TATA CONSULTANCY SERVICES

Building on belief

Six cybersecurity challenges facing manufacturers

TCS Risk & Cybersecurity Study:
Manufacturing Report

Six cybersecurity challenges facing manufacturers

Weighing the current 24/7 production schedule against the future risk of cyber threats lies at the heart of the manufacturer's paradox

Protecting manufacturing systems from cyberattacks is a critical but, in TCS' experience, often underinvested need in companies ranging far beyond traditional manufacturers such as automobile, steel, and chemical makers. Many more industries today have their own flavor of operational technology, from the fleet management of giant cargo ships to retail point-of-sale hardware to data center thermostats. While some of these capabilities have leapfrogged the security challenges facing manufacturers by being more recently developed and deployed, the risks threatening to take factories offline have the potential to affect the widest possible range of industries.

The manufacturer’s paradox

As operational technology (OT) is increasingly connected to IT systems and the Internet, it becomes more vulnerable to attack, as can been seen in rising cyberattacks on critical industrial control systems and network-connected assets.

A recent TCS survey, along with interviews with manufacturing cybersecurity executives, reveals six major challenges for manufacturers:

Challenges for manufacturers

1. Manufacturers struggle to balance security with the uptime required to make the most efficient use of expensive production machinery.
2. Many manufacturers underestimate their vulnerability to attack.
3. A complex mix of manufacturing systems makes it difficult to identify and remediate security risks.
4. The age and proprietary nature of many manufacturing systems makes them difficult or impossible to update with security patches.
5. The manufacturing workforce tends to be less aware of and skilled in the use of digital technology than those in other industries.
6. A lack of coordinated oversight of IT and OT makes it more difficult to properly identify, prioritize, and remediate risk.

The TCS Risk & Cybersecurity Study of more than 306 chief information security officers (CISOs) and 301 chief risk officers (CROs) was conducted in 2022 via survey and in-depth interviews amid an unprecedented upsurge in increasingly sophisticated cyberattacks from criminals, sovereign states, and other bad actors exploiting global socio-political and economic tensions. The survey respondents were drawn from North American, European, and UK-headquartered companies in four industries — manufacturing, banking and financial services, utilities, and media and information services — facing an unprecedented range of cyber threats and increased risks, whether to business data, customer data, operations, trade secrets, or supply chains.

In this report, we examine the greatest security risks manufacturers face, explore how effectively these 75 CISOs and 75 CROs collaborate on security, and offer suggestions for improvement based on our work with manufacturers worldwide.

Balancing uptime and security

The staff managing the manufacturing systems controlled by OT have traditionally focused more on uptime than data security for a good reason. If a production line shuts down, there is an immediate and severe impact on revenue. Cyber-related outages, while potentially much more damaging to the business and its long-term prospects, tend to happen downstream and at a later date from the actual moment of the breach.

This is not to say that security is not a consideration in OT systems; in fact, security is top-of-mind for most OT system operators, but OT and IT define security priorities differently.

For one thing, in OT security, safety (the number one consideration) trumps all others and is nonnegotiable. For its part, IT security generally puts its governing principles — confidentiality, integrity, and availability — in reverse priority order than the way those same principles influence OT security. (See Figure 1.)

