A holistic approach to securing operational technology

New cybersecurity challenges for OT

verizon business

Today's industrial landscape – shaped by the advances of the Fourth Industrial Revolution – demands rapid, secure and resilient services and systems. Organisations must prioritise the security of their OT and establish appropriate monitoring and response mechanisms to address any potential issues that may arise.

That's because, while providing connectivity between OT applications and OT devices can really empower organisations, it can also open routes for malicious users and cyber criminals to gain access.

OT networks have traditionally been isolated from IT networks and the internet for their own security and reliability. This is no longer the case.

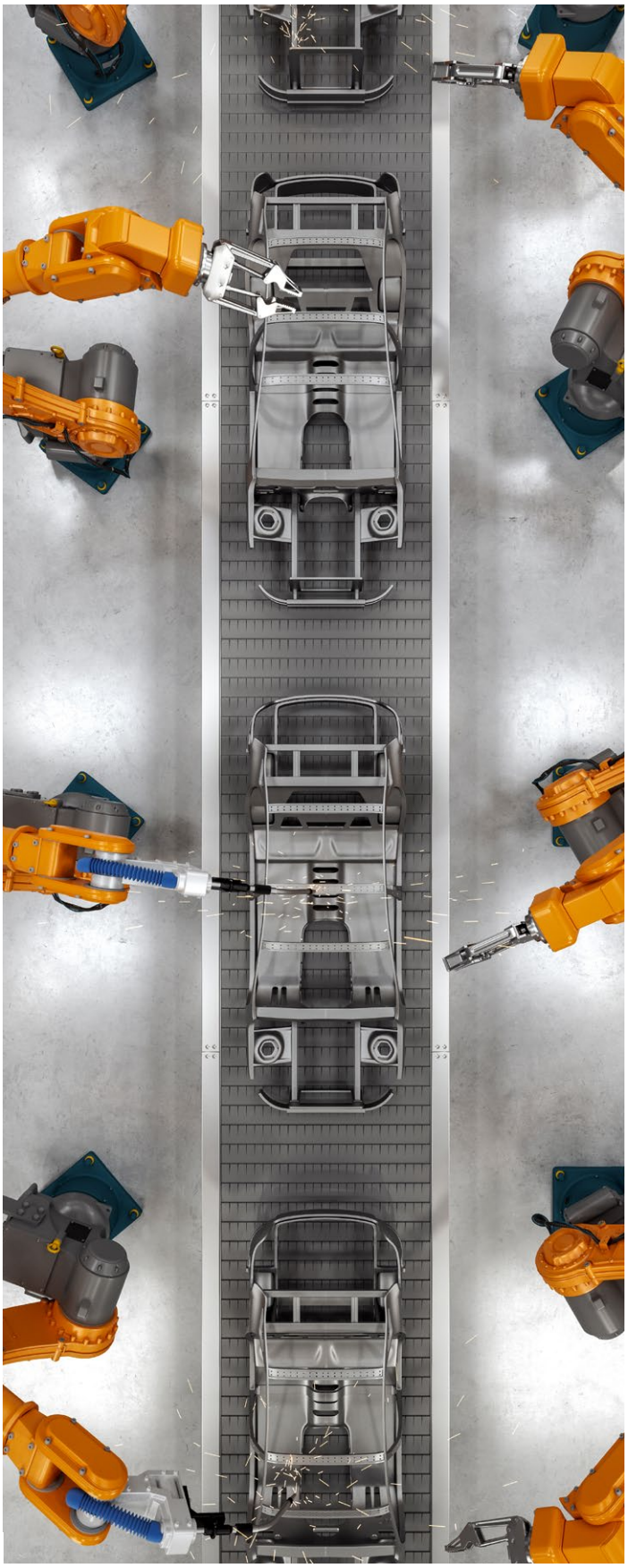
This paper will reveal insights on how to help secure integrated OT networks, so that they can be counted as a business enabler, not a business risk.

