Securing your future:

Protecting operational infrastructure during digital transformation.

verizon business

Securing your future:

Innovating fast while staying secure can feel like a tightrope walk.
Here’s what you need to know to move your business forward without falling.

The greatest opportunities in business are often accompanied by the greatest risks. Digitalisation is a perfect example.

On one side, digital transformation can enhance efficiency, improve product quality, elevate customer experiences and boost operational resilience. On the other, digitalisation can introduce unintended cybersecurity risks—particularly within the operational technologies (OT) so critical to production.

OT security is a vital consideration for a wide array of industries, including manufacturing, oil and gas, utilities, transportation, and more. It's essential to the critical infrastructure we all rely on. And to your business's profits.

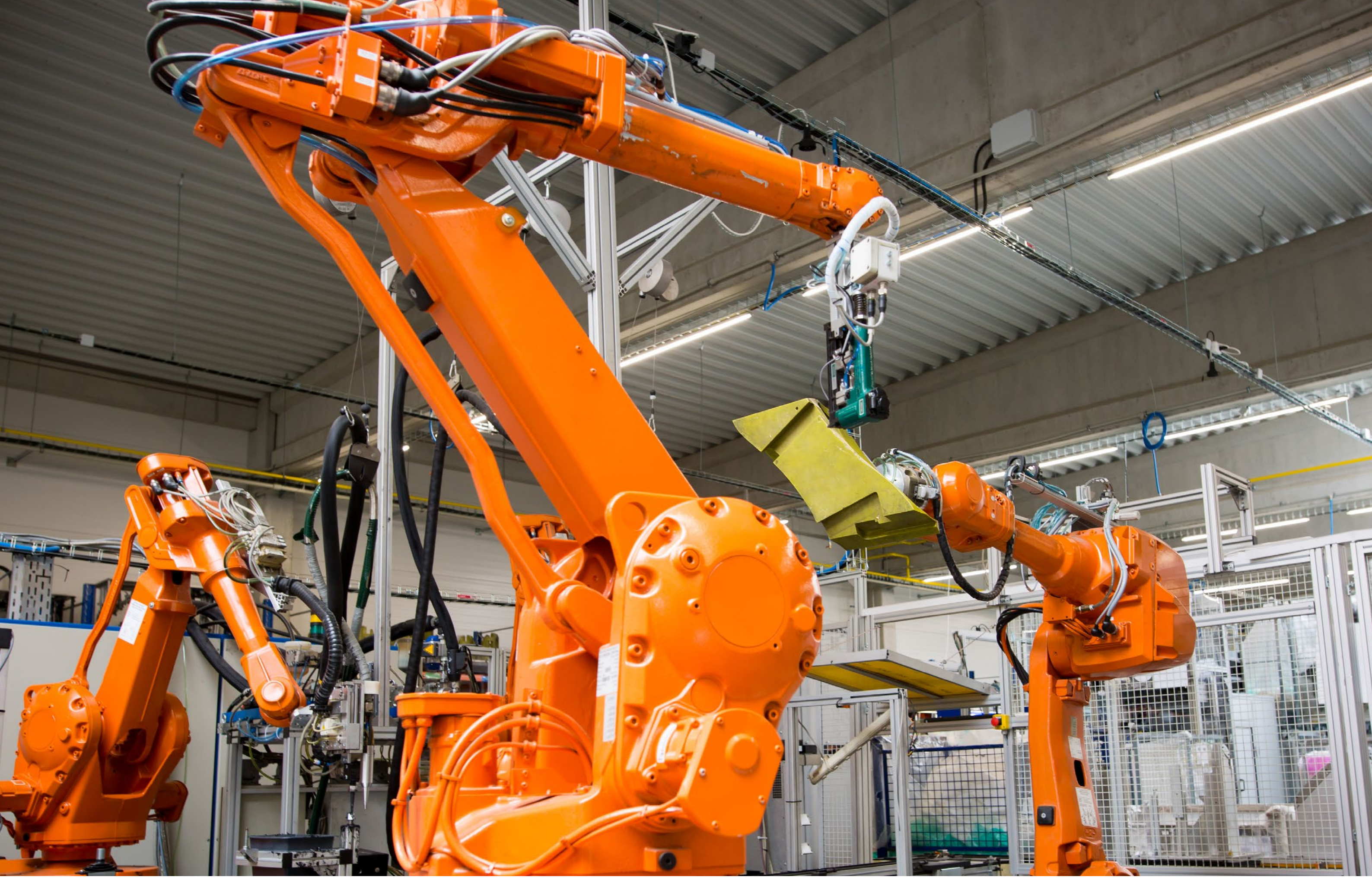
Thankfully, many of the key lessons we can learn from one industry's digitalisation can be applied to others. That means you don't have to put your business at unnecessary risk while innovating.