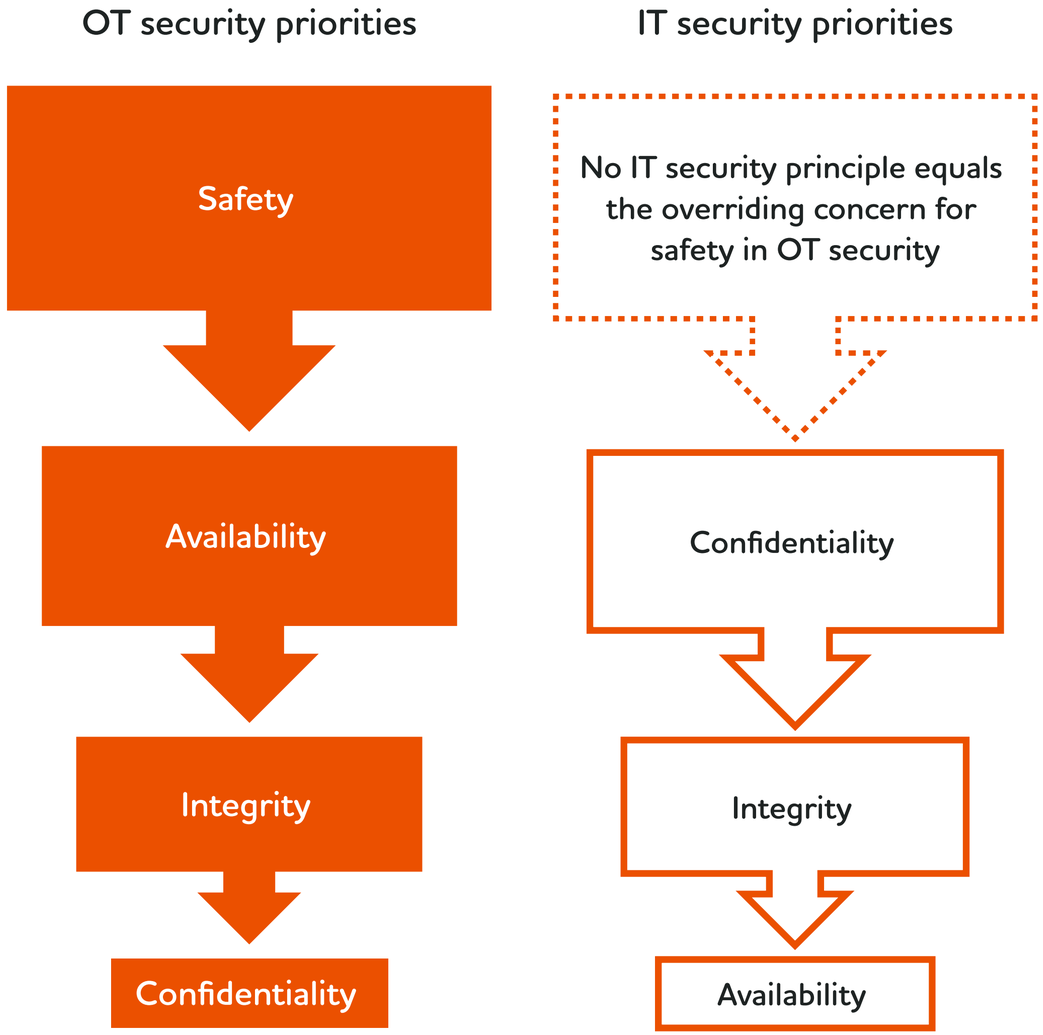

Figure 1

Balancing uptime with security

Despite the seeming cross-purposes of IT and OT security, there are some indications that the balance is shifting as more manufacturers recognize the increasing risk their OT systems pose to the business if they remain unprotected from cyberattacks. In our survey, more than one quarter of chief information security officers said they expect to increase their OT security budgets by at least 15% in the next fiscal year. (See Figure 2.)

Nevertheless, cybersecurity overall remains a lower priority for manufacturing compared to other industries, at least measured by budgets. For the overall information security budget of manufacturing companies, 59% of CISOs reported increases over the prior year — more than 10 points lower than the percentage of CISOs in other industries who reported the same. (See Figure 3.) Among their CRO counterparts, slightly less than half in manufacturing saw budget increases, which is more in line with CROs in other industries. And manufacturing CROs were less likely to see budget decreases than were CROs in other industries.