> The OT security market places a lot of emphasis on asset identification, and threat and vulnerability detection, but protection can't be forgotten.

Rethinking cybersecurity for Industry 4.0

Industry 4.0, or the Fourth Industrial Revolution, is characterised by a fusion of technologies blurring the lines between the physical, digital and biological spheres.

In this modern arena, organisations are adopting everything from autonomous robotics, near-real time remote controls, edge computing and advanced connectivity technologies. This kind of evolved operations, so intertwined with the cloud, require a ground-up rethink of security architectures. Zero-trust access will be required for strict security controls, for example.



Footnote: Sources: [1]The Forrester Wave™: Operational Technology Security Solutions, Q2 2024; Forrester

However, this shouldn't be seen as a burden. In fact, it may present new opportunities for simplifying and optimizing business architecture. One benefit to this restructuring can be found in the collection of massive datasets for analytics, helping power everything from incident handling to product improvements.

Evolving business drivers come with new risks

OT evolution

As organisations seek greater efficiencies, OT is moving to join IT in the cloud. Businesses are also beginning to use AI for predictive maintenance and automation and rethinking how to work with third parties—citing concerns around security controls and cost effectiveness.

> 80% of CIOs are set to embrace AI and automation for agility and insights-driven businesses by 2028"
>
> **CIO Predictions** in Asia/Pacific* for 2024 and Beyond Revealed by IDC

IT-OT convergence risks

The increased connectivity between IT and OT networks potentially expands the attack surface, as legacy OT systems were typically not designed with cybersecurity in mind.

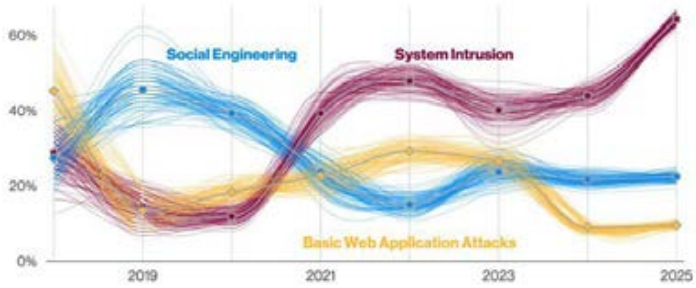
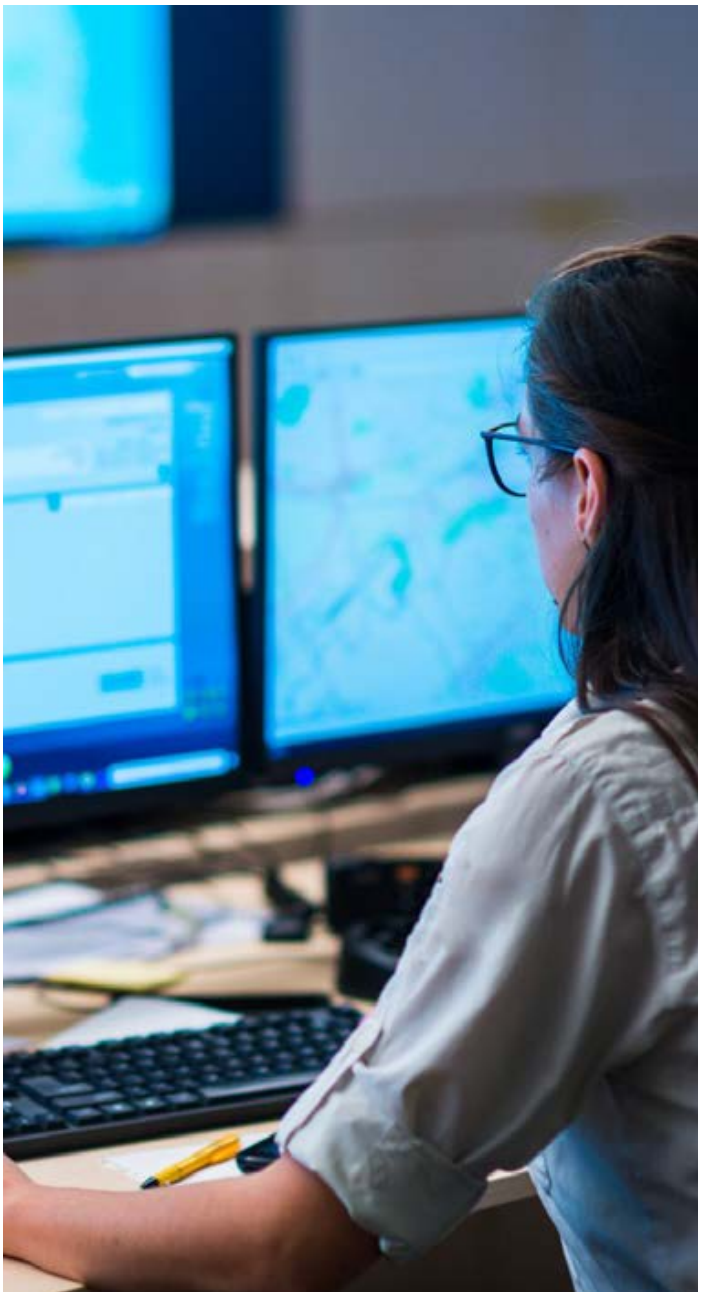


