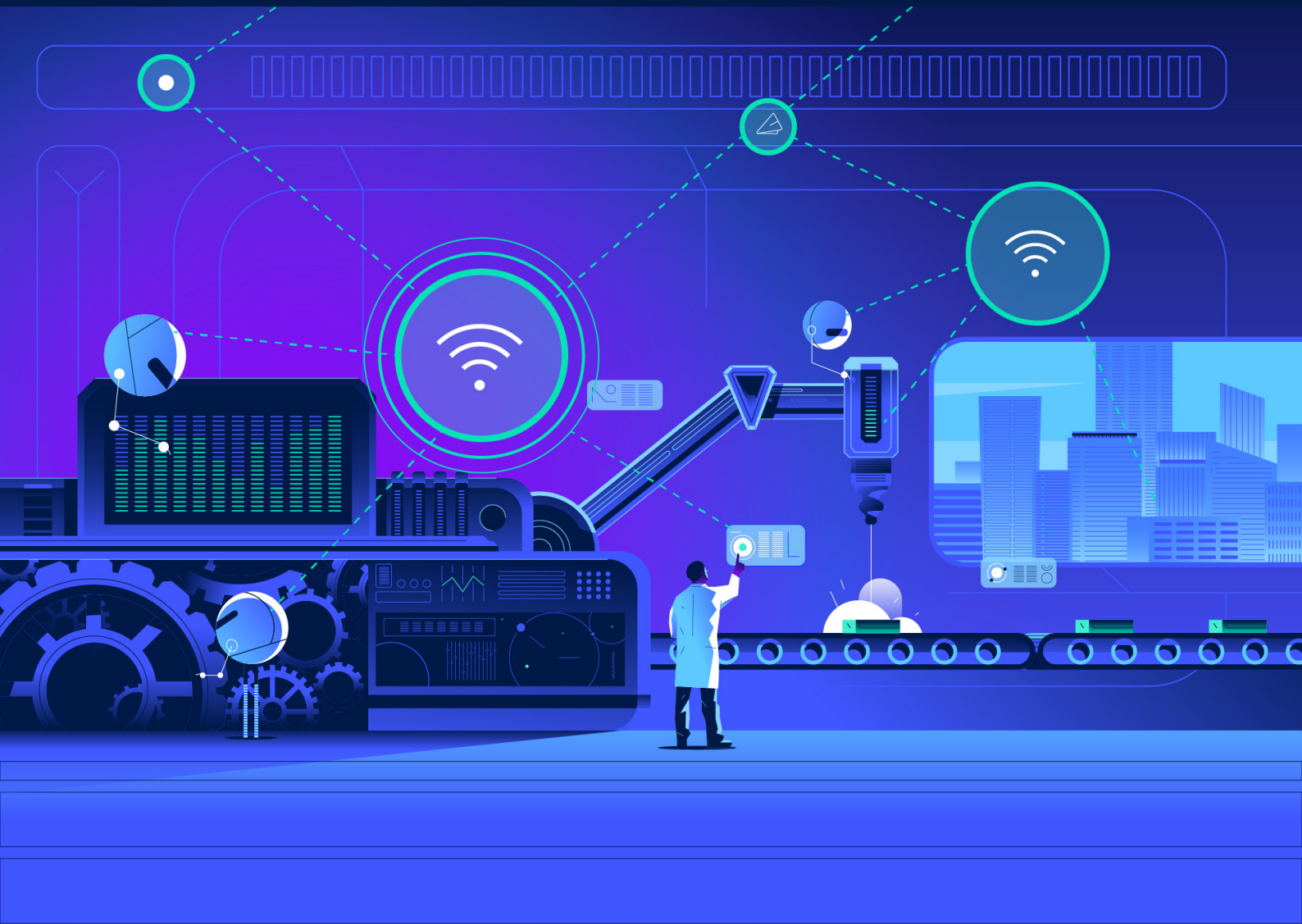
ISTARI Perspectives

Getting Cybersecurity Right for Manufacturing

Abel Archundia

06 • 2021



As industrial companies merge their information technologies with operational technologies, they need to foster more collaboration and refocus on building digital resilience.

At first glance, the distinction between information technology (IT) and operational technology (OT) seems clear. Information technology, typically led by a chief information officer, supports enterprise business processes and office workers through the use of computers, servers and applications. Operational technology, typically led by the chief operating officer, supports industrial control processes and other physical manufacturing equipment.

Intuitively, that distinction makes sense; an IT administrator will not repair an oil drill. An OT engineer will not use predictive analytics to protect the computer network from cyber threats. But over the last decade, OT and IT have started to converge. Thanks to the simple economics of automation and the industrial internet of things, operational technology today comprises cutting-edge software apps managed by the information technology department, which run on physical machinery managed by operational engineers. The lines between OT and IT have started to blur.

Unfortunately, alongside the benefits of lower total cost of ownership and much greater ease of use, these internet-facing systems expose industrial systems to new threat vectors. They also present a conflict: to what extent is it necessary to sacrifice technology competitiveness for enhanced security? Legacy organisational design compounds this technology challenge. Effective collaboration between IT leaders, manufacturing executives and the OT teams is lacking at many companies. Specific security and reliability measures may be delegated to the plant level, while overall accountability flows centrally. Resilience continues to be an afterthought unless there is a crisis, and that won't do for the digital age.