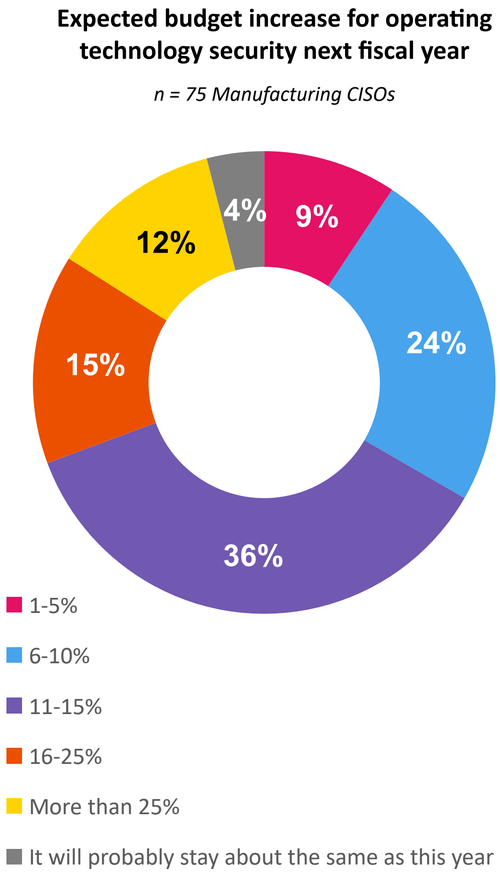

Figure 2

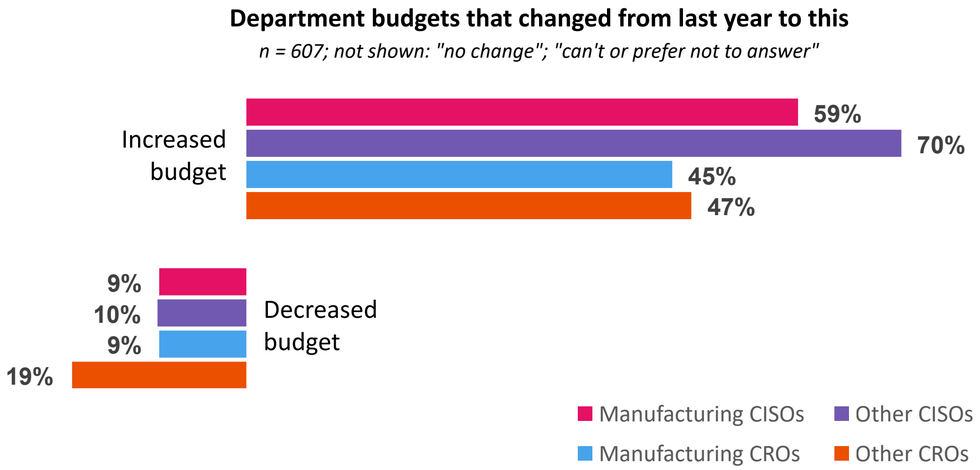

Figure 3

| Underestimating risk

Historically, manufacturers have believed they are unlikely targets of hackers because they do not store as much information about consumers as a retailer or a financial services organization would. They may also lack up-to-date information about the degree to which assets are linked to the internet. Such interconnections today often help optimize performance — but, without a full inventory of such interconnections, can also make manufacturers vulnerable to intrusions and malware.

Yet more traditional IT security threats — including the need to protect consumer data and intellectual property such as product designs, proprietary manufacturing processes, and customer lists — are real for some manufacturers. Protecting customer data and thwarting hackers who attempt to trick his company's employees into wiring money are the main concerns for the CISO at a US-based manufacturer. "Customer data in our case is a broad church," he says, and includes those who register products on its web sites and those whose data is protected by government regulations.

Corporate functions expected to see the greatest number of cyber attacks between now & 2025	Manufacturing CISOs & CROs *n = 150*	Other industries *n = 457*
Customer databases	1	2
Finance	2	1
Manufacturing plants/production/procurement	3	9
Sales/ecommerce	4	4
R&D	5	3
Distribution/supply chain	6	10
Human resources	7	6
Legal	8	8
Marketing	9	5
Ecosystem partners	10	7

Figure 4

Underestimating risk

Manufacturers are more aware of the potential for cyberattacks to leverage supply chains and distribution channels as their vectors, ranking these 6th compared to other industries' average ranking of 10 out of 10. (See Figure 4.) However, manufacturers seem unaware of the cyber risk presented by partners in their digital ecosystems — those data suppliers, buyers, aggregators, and service providers that have become central to global business today.