Figure 1: Top patterns over time in Manufacturing industry breaches

Footnote: Source: Figure 1; 2025 Verizon DBIR

This is already having a material impact. We can see, from the Verizon 2025 Data Breach Investigations Report (DBIR), that global system intrusions have increased greatly since 2020. The manufacturing industry, specifically has seen a significant increase in the past year. This industry has also seen a significant increase in data breaches, with the number of confirmed breaches almost doubling from the previous year.

While financially motivated external actors remain the primary threat, it's noteworthy that espionage was the motive in approximately 20% of manufacturing breaches, a substantial rise from just 3% the previous year.



Legacy and unpatched systems

Many OT environments still rely on outdated operating systems and software that lack vendor support—or have no support at all. Patching and updating OT systems is difficult due to concerns over downtime and lost production.

Lack of visibility and asset management

Organisations often lack a clear inventory of connected OT assets, making risk assessments difficult. Shadow OT devices and undocumented endpoints can introduce additional unknown vulnerabilities.

Ransomware and cyber threats

Ransomware is the leading action type affecting the manufacturing industry, according to the 2025 DBIR. Threat actors tend to exploit weak segmentation between IT and OT, then move laterally to disrupt other operations.

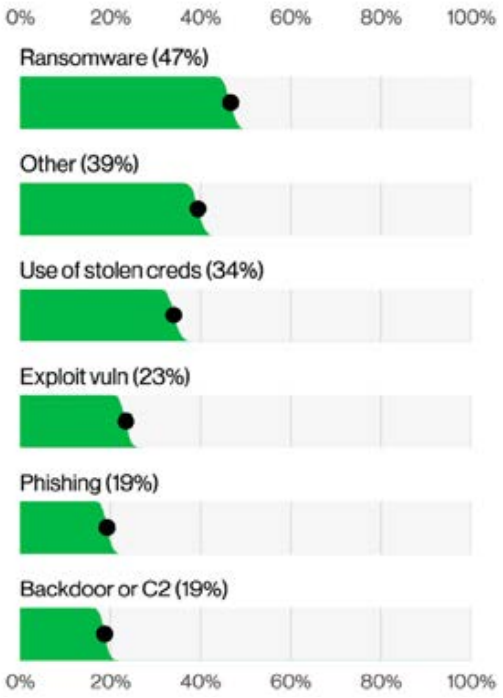


Figure 2: Top Action varieties in Manufacturing breaches

Ransomware incidents appear in 44% of all breaches reviewed in the 2025 DBIR, up from 32% on the previous year's report. Despite this rise, the median ransom paid has decreased to $115,000 from $150,000. This decline may be linked to the growing number of victim organisations refusing to pay ransoms.