That's not to underplay the challenge here. Cybersecurity threats facing manufacturing businesses are very real, but here we'll focus on the positive, practical steps you can take to safeguard OT, while reaping the rewards of digitalisation.

If you're aware of the issues around OT security, then you can tackle them. And that's exactly what Verizon is here to help you do: Protect and thrive.

Take a holistic approach to cybersecurity with Verizon.

Verizon's comprehensive IT and OT security solutions are already trusted by thousands of businesses around the world. Our holistic approach to cybersecurity centres on your business's needs, budgets and digital transformation goals.



The digital transformation imperative.

There's no doubt that, if you're reading this, digital transformation is high on your agenda, as it is for most other manufacturers. The pace of change in this sector has been accelerating since the concept of "Manufacturing 4.0" entered the mainstream.

> Digital transformation can lead to substantial gains in throughput, potentially ranging from 10% to 30%.
>
> Source: McKinsey & Company, Preparing for the next normal via digital manufacturing's scaling potential, 2020

The truth is that our interconnected world demands supply chains be resilient, agile and optimised – and that means digitalising, fast. Technologies like the industrial Internet of things (IIoT) and artificial intelligence (AI) have quickly become industry essentials. Together, they promise the transparency and coordination needed to proactively manage inventory, improve production efficiency and mitigate against system failures. Digital integration also extends to the realm of customer engagement, unlocking the real-time insights and personalisation necessary to enhance satisfaction and strengthen loyalty.

Beyond operational efficiencies, digitalisation can help to manage external pressures. Geopolitical instability and labour shortages necessitate flexible, digitally enabled operations that can adapt to changing demands. Digitalisation can also enable better environmental monitoring, energy optimisation and regulatory compliance, aligning with both consumer expectations and operational imperatives.

But transformation doesn't have to be a cost-centre. Digitalising can drive significant cost reductions through improved efficiency gained by waste minimisation and predictive maintenance. Digitalisation of your workflows and processes can also generate more data insights for your organisation to capitalise on. This can enable more informed decision-making, enhancing your ability to respond effectively to market fluctuations, regulatory changes and unforeseen disruptions. At a time of immense change, that's more important than ever.

Your business must be mindful, however, of opening unintended vulnerabilities as your operations evolve.

The threat landscape is becoming more complex.

The increasing application of digital technologies hasn't just opened the door to revolutionary improvements. It has also, unfortunately, expanded the potential avenues for cyberattacks.

The integration of information technology (IT) systems with previously isolated OT environments, coupled with the proliferation of connected IIoT devices and AI, has significantly broadened the attack surface that must be defended.

OT systems, for example, often rely on legacy communication protocols that modern security technologies don't necessarily support. Many OT devices could have unpatched vulnerabilities and lack the robust security features common in contemporary IT systems. Furthermore, the extended operational lifespans of OT equipment mean that they may be running outdated software and firmware for longer, creating further security gaps.

> The integration of IT systems with previously isolated OT environments ... has significantly broadened the attack surface that must be defended.

The arrival of AI creates a new vector for attack, potentially exposing isolated OT equipment and sensitive data to the wider world – as well as a wide array of non-human actors. This is, at the very least, creating a more complex identity management environment.

As you train and use AI tools, new security capabilities and practices may be needed to protect your infrastructure from intrusion and your data from misuse. Data sovereignty will be a key consideration as businesses like yours balance the need to generate, prepare, process and store data across diverse locations. Protecting intellectual property and personal information from data-hungry AI tools must be a priority.

Being unprepared can be costly.

Cybercriminals know that manufacturers have a low tolerance for operational downtime. They also know there is considerable value in your business's intellectual property. It's perhaps no surprise that system intrusion attacks in the manufacturing sector saw stark rises over 2025, with reported breaches almost doubling from 2024 (as reported in Verizon's 2025 Data Breach Investigations Report).

- **Phishing and social engineering** are employed to deceive employees into divulging sensitive information or performing malicious actions, often targeting individuals with access to both IT and OT networks.
- **Supply chain attacks** exploit vulnerabilities in the complex network of suppliers and partners.
- **Industrial control systems (ICS)** attacks represent sophisticated threats specifically aimed at disrupting critical infrastructure and industrial operations.
- **Zero-day attacks** exploit previously unknown vulnerabilities in technology and represent a persistent and evolving danger.
- **Unmanaged and unsecured IoT devices** within production environments can also serve as entry points for cyber threats.