While risks from such ecosystem partners ranked low for manufacturers overall, some are more aware of and are working to mitigate security lapses in their business partners that could give hackers a path to attack their systems. For example, the CISO for a European manufacturer assures its business partners have "the same level of security that we are running" as well as segregated access to only the applications and data each should see. It also has created "standard contractor clauses to make sure everyone is signing on to the same level of security that we are willing to support" and agrees to third-party security audits.

Attacks on business partners can be a risk even if the hacker doesn't use the relationship with a business partner to attack the manufacturer's systems directly, says the CRO for a US manufacturer. He describes cases where "our customer said they got faked invoices thinking that they're coming from us and then they paid the hacker, and after this, they say they don't want to pay us again, and then we have to discuss it with our lawyer."

| Complexity

CISOs and CROs ranked the complexity of managing their cybersecurity initiatives amidst the variety of workforce changes as their most daunting challenge. For manufacturers, “closing the workplace” (and suppliers closing their plants) due to COVID infections meant not only a total lack of revenue but diminished oversight and accountability for those operations remaining open. And manufacturing was one of the industries where “work from home” was often impossible to define or even imagine. (See Figure 5.)

Also hindering cyber initiatives: the mix of OT systems acquired over the years or through mergers and acquisitions, which make it difficult to identify and remediate security risks or even to determine the proper level of security investment. Manufacturing facilities have historically had great latitude in choosing their own equipment, which also adds to the complexity. Manufacturing cyber executives ranked this complexity of their accumulated processes and operations among their top three challenges, tied with their firms’ continued reliance on legacy IT systems.

The greatest challenges to cybersecurity & risk mitigation initiatives	Manufacturing CISOs & CROs *n = 150*	Other industries *n = 457*
Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.)	1	3
Skill sets to manage, engineer & support cybersecurity technology	2	1
Reliance on legacy IT systems	3	4
Accumulated complexity of our own business processes & operations	3	5
Lack of diversity (including of thought & experience) in staff assessing cyber risks & threats	5	9
Difficulty in demonstrating return on cybersecurity investments	6	7
Assessing cyber risks & quantifying relevant costs	7	2
Budget constraints	8	11
Difficulty in mandating that our current vendors adopt advanced technologies & policies	9	8
Lack of collaboration across enterprise units (business, IT & security)	10	6
Competing interests for the board or senior leadership	11	10
Outdated, siloed & non-integrated security tools	12	12

Figure 5

Complexity

The need to better understand these complex environments, including the risks posed by unsecure supply chain partners and geographically distributed manufacturing facilities, is reflected in the importance the CROs attach to understanding their concentration risk and identifying critical operations. (See Figure 6.)

And while every industry's CROs ranked gaining a view into the "identification and clear ownership of digital assets" in the top half of resiliency priorities, in manufacturing the problem of lacking a view of a company's threat landscape is acute.

Systems and assets that were once assumed to have been air-gapped from network connectivity have been connected — for reliability, availability, and safety reasons — using rudimentary protocols. Yet if CROs don't understand the asset landscape, they can't understand the threat landscape, and therefore have a limited view into the impact on other parts of the process when one part is breached by hackers.

Most important to cyber resiliency between now and 2025	Manufacturing CROs *n = 75*	Other industries *n = 226*
Understanding concentration risk (e.g., information assets, suppliers, geographies)	1	3
Integration of cyber & business strategies	2	2
Identification of critical operations of core business lines	3	1
Identification & clear ownership of digital assets	4	4
Plans for business continuity/disaster recovery	5	5
Measurements of resilience	6	8
Partnerships with industry groups, government agencies	7	7
Fostering an organizational culture of resiliency	8	6

Figure 6

| Older, difficult-to-upgrade systems

The high cost (and far longer depreciation period) of manufacturing systems means OT environments have much longer lives than IT systems. This often means they do not comply with the latest security protocols as dictated by IT standards and may be difficult or impossible to update with security patches, especially if the update requires downtime.

