%

increase in global cost of cyber attacks

€4.3M

Average cost of a data breach in industrial settings

€9.4T

Projected costs of cyber attacks globally by 2025

(SOURCE: WORLD ECONOMIC FORUM)

Fundamentally, Turedi says, cyber criminals understand that if they can successfully disrupt a manufacturer's operations, they can cause havoc downstream. This, in their estimation, could land them an easy pay-out.

Turedi warns that manufacturers aren't only faced with financially-motivated cyber criminal groups, however. Sophisticated state-sponsored groups are also accelerating attempts to target the sector in a bid to steal valuable intellectual property (IP).

"We've also got to realise that the majority of manufacturing organisations have intellectual property," he explains. "They're manufacturing something either themselves or on behalf of someone else, and they're using information that is probably going to be the secret sauce, the USP, of an organisation – and that IP could also be worth a lot of money to someone else."

"That is a second element that criminal organisations are interested in, so they can get access to that information and threaten to get that ransom. But also we see a keen interest in nation states who don't want to fund the research and development into IP, they'd rather steal it," Turedi adds.

"We've seen that for numerous years through a number of organisations and countries."

Converging business functions creates significant challenges

The manufacturing sector is "extremely complex", Turedi notes, both in terms of global supply chains and the technologies that are used in day-to-day operations.

The use of IoT in the industry has become commonplace over the past few years while investment in operational technology (OT) has also ramped up.

Operational technology (OT) interfaces with the real world, and in a manufacturing context, includes software and hardware used to monitor and maintain industrial control systems and equipment.

Much like IoT, the use of OT has enabled manufacturers to both automate aspects of their processes while gaining detailed insights on operational efficiency.

While this has delivered benefits for operators, it has also opened new avenues of attack for adversaries, according to Turedi, and presents new, highly complex considerations for manufacturers.

“Most businesses will have IT that operates their business. But on the manufacturing side, you [also] have operational technology,” he explains. “These could be human management interfaces (HMIs), sensors, or even robots. These components are being powered by huge amounts of technology that may eventually be something that is very similar to an IT computer, but has lots of activity around it.”

“Complexity can’t be updated. Maybe it is running out of date software because the platform was built 10 years ago, and you can’t touch it because it was built specifically for that version of the operating system and those components,” Turedi continues. “A lot of the IT threats that the IT security teams have been dealing with for some time are starting to leak out the OT side.”

> **“That complexity means that there are a multitude of ways that threat actors can target a manufacturing organisation.”**
>
> — Zeki Turedi, CTO for EMEA at CrowdStrike

57%

of cyber attacks on OT in 2022 had physical consequences

ITPro’s poll of manufacturing leaders also specifically highlighted IoT-related threats as a leading cybersecurity concern.

Attacks against OT and IoT often have significant real-world implications, according to research from the WEF. More than half (57%) of cyber attacks on OT in 2022 had “physical consequences”.

This included interruption of production processes, for example, as well as industrial equipment damage. Notably, the WEF found that these incidents put workers at risk of physical harm.

Turedi emphasises that this confluence of OT and IT now poses a significant challenge for manufacturers seeking to bolster their cybersecurity capabilities and, ultimately, creates a larger attack surface for threat actors to target. The blind spots between these two functions essentially provide ample opportunity to wreak havoc.

"That complexity means that there are a multitude of ways that threat actors can target a manufacturing organisation. It all comes down to the sophistication of the adversary. So of course for the everyday threat actor, maybe they'll be targeting it through ransomware," he says.

"We've also seen threat actors taking more custom approaches, specifically targeting manufacturing," Turedi adds. "But on top of that, what we're starting to see is a huge increase in what we call 'living off the land'."

This refers to using legitimate tools already installed on a computer for malicious activities.

"We've seen a pretty steady increase of this going on year on year, and now that is predominantly what we see."

'Living off the land' attacks have become a key concern for cybersecurity agencies on both sides of the Atlantic in recent months. In February 2024, the UK's National cybersecurity Centre (NCSC), along with its Five Eyes Alliance issued a new warning to critical infrastructure operators about these techniques.