Ransomware disproportionately impacts small- and medium-sized businesses (SMBs), accounting for 88% of their breaches, compared to 39% in larger organisations.

Footnote: Source: Figure 2; 2025 Verizon DBIR | Figure 3; Verizon

Regulatory and compliance complexity

Organisations must comply with multiple cybersecurity frameworks and industry regulations, for example the National Institute of Standards and Technology (NIST), IEC 62443 and the Cybersecurity & Infrastructure Security Agency (CISA) guidelines. Ensuring compliance across global supply chains adds another level of complexity, especially for smaller businesses.

Third party and supply chain risks

Having a number of vendors, contractors and suppliers can create multiple points of cyber exposure throughout connected OT networks. Robust controls around identity and zero-trust access management are a must for any kind of remote access.

Skills and workforce gaps

There is a shortage of cybersecurity professionals with expertise in OT security. When new staff are brought in, they may lack cybersecurity awareness, which can result in increasing the risk of insider threats and human error.

Building an OT security strategy

Frameworks like NIST CSF, NIST 800-53, ISO 27K, IEC 62443, NIST 800-82, and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) are very helpful in providing a consistent approach toward managing any cybersecurity programme, as well as in building a customised OT security strategy.

Figure 3: Features of a comprehensive OT security strategy

A simplified strategy for OT security must at least include the following components combined in a governance structure:

- A comprehensive asset management framework to keep track of what you have, how old it is, its end-of-life status, and software or firmware versions.
- Periodic security assessments of the OT network to identify any security weakness or gaps.
- A multi-layered network architecture with a safe IT 'demilitarized zone', providing simplified access to applications hosted in the cloud.
- Continuous threat monitoring for improved detection capabilities within operational technology networks. This should encompass both network and application layers and use YARA (Yet Another Recursive Acronym) rules to detect OT-specific malware.
- OT-specific threat intelligence, for early attack detection and prevention. The should be made up of a combination of public and government threat intel, industry-specific threat feeds, open-source and community feeds, and both vendor and private threat feeds.
- A well-designed and tested incident response plan enabling early detection of threats.

OT security framework transformational phases

The phases above are an example of an ideal OT network security journey—when you choose Verizon to assist with your transformation, this is the process we will likely take.

Your business can begin at the phase most relevant to your needs and operational maturity level. In parallel, the following areas of OT governance and organisation should be a focus:

- Aspects of the organisation that are concerned with innovation and future development.
- Executive strategy planning and execution at corporate and business-unit level.
- Identifying a local champion per factory or group to make the OT planning and execution a bigger success.

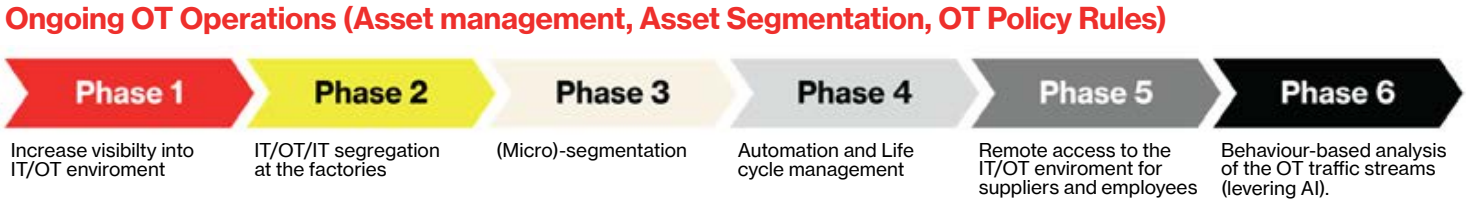


Figure 4: OT security framework transformational phases

PHASE 1: Increase OT visibility

Verizon Security Consulting Services aim to enhance your understanding of the interconnected IT and OT devices within factories, warehouses and similar environments. This is achieved through a comprehensive factory asset discovery and assessment. This can be conducted either onsite or remotely for visibility of the OT devices and their risk factors.

