IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

The Strategic Role of Channel Partners in Enterprise Cyber Resilient Storage Solutions

James (JT) Lewis

James (JT) Lewis
Director of Channels
EMEA and APJ
Infinidat

Biography

James (JT) Lewis is the Director of Channels EMEA and APJ at Infinidat (https://www.infinidat.com). He is an experienced international Sales Director with a proven track record in the enterprise IT, storage, and network security industries. His broad industry experience includes roles involving cyber security, Storage Area Networks (SAN), enterprise storage, IT service management, IT strategy, professional services, cloud computing and virtual computing environments.

Based in Frankfurt, JT has responsibility for Infinidat's EMEA and Asia Pacific regions, including Japan. JT served in the US Military before embarking on his technology sales career, more recently he worked for Data Interchange as Head of Channel Sales and was the Strategy and Growth Officer for Altdata Technology Solutions, focusing on the cyber security market. He also spent 15 years at EMC and RSA, based in London and Frankfurt, where he built up comprehensive experience in the recruitment, enablement, and leadership of channel partners and distributors.

JT blogs at https://www.infinidat.com/en/blog

Keywords Operational Technology (OT), Cybersecurity, Manufacturing, Industry 4.0, Channel partners
Paper type Research

Abstract

A significant transformation is underway in many manufacturing enterprises, triggered by greater interaction between Operational Technology (OT) and IT systems. Channel partners should be aware of how this trend has implications for cyber security and help their clients to mitigate the risks. Sharing insights like these creates an opportunity to add more strategic value during consultations and strengthen the trusted technology partner relationship, explains the author of this article.