This is one reason more than half of manufacturing CISOs believe they are not keeping up with the more sophisticated threats presented by professional hackers. (See Figure 7.) Nearly one-third of manufacturing CISOs say they are still using the most basic, out-of-the-box enterprise solutions — such as those relying on definition lists of known viruses — even as they agree these are insufficient to fight more sophisticated attacks.

To be sure, other industries' CISOs have similar confidence levels in their cyber capabilities. But for CISOs in manufacturing, the potential attack surface is generally older and less amenable to implementing modern cyber solutions.

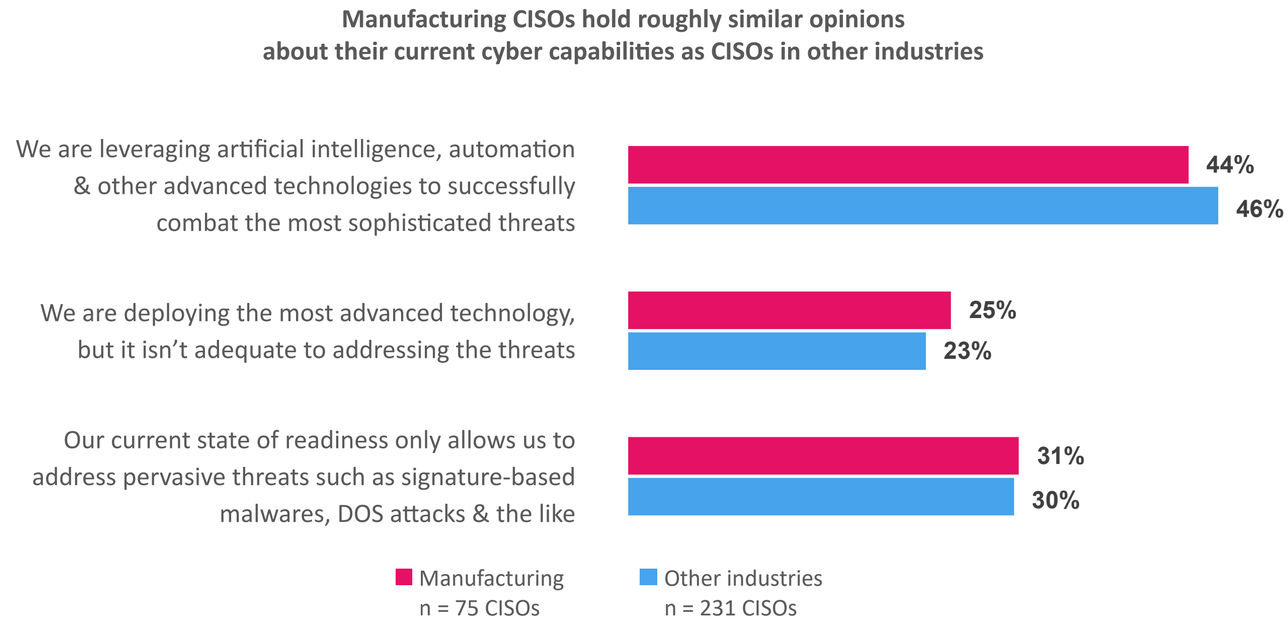

Figure 7

| Staff and skill shortages

On average, the manufacturing workforce — trained for decades to ensure equipment safety and production readiness — tends to be less aware of and skilled in the use of digital technology than employees in other industries. This means they may need more education about how to mitigate security risks. Manufacturing CISOs ranked enterprise-wide employee awareness and training regarding security second on their priority list, higher than in any other industry we surveyed. (See Figure 8.)

“There's a compulsory training time each year for each employee,” says the CRO for an Italian manufacturer, with the percent of employees completing the training included in the manufacturer’s risk reporting. Supervisors are alerted to employees who have not completed the required training.