PHASE 2: IT and OT Segregation

Verizon will work with you to segregate the OT network from the IT network by using basic protection controls.

Such segregation can be achieved through the implementation or reuse of physical or virtual firewalls. The following security controls must be activated, at a minimum:

- Threat prevention
- Anti-malware
- Domain Name System (DNS) protection

Our consulting service experts facilitate the implementation and configuration of security controls, while Verizon's managed service teams can oversee their operation from our Security Operations Centres (SOCs).

PHASE 3: Micro-segmentation

Segmentation within the OT environment is performed. This is achieved through the development of custom blueprints that are repeatable across the company facilities, driving standardisation and simplification. This phase makes the different security zoning and policies abundantly clear.Verizon Security Consulting services can develop and implement these blueprints on existing security controls (Phase 2).

PHASE 4: First automation and life cycle management

The development of specific OT playbooks for seamless creation and updating of OT segment rules begins in this phase, leveraging available tools, ticketing systems or script development.

Life cycle management will be used to keep devices aligned with required security controls. Devices will be placed in an extra security zone if no proper maintenance is possible.

Footnote: Sources: Figure 4; Verizon

PHASE 5: Remote access to the OT environment for suppliers and employees

In this phase, we activate modern remote access services on a zero-trust, 'need-to-know' basis. We then implement access controls for employees and different suppliers, as well as support agent-based and browser-based solutions.

PHASE 6: Activation of advanced—mainly AI-driven—security controls and automation

AI-enhanced security controls such as data-loss prevention (DLP), intrusion prevention systems (IPS), and security analytics with user and entity behaviour analytics (UEBA) services, can provide an additional level of visibility in the IT and OT streams. This information can be used to develop new OT playbooks or update existing ones. It will also help improve OT incident response services and enable the development of OT deception-based services.

Operating model recommendations for OT environments

Verizon's experience of transformation programmes within manufacturing environments enables us to present a recommended organisational structure for this new industrial era.

This diagram represents a structure that Verizon has effectively utilised in previous IT/OT programmes.

Of course, this should not be seen as a one-size-fits-all solution. Your near-term goals might mean using a structure better aligned with desired business outcomes. A defined long-term vision might mean restructuring the organisation and all its processes.

The proposed organisational structure has all cross-functional horizontal technologies and relevant resources reporting through the group Chief Information Officer (CIO), with the CIO being accountable for the common services provided to the business unit. Each unit then has a Chief Technology Officer (CTO) or CIO function that is responsible for the differentiated operational technology.

The division CIOs report into their division but have matrix reporting into the group CIO while sitting on the CIO board. The purpose of the CIO board is to provide common alignment and governance on technology. A Chief Information Security Officer (CISO) would be accountable for the security functions while also sitting on the CIO board.

As a security services provider, Verizon can provide managed transformation and takeover services, as well as other managed security services. Such an arrangement can enable you to focus on their areas of differentiation.