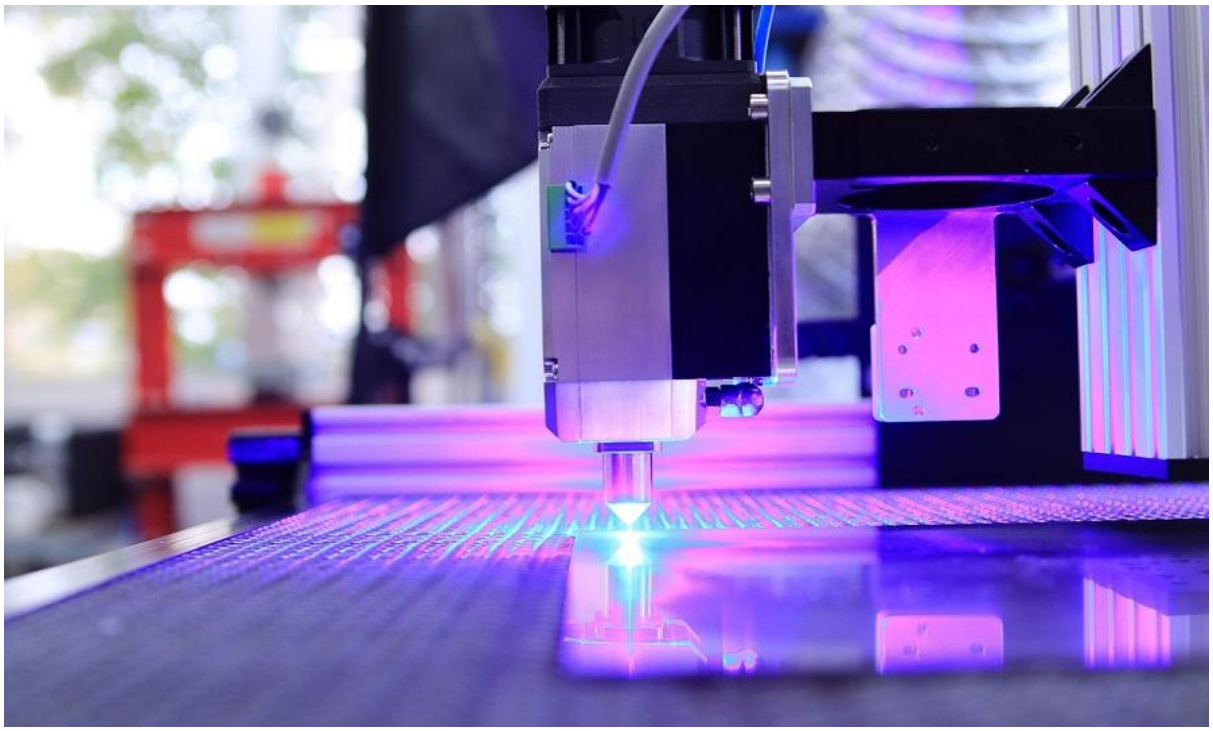
Introduction

Traditionally, Operational Technology (OT) systems have focused on controlling physical processes and equipment. In contrast, IT systems handled data processing and business operations. These two systems have evolved in recent years and the traditional separation between the two is very rapidly disappearing, as manufacturers embrace digital transformation and Industry 4.0 to drive efficiencies. The result is an integrated approach that enables real-time monitoring and data

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

analysis, improved efficiency and enhanced productivity across the entire manufacturing operation. It means communication between shop floor operations and enterprise-level systems is seamless, leading to better decision-making and better optimized production processes.



The Manufacturing Execution System (MES) lies at the heart of the integration between OS and IT. It supports the planning, monitoring, documentation and control of manufacturing processes in real-time. It also links higher-level ERP systems and industrial automation systems through process and machine control systems. Data flows seamlessly between production equipment and business systems, allowing for comprehensive visibility and optimization of manufacturing processes. Enterprises can now make data-driven decisions based on real-time information, significantly enhancing their operational capabilities. This offers huge advantages to manufacturers, but integration also brings many risks and vulnerabilities – which channel partners, in their role as trusted technology partners, should be communicating to clients.

New research from Deloitte conducted with the Manufacturing Leadership Council in 2024 reveals that one of the biggest risks is a potential data breach/cyber threats[1]. The study reported that 48% of manufacturers experienced at least one data breach in the past 12 months, with an average cost of £2.1 million per breach. By helping manufacturers to understand these risks comprehensively, channel partners have a unique opportunity to position themselves as strategic advisors rather than just technology vendors, creating stronger, more successful long-term relationships.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Integration brings vulnerability

As OT and IT systems become interconnected, they also become more vulnerable to cyber threats that specifically target enterprise storage systems. According to a 2024 survey by industry research firm Omdia, 80% of manufacturing firms had experienced a significant increase in overall security incidents and breaches in 2024[2]. The same study also found that less than 50% of manufacturing firms are prepared for the threat of these cyber security breaches, leading to significantly increased risk. This is critical because data is one of a manufacturing company's most valuable assets. With enterprises globally suffering an average of more than 1,650 cyberattacks per week, it is not a case of if you will suffer a cyberattack, but when, and how often.

Devastating impact of storage targeted attacks

A ransomware attack on enterprise storage systems can cripple a manufacturer, completely halting production processes as data and files become encrypted and inaccessible. Such an attack can also compromise the entire manufacturing operation, from design and engineering data to supply chain management information. If key files are encrypted, the enterprise may not have access to product specifications, production schedules, and customer orders. Operations can be brought to a standstill and the implications are far reaching, potentially also damaging long-term projects, customer relationships and the business reputation.

This is corroborated by data published by the manufacturing industry body, Make UK. Its most recent report published in 2023 highlighted that during the previous year, nearly half of British manufacturers suffered cyberattacks. A quarter of affected companies reported losses ranging from £50,000 to £250,000, but the financial implications were just one aspect of the problems encountered – 65% also experienced production downtime and a further 43% faced reputational damage[3].

That's not all. Modern ransomware attacks have evolved beyond simple encryption to also include data exfiltration. Sensitive intellectual property and proprietary manufacturing processes can be stolen and sold on dark web marketplaces, causing long-term damage to an enterprise's competitive position. Furthermore, if personally identifiable information is compromised during these breaches, manufacturers may face significant regulatory penalties under frameworks like GDPR.