An Industry Under Threat

Criminals continue to deploy ransomware attacks and commit data theft to extort businesses. Ponemon Institute's 2020 Cost of Data Breach study showed the average global cost of a breach was $3.86M, though the average cost in the United States was $8.64M. Lost business, including unscheduled downtime, was the single largest factor in the cost, amounting to $1.52M on average.[1]

For manufacturers, where unscheduled downtime is likely to be more disruptive to operations, the ultimate figure is surely much higher. Consider the recent attack on a plant in Mexico belonging to electronics producer Foxconn. In that incident, hackers encrypted around 1,200 servers, exfiltrated (and partially leaked) 100GB of data, deleted backups and demanded a $34M ransom. Operational disruption followed.

But, for many cybercriminals, such disruption is merely a by-product. In the Colonial Pipeline cyber attack that disrupted fuel supply in the US this spring, the group behind the attack bluntly declared: "Our goal is to make money and not to create problems for society".[2]

Global supply chains, already strained by the pandemic, leave the manufacturing industry especially exposed to cyber risks that extend beyond one company's network boundaries. The recent Russian state-attributed attack on software company SolarWinds is a timely reminder of how hackers can start by attacking suppliers or vendors as a stepping stone to reach companies higher up the value chain.[3]

Nevertheless, too many ignore this threat. Research by cybersecurity services company BlueVoyant found that the average manufacturer relies on 1,325 third-party vendors, but only 18% of manufacturers monitor third parties for cyber risk.4 Furthermore, four out of five had experienced a breach via third parties. Supplier due diligence assessments and questionnaires rarely collect sufficient detail to adequately determine the risk of compromise. They are also seldom updated or audited. While insurers may cover losses, affected customers and regulators will be less forgiving unless a company can show it has made reasonable efforts to improve.

Preparation is the best defence

As a chief information officer and head of digital transformation in a number of manufacturing environments, I have witnessed first-hand the technical and organisational challenges of making improvements across dozens of plants. From that experience and my current work with manufacturers globally, I have identified three steps organisations must take to create resilience in an increasingly connected IT/OT environment:

Culture and organisation are your 'first-line'

Tone from the top — Boards must communicate that preparation is the best defence. This empowers senior management to make a budget commitment and align around a vision of success.

Collaboration — To resolve challenges resulting from legacy organisational structures and processes, executives and employees alike must acknowledge that resilience is a team sport and work together to build it. This security coalition should be led by the COO, CIO/CDO and CISO.

Risk

Visibility — Gaining centralised visibility across all IT and OT assets (now usually characterised as Industrial Internet of Things) is essential for threat monitoring and provides a unified view of vulnerability. Effective decisions can then be made about which assets are most critical from a business perspective.

Prioritisation — Knowing the assets vital to production and customer processes should prompt at least two further steps: Joint IT/OT executive bodies must document vulnerabilities and clarify where unscheduled downtime cannot be tolerated.

Real-time reporting — Annual updates do not suffice. Agreed upon metrics must be regularly reported to reflect established as well as emerging risks. Update these action plans and provide timely reporting to the board on progress towards building resilience.

Strengthen your ecosystem

Third-party risk management — Communicate resilience expectations to the extended supply chain, not only to the most critical suppliers. Once expectations are clear, there are two options: work with suppliers to improve cybersecurity – or find anew supplier that truly understands the exposure at hand.

Collective defence — Acting alone gives the adversary an advantage. When industry peers share best practices and actionable, relevant and timely threat information, the entire ecosystem becomes stronger.

Competitive advantage as the prize

None of these steps is one-and-done. Resilience requires constant investment. And while manufacturers face special challenges, their commitment to both technological and organisational adaptation can bring the same payoff that every company that gets this right will enjoy: competitive advantage. Resilient organisations adapt quicker to risks and threats and recover faster when incidents do occur. That drives value for customers and investors alike and positions a company for long-term success.

About the Author

Abel Archundia is Managing Director for Global Life Sciences & Industrials at ISTARI. Previously he was Global CIO at Bayer Pharma, and at Novartis' Sandoz Division. He started his career as a consultant at BCG and was later responsible for Dell's business unit in Mexico.

If you would like to explore this topic in more depth, please contact the author:
abelarchundia@istari-global.com

Sources

[1] IBM (2020). Cost of a data breach report. (https://www.ibm.com/security/data-breach)
[2] Hope, A. (2020). DoppelPaymer ransomware attack disrupts Foxconns operations in the Americas, hackers delete terabytes of data, demand $34 million. CPO Magazine (https://www.cpomagazine.com/cyber-security/doppelpaymer-ransomware-attack-disrupts-foxconns-operations-in-the-americas-hackers-delete-terabytes-of-data-demand-34-million)
[3] Russon, M. (2021). US fuel pipeline hackers 'didn't mean to create problems'. BBC (https://www.bbc.com/news/business-57050690)
[4] BlueVoyant (2020). Understanding the frailty of the software supply chain. Bluevoyant (https://www.bluevoyant.com/blog/understanding-the-frailty-of-the-software-supply-chain)