CISOs‘ work priorities	Manufacturing CISOs *n = 75*	Other industries *n = 231*
Establishing a more robust cybersecurity strategy	1	2
Enterprise-wide employee awareness & training	2	6
Enhancing security governance & risk management (e.g., assessing the security posture of the company, defining controls & standards, etc.)	3	1
Security talent acquisition & development	3	3
Executive/board mandates on cybersecurity risks	5	6
Regulatory or industry compliance mandates	5	9
Implementing models like "zero trust"/perimeterless security	7	5
Managing ecosystem & supply chain risks	8	8
Strengthening enterprise-wide cyber hygiene (patching, hardening, etc.)	9	4
Outsourcing our security operations	10	10

Figure 8

Staff and skill shortages

Additionally, manufacturing CISOs ranked recruiting and retaining talent with the right skills to manage, engineer, and support cybersecurity technology as their top roadblock to implementing cybersecurity initiatives. (See Figure 9.) Their CRO counterparts, however, ranked it only fifth — perhaps demonstrating a divergence of agendas. (By contrast, for example, banking and financial services CROs ranked the lack of skills to run cybersecurity technology first among their obstacles to risk mitigation initiatives and CROs working for utilities — another industry wholly dependent on its OT systems — ranked the skills shortage second.)

This "splintered" view — in which manufacturing CISOs ranked "difficulty in demonstrating return on cybersecurity investments" seventh as a cybersecurity challenge but CROs ranked it first, and CROs ranked the "accumulated complexity of business processes and operations" seventh, even though CISOs consider it the second greatest hamper to cybersecurity and risk mitigation initiatives — is evident in other areas, as well.

The greatest challenges to cybersecurity & risk mitigation initiatives	Manufacturing CISOs *n = 75*	Manufacturing CROs *n = 75*
Skill sets to manage, engineer and support cybersecurity technology	1	5
Accumulated complexity of our own business processes and operations	2	7
Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.)	3	3
Reliance on legacy IT systems	4	2
Assessing cyber risks and quantifying relevant costs	5	10
Lack of diversity (including of thought and experience) in staff assessing cyber risks and threats	6	4
Difficulty in demonstrating return on cybersecurity investments	7	1
Lack of collaboration across enterprise units (business, IT and security)	7	10
Difficulty in mandating that our current vendors adopt advanced technologies and policies	9	9
Competing interests for the board or senior leadership	9	12
Budget constraints	11	6
Outdated, siloed and non-integrated security tools	12	7

Figure 9

A splintered view of security

The increased digitization of manufacturing and use of networked OT expands the “threat surface” hackers can exploit and can magnify the effect of any attack across OT and IT systems. Yet manufacturers often lack the single point of security knowledge and control they need in their co-mingled systems environment.

We have found CISOs often lack adequate knowledge of or control over OT, while OT managers may lack an understanding of IT systems and how threats to those can spread to their OT systems. CROs often take a hierarchical, top-down view of risks and lack detailed knowledge of the OT environment required to understand the cyber risks their organizations face.

Yet only one-fifth of manufacturing CISOs and CROs said they coordinated and collaborated in their work with each other on a daily or semiweekly basis, compared with other industries where more than one-third of respondents said such collaboration occurs daily or several times a week. (See Figure 10.)