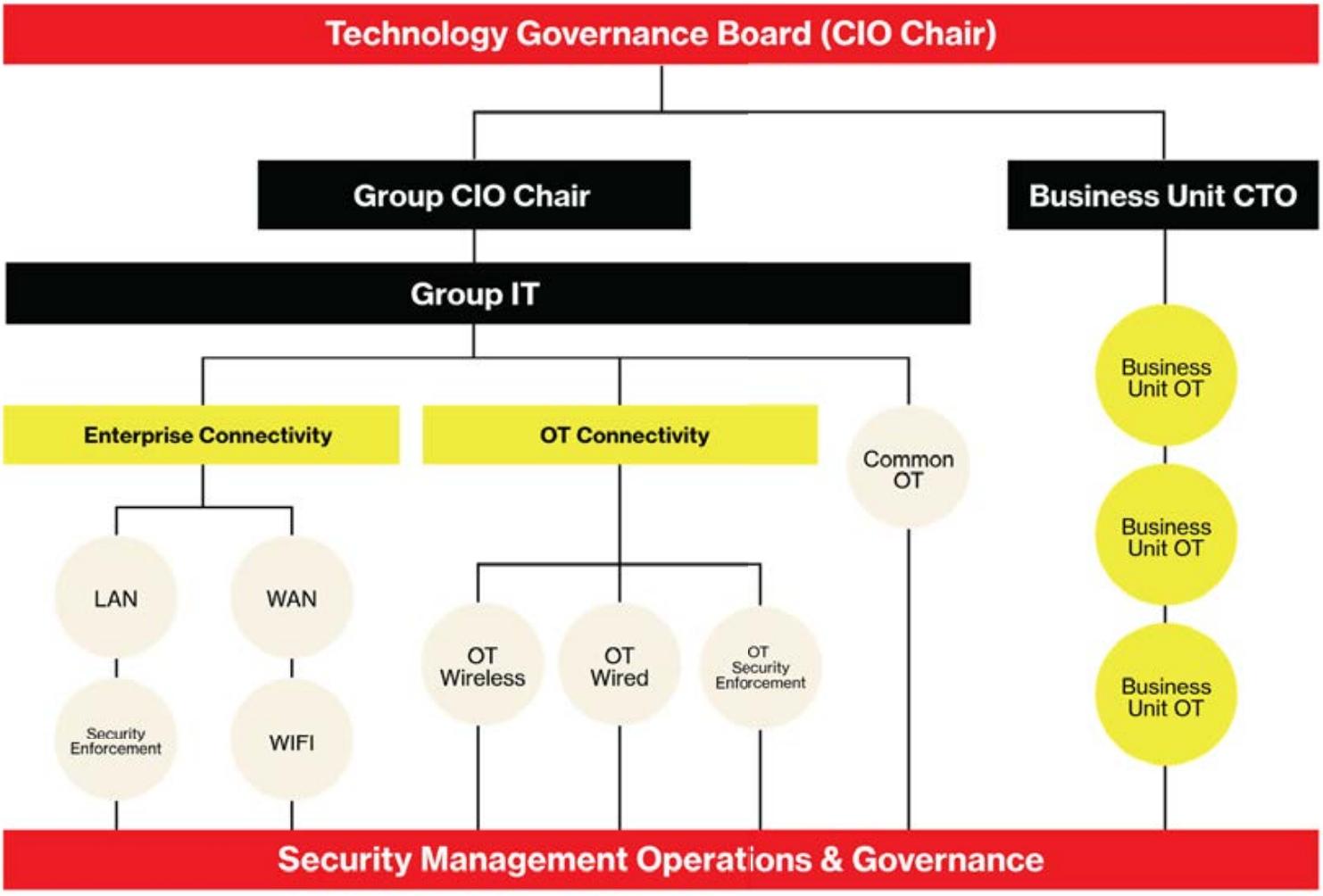


Figure 5: The common/group technology operating model

Footnote: Sources: Figure 5; Verizon

Conclusion

With this holistic approach to OT security, businesses like yours can better achieve the right security setup and help address business needs and budgets. Verizon can help prepare your company to address or mitigate cyber threats.