“

> System intrusion attacks in the manufacturing sector saw stark rises over 2025, which contributed to reported breaches almost doubling from 2024.
>
> Source: Verizon, 2025 Data Breach Investigations Report

In addition to the financial cost, attacks can cause substantial disruption to production, compromise valuable intellectual property and sensitive data, damage physical assets, and impact compliance. In critical infrastructure sectors, such attacks can even pose direct threats to public safety.

Addressing these cybersecurity challenges is often complicated by several factors. Maintaining accurate and up-to-date inventories of the rapidly growing number of OT and IIoT devices can be a significant hurdle. There's also a relative lack of specific threat intelligence focused on OT and IIoT infrastructure attacks compared to the IT domain. A fundamental difference in priorities and culture between IT and industrial environments can impede the effective implementation of cybersecurity measures in OT.

If your business is aiming to bring IT and OT closer together as part of its digital transformation, it needs to also align its security practices.

Addressing the challenges for global manufacturers.

Manufacturers often operate with intricate and geographically dispersed IT and OT environments. These complex systems include a mix of modern and legacy technologies, as well as a vast array of interconnected devices, creating significant challenges for security management.

The sheer scale of these operations demand a sophisticated and unified approach to cybersecurity.

Historically segmented networks and operational cultures now need to be integrated. Overcoming the inherent cultural and operational gaps between IT and OT teams is crucial for establishing a cohesive security posture.

Manufacturers also rely on intricate and often lengthy supply chains. The interconnected nature of these global supply networks means that a security breach at any point in the chain can create a cascade of unwelcome consequences across the entire operation. Manufacturers must ensure all their suppliers operate within strict security policies to limit exposure.

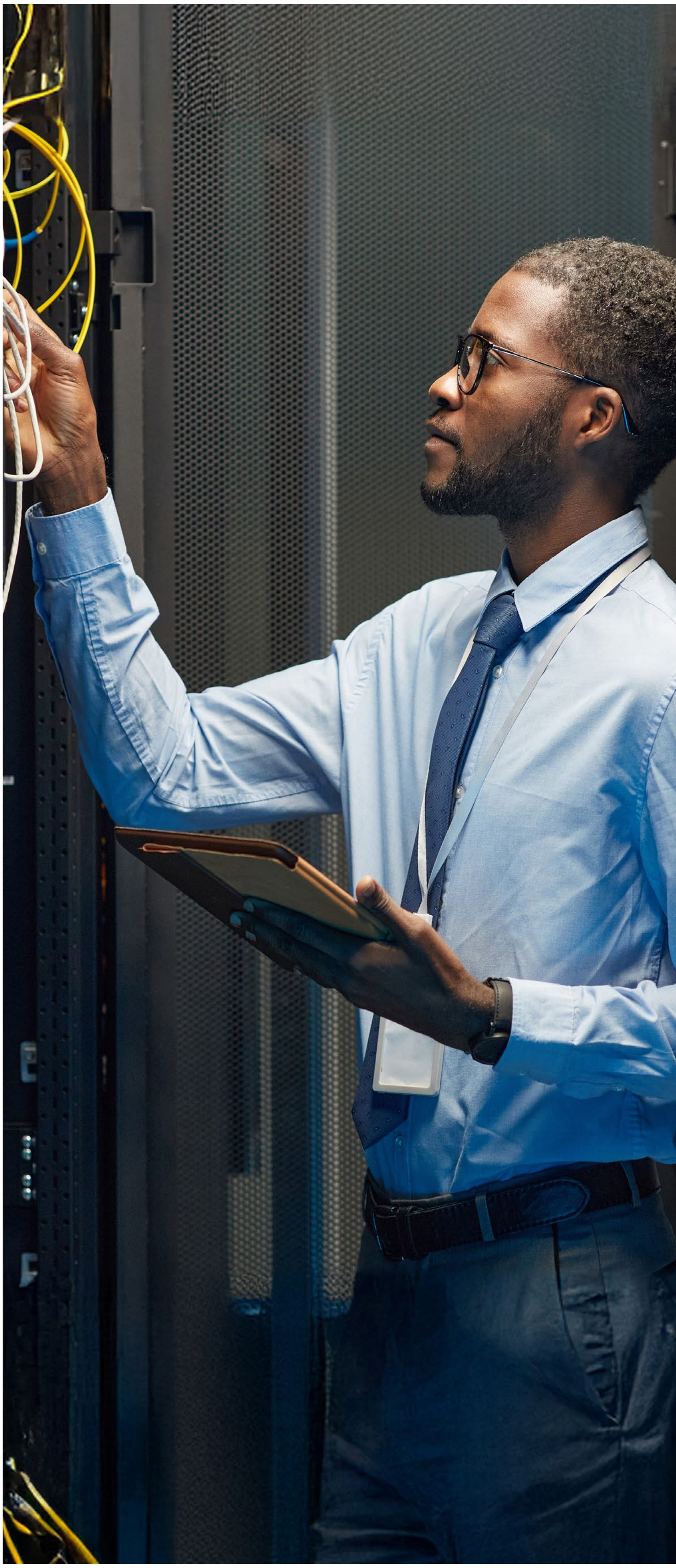
Failure to act on cyberattacks can have very real, very dangerous consequences in this sector – not just for businesses, but for environments and communities around them. For example, while an office-based business may simply shut down systems to contain a cyberthreat, OT like cooling or power systems may have to keep running for safety's sake. Preventing a physical industrial disaster must always be a priority.