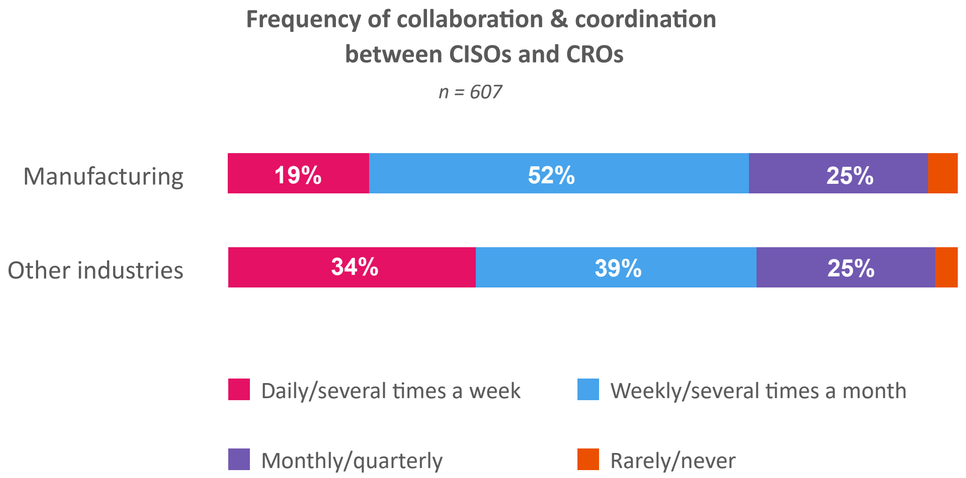

Figure 10

A splintered view of security

While there may not be as thorough a partnership between CISOs and CROs in manufacturing as exists in other industries, there are encouraging signs that the traditional segregation of OT security from IT security is at least diminishing at manufacturing firms. Where once OT security was solely the responsibility of the department also in charge of equipment maintenance and safety, today three-fifths of manufacturing CROs report that their CISO counterparts have some major involvement in OT security along with their IT security responsibilities, and a third of manufacturing firms center security for both IT and OT systems squarely with the information security staff. (See Figure 11.) Only a fifth of firms expect their general OT engineering department to also defend against cyber breaches and hacker attacks — if they even have such expectations at all.

Assigning responsibility for combined IT/OT security is still a work in progress, however. An Italian manufacturer segregates its OT security from IT to avoid a potential conflict of interest. “For example,” the CRO says, “the chief IT officer could say that the system is perfect because, simply, ‘We built it. We know it works. We know it's secure.’ Sometimes they're smitten with their own technological acumen rather than the understanding of what the threats are out there.”

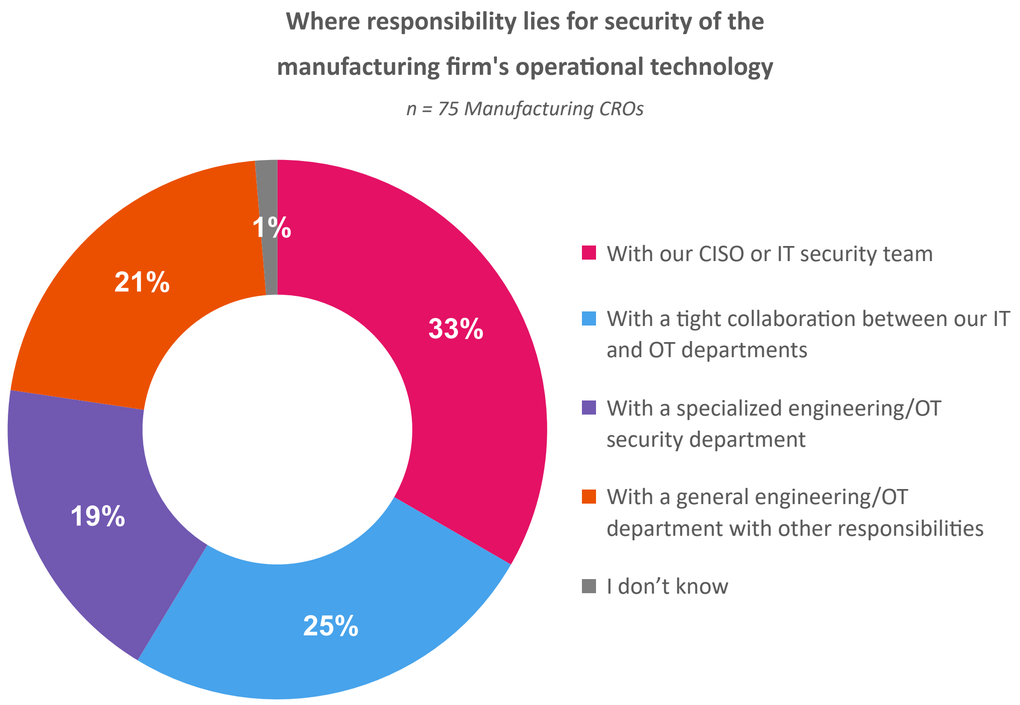

Figure 11

Meeting the manufacturer's challenges

Long gone are the days when you could have any color of Ford motor car "so long as it's black"