Learn More

To learn how Verizon can help you mitigate cyberthreats and protect your business, contact your Verizon Account Manager and visit www.verizon.com/business/en-gb/solutions/secure-your-business

Author and contributors

Author

Marc Borking, OT SME and Principal SecurityConsultant, Consulting Services , Verizon Business

Contributors

Ashish Khanna, Senior Director and Head of EMEA Security Consulting Services

Stephen Young, Director, Security Consulting Services

Beat Kueng, Associate Director, EMEA Security Solutions Architecture

Chris Zijderveld, Associate Director, Security Consulting Services

Ali Akl, Head of Risk and Resilience, EMEA Security Consulting Services

David Samreth, Principal Consultant, Consulting Services

Case study: Global manufacturer

As this global manufacturing business increased the use of automation across its operations, it began to see a high growth in traffic between IT and OT systems. This came with a corresponding increase in security risk and a widening of the attack surface. To continue evolving while focusing on protecting people, data and infrastructure, the company took proactive measures, performing a complete security assessment on their existing OT environment and identifying several imperatives.

Business imperatives:

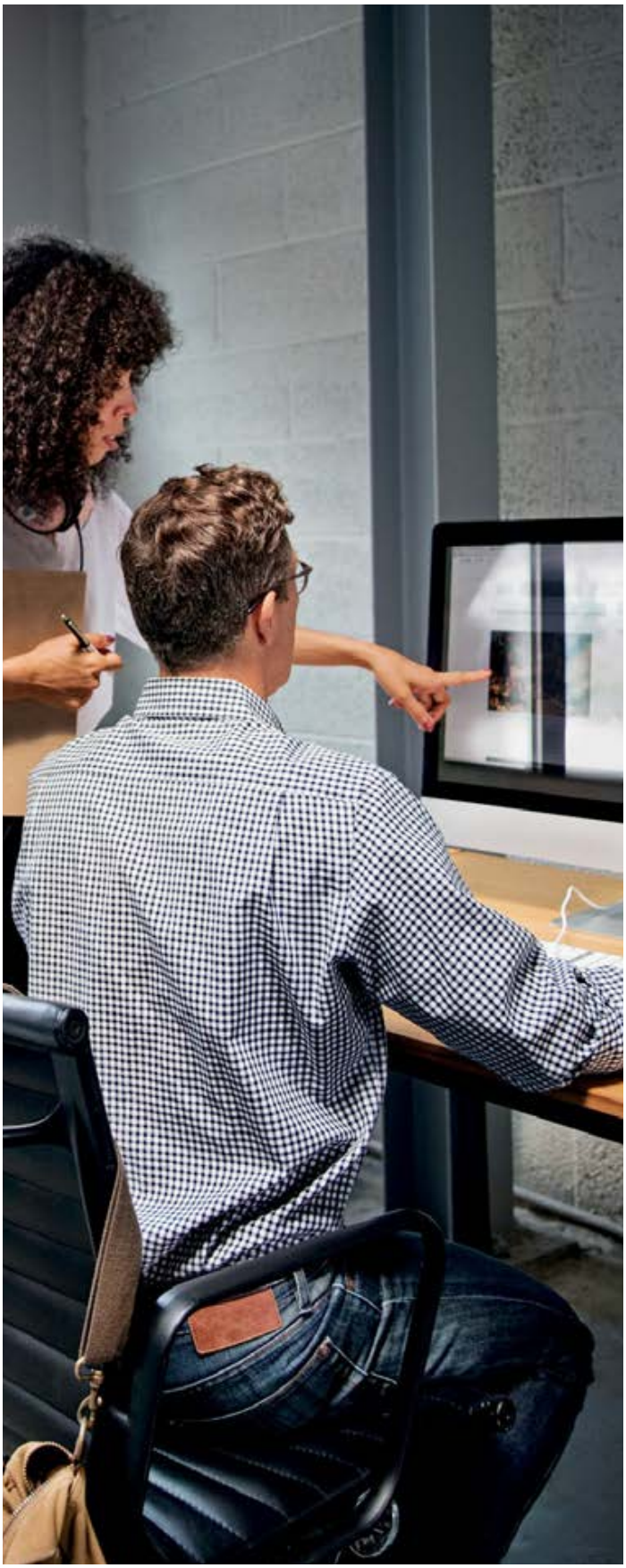
- Update existing security infrastructure that was no longer fit for purpose
- Get a clear view of current architecture, security requirements, segmentation policies, business flows, devices and processes
- Understand security risks caused by a lack of segmentation
- Enable security controls to protect the business assets
- Align security setup and policies
- Mitigate evolving global security risks
- Update the environment ready for future growth and compliance