In particular, Five Eyes warned that state-sponsored attackers from China and Russia had been observed using this technique on compromised critical infrastructure networks.

Boosting collaboration to tackle cross contamination

With the growing risk of OT threats spilling over into IT – and vice versa – organisations must improve collaboration to prevent cross-contamination, Turedi says.

Best practices and processes from the OT side of the business should be shared with the IT department, he adds. Likewise, there are elements of IT best practice that could be beneficial to OT teams. This, he adds, "provides a great opportunity to make those organisations stronger".

"There's definitely a separation between your IoT, and IT space," he says. "What we are seeing at a lot of manufacturing organisations, specifically with cybersecurity, is about trying to make those teams work cohesively together, rather than being completely separated."

"It provides a great opportunity to share intelligence and share knowledge. But we also have to remember that with OT, just because it is running on a device that looks like a computer, the way it is manufactured and maintained and managed is very different."

Regulatory considerations and industry standards

Manufacturers already adhere to a host of industry standards, including the ISA/IEC 62443 series of standards, for example. These outline requirements and processes for maintaining secure industrial automation and control systems (IACS), and are regarded as best practice for improving security performance.

Additional global regulatory frameworks mean the stakes have never been higher for manufacturers when it comes to cybersecurity. Regulatory guidelines on both sides of the Atlantic place strict requirements on manufacturers to ensure robust security practices.

These include the EU's Cyber Resilience Act (CRA), for example. Non-compliance with the CRA can include sizable fines of up to €15 million ($16.76 million), or 2.5% of worldwide sales.

Given the critical role of the manufacturing industry, the EU's Directive of Resilience of Critical Entities (CER) is also a key piece of legislation on the minds of IT leaders in the space.

The directive aims to bolster the resilience of critical infrastructure entities against emerging threats, both physical and virtual, including sabotage, insider threats, and natural hazards. This entered into force in January 2023, and member states have until 17 October 2024 to adopt new legislation to accommodate for the regulations.

Perhaps among the most critical EU regulations for manufacturers is the NIS2 Directive.

This is a revision of the union's original Network and Information Systems (NIS) Directive, and aims to tighten cybersecurity requirements and standards across a host of sectors, including manufacturing.

Under NIS2, manufacturing is designated as an 'important entity' due to its proximity to critical infrastructure. This will require operators in the sector to place a stronger focus on supply chain security capabilities, as well as increased collaboration with IT providers to drive proactive security improvements within hardware and software.

The updates to NIS2 are just one of several regulatory frameworks manufacturers must consider, which the WEF notes creates challenges for organisations with regard to compliance.

"The decentralised operational environment and fragmented and diverse local, regional, and industry specific regulatory landscapes add another layer of complexity to cybersecurity efforts," the WEF states in its *Building a Culture of Cyber Resilience in Manufacturing* report.

> **"The decentralised operational environment and fragmented and diverse local, regional, and industry specific regulatory landscapes add another layer of complexity to cybersecurity efforts."**
>
> — World Economic Forum's (WEF) Building a Culture of Cyber Resilience in Manufacturing report

Despite these challenges, Turedi expects NIS2 to ultimately have a positive impact on the sector, noting that this represents "quite an overhaul in terms of cyber regulation and compliance".

"I think NIS2 regulations are fantastic. First of all, if you're an organisation that takes cybersecurity seriously, NIS2 is not going to come after you," he says. "It makes organisations aware - that may have not been already - that cybersecurity is important to their business."

Compliance with US regulations will also be front and centre for IT leaders in the manufacturing sector moving forward. In February 2024, the US government's National Institute of Standards and Technology (NIST) unveiled a major update to its cybersecurity Framework (CSF).

CSF 2.0 will provide a voluntary framework for manufacturers aimed at enabling them to enhance their cybersecurity capabilities.

Tackling future threats with AI

Contending with an array of new, increasingly sophisticated threats, requires an equally potent kit of tools to support cybersecurity practitioners. As mentioned previously, generative AI poses a prime opportunity for manufacturers to equip themselves with industry-leading capabilities.