Even the notion of off-the-shelf, one-size-fits-all cybersecurity solutions for any large-scale enterprise in today's digitally integrated, globally networked economy has been consigned to the dustbin of history. Yet despite uniquely combined capabilities and bespoke configurations becoming readily available to manufacturers ready to secure their OT and IT systems against cyberattacks, some general principles have begun to emerge. These are six steps we're seeing forward-thinking manufacturers taking to better secure their critical business and operational environments. They don't necessarily require wholesale changes to BAU ASAP. In fact, many of them come down to good communications and creating a shared vision.

Recommendations

1. Understand and respect the OT culture, which is much more “hard hats and safety vests” than suits and ties, where professionals have historically been focused – with good reason – on uptime over all other considerations except for safety. Understand how this affects everything from networks that seem insecure by design (stripped of security protocols to reduce latency) to the presence of 20-year-old operating systems running the programmable logic controllers, because it often takes that long to amortize costly production equipment.

2. Build a relationship with the chief operations officer to whom your plant managers report and ensure his or her support for the sometimes difficult tradeoffs between security and the need for availability and output. Use examples to describe how a cybersecurity breach could harm the managers’ ability to meet their KPIs in areas such as production, uptime, and quality, and how in a networked world, a breach at one facility can spread to others.

3. Since it’s often impossible to immediately replace older, insecure technology, use internal firewalls to segment your OT networks so an attack on one part can’t spread to others. This “network segment by network segment” approach is also a less expensive and less risky way to introduce new security methodologies such as zero trust than an enterprise-wide rollout.

4. More than 150,000 security specialists worldwide are Certified Information Systems Security Professionals (CISSP), compared to only about 4,000 Global Industrial Cyber Security Professionals (GICSP), the certification that covers OT security specifically. Leverage the 65% to 70% overlap between the two by giving your more numerous IT security specialists the extra training they need to implement OT security.

5. Work to develop ways security can deliver financial benefits beyond preventing attacks. One example is a “digital twin” of your OT infrastructure that can be used to do penetration tests of your OT security that would be too risky with actual systems. The digital twin can also help fine-tune production and may eventually serve as a backup if an attack or technical failure disables your OT infrastructure. While you may only currently know about 50 percent of the assets you’d need to include as part of your digital twin(s) to be effective, you can move the number toward 95 percent (or higher) and make the inventory process manageable by conducting it one geography or business unit at a time.

It is possible to overcome the 10- or 20-year lag in awareness and maturity between IT and OT cybersecurity.

But success requires understanding the fundamental differences between IT and OT systems and adapting IT security thinking and processes to the unique needs of the nuts-and-bolts OT world.

Executive champions

Santha Subramoni
Head, Cyber Security Practice, TCS

Margareta Petrovic
Managing Partner, Risk & Cyber Strategy, TCS

Contributors

Marcel Wright
Program Director, Risk & Cyber Strategy, TCS

Lucien Sikkens
Consultant, Risk & Cyber Strategy, TCS

Ganesh Subramanya
Solution Architect, Cyber Security Practice, TCS

For the most up-to-date content and news, download the 'TCS Perspectives' app for your iOS and Android device.

Download on the App Store

ANDROID APP ON Google play

Get more insights

If you would like to have more information on the TCS Risk & Cybersecurity Study, please visit on.tcs.com/risk-cybersecurity

For more information or any feedback, email the TCS Thought Leadership Institute at TL.Institute@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 50 years. TCS offers a consulting-led, cognitive powered, integrated portfolio of business, technology and engineering services and solutions. This is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 600,000 of the world's best-trained consultants in 46 countries. The company generated consolidated revenues of US $25.7 billion in the fiscal year ended March 31, 2022 and is listed on the BSE (formerly Bombay Stock Exchange) and the NSE (National Stock Exchange) in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit **www.tcs.com** and follow TCS news **@TCS**.