Solution:

- Ran an onsite discovery and OT assessment at the factories
- Built a configuration management database and a suitable architecture design
- Created a security policy template, as well as an OT and IT segmentation template Reused or installed new on-premises firewalls, configuring new policies, segments and zones before handing over to Verizon Managed Security Services
- Applied LAN segmentation to all (25+) global factories, enabling IoT discovery
- Fine-tuned security policies in a phased approach
- Automated playbooks to create and simplify OT segmentation

Benefits and outcomes:

- Helped address cyber risk by performing isolation of the IT and OT network, as well between OT and OT segments
- Improved monitoring of security devices with Verizon MSS
- Increased visibility of devices and business flows
- Enhanced compliance in line with new requirements and global threats
- Created a new security environment, ready for future growth



Lessons learned:

What has been agreed in theory always takes more time in practice. That's par for the course for most projects. In this case, the client needed to shift scope before the project could begin. Then, when the green light was given, capturing the necessary data, finding the right people, discovering of the right switches, and implementing the correct configuration, took longer than anticipated. The business also encountered longer time leads due to competing business priorities.

Designate client-side help

Once a dedicated team was assigned to this project, it started to accelerate. Once one location was set up, lessons learned about processes, design and potential pitfalls could be applied to the next location, working faster and with Network traffic and data capture (via SPAN ports) was also challenging, with microsegmentation taking time due to possible business impact. The flows of assets was not always known, meaning multiple firewall log analytics had to be performed before enabling a deny rule. In addition, it was difficult to discover assets due to old switches not being able to handle the configuration or extra load. This was fixed when traffic was sent via the firewall.

Align, inform, include and motivate

Coordination proved crucial. Automation required alignment between different teams to ensure that playbooks work as designed.

It was discovered that equipment vendors generally had broad access to devices. Access could be limited but only by Secure Shell (SSH), Remote Desktop Protocol (RDP) or browser-based access.

Clear and direct requests to vendors should be made to ensure timely architecture changes. Collecting and analysing traffic can be resource-intensive, so this needs to be planned and budgeted for appropriately.

The transformation in detail

Phase 1

- By establishing a clear, key point of contact, we were able to streamline communication and ensure all project activities remained aligned.
- Initial discovery and configuration was thorough and meticulous.
- We successfully addressed the challenge of network traffic capture by innovating a solution to route data through the firewall.
- Although the project's start date was adjusted, this allowed for a more comprehensive and well-aligned final plan, ultimately leading to a successful implementation.

Phase 2

- The firewall delivery process in some regions took longer than anticipated due to local restrictions and renewed government requirements, specifically regarding legal documentation and signatures. This caused some parts of the project to experience delays.
- Initial segmentation phase began at a measured pace, but proved essential for developing a smooth, accelerated and repeatable process across other sites.

Phase 3

- The second phase of microsegmentation required a careful, phased approach to minimise disruption.
- A key factor of success was the insight gained from the local contact.
- To ensure accuracy, extensive firewall log analysis was performed to fully understand all asset flows.

Phase 4

- Aligning different teams proved essential for developing effective and efficient automation playbooks.
- With all teams in sync, we were able to create solutions that functioned smoothly.

Phase 5

- Verizon is helping the business move to a more controlled access model for vendors.
- This includes establishing a new standard that limits access to SSH, RDP, or browser-based methods only.
- This change is being implemented through direct requests and close collaboration with vendors to provide access while aligning with the new architecture.

Phase 6

- Behavioural analytics provided critical insights, providing a deeper understanding of network activity.