Since the technology emerged in late 2022 with the release of OpenAI's ChatGPT, various notable use cases have been identified for its use in the enterprise. One of the most popular and widely applicable uses is software designed to improve worker productivity.

In cybersecurity, the same advantages are being unlocked for frontline staff, with powerful new tools helping to alleviate the pressure of daily tasks.

Turedi believes that generative AI represents a "great opportunity" for security teams not only in terms of arming them with tools to contend with threats, but also to help create a more aligned company-wide cybersecurity strategy.

Simply put, AI can help fill the skills gaps in respective functions, which given long-standing issues on OT and IT alignment, could prove vital for manufacturers.

> **"I see AI as being a great opportunity to help these teams to be more cohesive, and help the automation of workflows."**
>
> — Zeki Turedi, CTO for EMEA at CrowdStrike

"I see AI as being a great opportunity to help these teams to be more cohesive, and help the automation of workflows," he says.

"An example of where we forget artificial intelligence and cybersecurity can be really helpful is in the case of an OT team member, who understands the OT environment and its nuances really well, but they may not be a cybersecurity expert.

"Generative AI allows us to take the knowledge of cybersecurity and embed it into other teams that maybe don't use every single day. It can then provide recommendations on what they should do next, or surface other pieces of information to allow them to make good decisions on next stages and steps as part of their response cycle."

The benefits of AI often focus on productivity and finances, he notes, but using this technology as a tool to upskill and "passively educate" all staff to improve security alignment is where he sees long-term value.

What manufacturing gets right with cybersecurity

Focusing largely on the potential dangers faced by the manufacturing industry is vital, Turedi notes. However, acknowledging what the industry does right is equally important from both a morale and leadership perspective.

There are key areas in which the manufacturing sector excels, he believes, especially with regard to transparency, incident reporting, and its eagerness to learn from mistakes and engage in knowledge exchange with peers.

“We’ve seen over the last few years a number of manufacturing organisations that have unfortunately found themselves to have been victims,” Turedi says. “And again, publicly released information about their losses.”

This proactive, communicative culture should be applauded, Turedi believes, and is one that separates the industry from others. Organisations in other sectors, he says, can often be reluctant to reveal too many details in the wake of a cyber incident.

But this does little to help counterparts within their respective sectors, and even has a detrimental effect on their ability to counter future threats. In the modern threat landscape, information sharing is critical.

“That is great data that allows other manufacturing organisations to take that information, help them invest correctly in cybersecurity, and provide the right data to show the return on investment, show what bad could look like, and use that evidence to be able to make sure that you invest in cybersecurity,” he explains.

“It is quite unique, because if you’re looking at other sectors, some don’t over communicate this information, or the fact that these organisations have been breached is hidden rather than being public.

“That can be really hard for a sector that actually has been targeted, to be able to raise awareness and be able to properly articulate [the importance of investing in cybersecurity] to their management, their teams, and their board.”

Q&A: The unique role of security in manufacturing

Zeki Turedi, CTO for EMEA at CrowdStrike, explains the role of AI and NIS2 in defending manufacturers from cyber attacks

What are the biggest cybersecurity challenges facing companies in general right now?

There are a lot. From a technical perspective, we're seeing a huge increase in the cloud being targeted. Many organisations rushed to migrate their old on-premise systems into the cloud and security often wasn't enabled as part of that process; it was an afterthought. The cloud is fantastic and can actually be great for security, but if it is not built into the process you're going to be vulnerable.

We also see threat actors evolving; they have become more sophisticated and highly persistent, whereby we have seen them heavily investing in new ways to target organisations. Identity is a leading threat facing organisations, for example.

Whether they get credentials through social engineering or find them on the dark web, they will use them to try and masquerade as legitimate users to get into the organisation. There are many ways, unfortunately, that organisations can fall foul of that and we've seen the threat actor become even quicker than before.

Are there any unique challenges faced by the manufacturing sector, for example around IoT and operational technology?

Yes. This is due to the complex role both IoT and OT play in technology architecture, which is reflected in the threat landscape as well.