Switch from prevention to recovery

The cybersecurity landscape has now evolved to a point whereby expecting to completely prevent a cyberattack is unrealistic. Cyber criminals are continuously refining their techniques, often applying social engineering and phishing campaigns that bypass traditional security measures. This means manufacturers need to shift the focus away from prevention alone to ensuring a rapid recovery when, and not if, a cyberattack occurs.

This shift in perspective is particularly critical because cyber criminals typically don't discriminate between targets based on company size or industry prominence. Any

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

enterprise is fair game. Small, regional manufacturers face the same sophisticated threats as multinational corporations, so ensuring cyber resilience across the entire manufacturing sector is essential.

Cyber resilience is also a regulatory requirement

Depending on the scope of an enterprise's business operations, cyber resilience may also be a legal requirement. In the EU, manufacturers must comply with the NIS2 directive (2024). The situation for UK manufacturers is more complicated because although NIS2 does not directly apply to all UK companies due to Brexit, it may apply if they have operations or customers based in the EU. This is equally true if a manufacturer has operations in the US or Japan – both of which have similar cyber regulations to the EU and the UK.

In addition, the UK continues to operate under its own NIS Regulations (introduced in 2018) and is updating its cyber security framework through the upcoming Cyber Security and Resilience Bill. This Bill is expected to be presented to Parliament later in 2025. Clearly, what all manufacturing enterprises need now more than anything is the strategic guidance to develop a cyber resilient storage infrastructure. Channel partners could be adding significant value here by sharing these foundations.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Five foundations for cyber resilient storage

A cyber resilient storage infrastructure to support manufacturing business continuity is built on five key principles:

1. **Immutable Snapshots** – Rather than creating simple backups, manufacturers need secure, unalterable data copies taken at specific intervals. These immutable snapshots ensure that critical production and business data remains unchanged after creation, providing a reliable recovery source regardless of attack sophistication.

2. **Logical and Remote Air-Gapping** – Effective cyber resilient storage requires logical isolation of immutable snapshots from network access. Air-gapping – implemented locally, remotely, or both – creates an additional protection layer that keeps recovery data segregated from potential infection vectors.

3. **Automated Detection and Response** – The speed of modern cyberattacks renders manual monitoring insufficient. Manufacturing companies need automated cyber security capabilities that integrate seamlessly with their existing security stack, including Security Operations Centres (SOC), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR) platforms. These systems should automatically trigger immutable snapshots when security incidents are detected.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

4. **Fenced Forensic Environment** – Recovery from cyberattacks requires a completely isolated network environment for forensic analysis. This "fenced" area allows for thorough data testing and integrity verification, ensuring that recovered data isn't compromised before reintroduction to production systems.

5. **Near-Instantaneous Recovery** – Critical for manufacturing operations is the ability to retrieve clean data copies within minutes, regardless of dataset size. Manufacturing processes are particularly time-sensitive, making rapid recovery capabilities essential for minimizing production disruption and financial losses.

In conclusion – storage decision making gets strategic

The basic principles of building a cyber resilient storage infrastructure may be well-understood, but a successful implementation is more challenging. It calls for a strong strategic technology partnership between technology vendors, channel partners and the end user enterprise. When evaluating a storage vendor, manufacturing companies should look beyond the traditional criteria, like capacity, speed, price/performance-ratio, and the availability of a flexible consumption model. Channel partners can help customers perform this analysis and potentially also support the final implementation process.

Today's threat landscape demands a more strategic approach, with equal consideration to cyber resilience capabilities. When supported by partners to implement a comprehensive cyber resilient storage infrastructure, manufacturers can protect their most valuable asset – data – while ensuring business continuity, even in the face of sophisticated cyberattacks.

Reference

1 Coykendall, J. Hardin, K., and Morehouse J. (24 November 2024) '2025 Manufacturing Industry Outlook'. Deloitte. Available at: https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook.html

2 (24 February 2025) '80% of manufacturing firms experienced cyber attack last year'. IOT Insider. Available at: https://www.iotinsider.com/industries/security/80-of-manufacturing-firms-experienced-cyber-attack-last-year/

3 Make UK (2023) Cyber Security in UK Manufacturing. Available at: https://makeuk.org/insights/reports/2022/12/01/cyber-security-in-manufacturing