> Overcoming the inherent cultural and operational gaps between IT and OT teams is crucial for establishing a cohesive security posture.

The commercial imperative for continuous operation can also sometimes lead to compromises in security practices. Management may be hesitant to implement necessary updates or take systems offline for maintenance, leaving them more open to cyberattacks.

Organisations may face budget constraints that limit their capacity to invest in the latest security technologies or specialised expertise. Efficiently allocating security resources across numerous global locations and diverse operational units can present a significant challenge. This is especially true if cybersecurity budgets rest with IT, rather than operations as a whole. OT and IT budgets must be united if all areas of a business are to be given appropriate protections.

There's also the issue of legacy OT systems often being deeply embedded in production processes. These older systems can be difficult and costly to update, creating significant security vulnerabilities. Addressing this technical debt in OT environments, while ensuring uninterrupted production, requires careful planning, specialised expertise, and a phased approach to modernisation.



Get a global perspective on today's cyberthreats.

Verizon's annual Data Breach Investigations Report (DBIR) is a trusted resource on the evolving cybersecurity landscape, reflecting our commitment to a data-driven approach to security.

The authoritative source of cybersecurity breach information, the DBIR reveals key risks for manufacturing and other sectors and presents expert advice on mitigating them. The 2025 report alone analysed over 22,000 real-world incidents, offering powerful insight that could help you defend against evolving threats.

Download the report today.

Embrace end-to-end cybersecurity for safer OT.

Having an expert partner at your side can alleviate much of the complexity of OT cybersecurity.

Verizon has a track record of helping companies bolster their cybersecurity defences. We provide end-to-end protection, safeguarding not only IT infrastructure but also increasingly interconnected OT environments.

In addition to our own extensive capabilities, we partner with other security leaders to deliver specialised OT security. Such collaborations allow us to provide tailored solutions that meet your unique and evolving needs as you digitally transform.

If you want to ensure your business's vital OT infrastructure is operating under industry-leading security, Verizon can complete an on-site assessment to uncover the most cost-effective and immediate areas for improvement.

Your OT is the beating heart of your business. Make sure you protect it.

Case study: Securing a modern manufacturer

A global manufacturer of spirits, wines and soft drinks found that its security infrastructure hadn't kept pace with its speed of connected technology adoption. This business worked with Verizon to urgently update its security controls to better meet changing demands and ensure that security was closer to where data actually sat.

Verizon worked to:

- Install new on-premises firewalls and configure new policies/zones
- Take on responsibility for managing these via Verizon Managed Security Services
- Segment OT and IT LAN for 20+ global factories
- Initiate security policy interactions with minimal production impact

This helped to:

- Create a new security environment ready for future growth
- Improve monitoring of security devices
- Reduce cyber risk by isolating IT and OT networks
- Increase visibility of devices and business flows

Want to go deeper on digital transformation?

Read key insights from industry experts on how to integrate the latest technologies to create a fully connected enterprise.

Learn more about Verizon's Manufacturing solutions

Discover the latest transformative tools that are giving manufacturers the edge by visiting one of our Innovation Centres.

Visit an Innovation Centre

Learn more about how to protect your OT environments.

Download our detailed whitepaper on protecting OT here.

verizon business