On top of that, there is a very complex environment they have to manage. Manufacturers in some cases may operate their own factories, some of which will be new, some will be old. Some factories, however, may be rented, so it could be their own equipment or someone else's. This is a very difficult security landscape for someone trying to look after a network. Additionally, you may have to interconnect into an organisation that you know has fewer security capabilities, but they have a unique tool that allows you to manufacture in small amounts of time. These are huge risks to manufacturing.

Is this a global issue or are there certain regions where there are heightened levels of threat?

We definitely do see a lot more threats and threat actors directly targeting European and North American companies by volume, but in all honesty, they are after everyone.

We have to remember that while we tend to focus on the ones that cause the most damage or go for the largest ransom, there is a threat actor for everyone. This could include a threat actor targeting small organisations, threat actors targeting specific countries, anyone.

NIS2 – the EU's latest cybersecurity regulation – is coming into force in October 2024. What impact is that going to have on businesses?

If you're an organisation that takes security seriously and you are doing the best you can do with cybersecurity, NIS2 isn't going to come after you. It is about those that aren't investing in cybersecurity and I think that is really important to understand.

It really makes many organisations aware that cybersecurity is important and crucial to your business. If you're not implementing it and taking it seriously, this is a perfect reason to change that.

If you're a business that already has a cybersecurity program, you're taking it seriously, it is important to you. If you have a CISO, you're reporting to the board about events and incidents, and you have a security partner like CrowdStrike, you're going to be in a very good place for NIS2.

How is AI shaping the cybersecurity landscape, both offensively and defensively?

We have to remember the cybersecurity industry has been using AI for the last 10 to 15 years. AI is fantastic at identifying malicious activities and malware at scale, whereby a lot of security organisations, like CrowdStrike, built their platforms on AI. We've been doing this for a lot longer than the adversary. I think generative AI opens a whole new angle, such as being able to use AI to support the analyst, help them automate as many tasks as possible, and make that interaction with technology as simple as possible. That could even support upskilling and cross-skilling, but also just being able to keep up with the sheer amount of intelligence that organisations see today.

On the other hand, if we have a keen interest in this, the threat actors do as well. We know they want to better themselves and are investing in themselves. Indeed, we have seen chatter in hacker forums about how AI can be used.

We have to remember that the technology available to the defender is also potentially available to the malicious actor. Generative AI can be used to create scripts that can be fantastic for an incident responder, but it can also be used to create a script that can be used by a malicious actor to extract sensitive information rapidly. So we have to make sure we know how these tools that are available can be used maliciously, and make sure we can protect ourselves from being targeted.

What impact will an increase in organisations' use of AI in cybersecurity have on security teams?

I'm a big believer that these AI tools are here to augment, not replace. We have to remember that these AI tools are fantastic, but they are trained. They still have to be taught the difference between good and bad, between what's a real incident versus noise. We can't remove the human from the loop. There is going to be a lot of important information about your business that you can't use to train generative AI, such as really important knowledge that is shared between people, but which isn't correctly documented. That information is necessary and is what you need when dealing with a real incident quickly.

If we've seen an incident before, we've gone through the investigations, and that is something that ends up repeating itself frequently, that is going to be monotonous work that we don't need an analyst for. We want them to focus on what they can do best – the nuance, the input that is very unique. Let the technology take over and deal with that noise, deal with that scale for the human analyst.

> **"These AI tools are fantastic, but they are trained. They still have to be taught the difference between good and bad, between what's a real incident versus noise. We can't remove the human from the loop."**
>
> — Zeki Turedi, CTO for EMEA at CrowdStrike

My biggest worry when we start focusing on replacing the human out of security is we have an opportunity to miss stuff that is important or classify things incorrectly. And we can't have that fault in cybersecurity.

Do you have any advice for IT professionals in manufacturing specifically who are keen to enhance or bolster their security with AI?

A really good example would be, even if you're in the UK and don't even have to comply with NIS2, look at it anyway. It is an important baseline benchmark that all manufacturing organisations should be focusing on, as well as a really good framework to focus on building good security in their businesses.