Manufacturers ramp up cyber defenses as supply-chain bottlenecks – and vulnerabilities – deepen

February 2022

pwc

NATIONAL ASSOCIATION OF Manufacturers

Manufacturers worldwide are being targeted by cybercriminals at an astonishing − and increasing − rate. The rise in cyber attacks is particularly concerning given that it's occurring during a period of entrenched supply chain bottlenecks. At the same time, manufacturers are experiencing increased vulnerabilities to their businesses due to weaknesses in their supplier networks. Building cyber security protection throughout the supply chain has, therefore, become increasingly critical to achieving not only cybersecurity writ large, but also supply chain agility and resilience.

> Last year, the number of cyberattacks on manufacturers spiked by more than 300%, accounting for 22% of all attacks across all sectors, up from 7% the previous year.
>
> **Source:** 2021 Global Threat Intelligence Report, NTT, 2021

The highlights

Last year, the number of cyberattacks on manufacturers spiked by more than 300%, accounting for 22% of all attacks across all sectors, up from 7% the previous year. That makes manufacturers the second most attacked, up from fifth the previous year.[1] According to PwC's 2022 Global CEO Survey, nearly half (49%) of respondents agreed cyber risks pose the number-one threat to their growth.

This rise in cyber attacks on manufacturers has been triggered by converging and intensifying factors. Vulnerabilities have deepened during the pandemic as hybrid workforces, remote work and the sudden need to create a "no-touch" work environment have accelerated the deployment of digital solutions, including cloud technologies, client portals and mobile and web-based apps, all of which need to be properly monitored and patched. Additionally − especially for bigger enterprises − there are the perennial challenges of creating and monitoring stringent cybersecurity programs and protocols at numerous facilities − as well as their complex third-party networks − both in the US and around the globe.

These trends and conditions have hardly gone unnoticed by criminals. Most cyber attacks on manufacturing firms last year occurred via application-specific breaches (49% of all attacks) or reconnaissance activity (24%) − the covert discovery and collection of information about a system followed by hacking or system penetration.[2]

To learn more about how industrials are battling against cyber threats on numerous fronts (shop-floor, supply chain and customer) and how cybersecurity has become a core business priority, PwC carried out a global survey of industry leaders in our 2022 Global Digital Trust Insights Survey. For this report, prepared in collaboration with the National Association of Manufacturers, we delve into the survey results of our US manufacturing sector respondents. We also conducted interviews with chief information security officers (CISOs) at five leading US manufacturers, and we share their insights, too.

[1] [2] 2021 Global Threat Intelligence Report, NTT, 2021

Some key findings

- Most US industrials sector executives expect cyber threats to increase in 2022, with 66% saying they believe there will be increased threats from cyber criminals, hacktivists (62%) and nation-states (60%).
- Increasing complexity is creating critical vulnerabilities. Most of these executives agree that complexity across their organization poses cyber and privacy risks at "concerning levels." Complex cloud environments pose risks for 81% of respondents, as do complex governance of data (79%).
- Cyber lies at the core of business, attested to by 82% of respondents agreeing that they've seen an increased alignment of cyber strategy with business strategy over the last two years. Another 82% say recent key mergers and acquisitions have involved cybersecurity considerations.
- Supply-chain risks are the next big thing. Sixty-three percent of sector leaders expect that third-party threats will increase in 2022 over 2021, with 58% anticipating an increase in reportable incidents occurring at the supply chain software level.

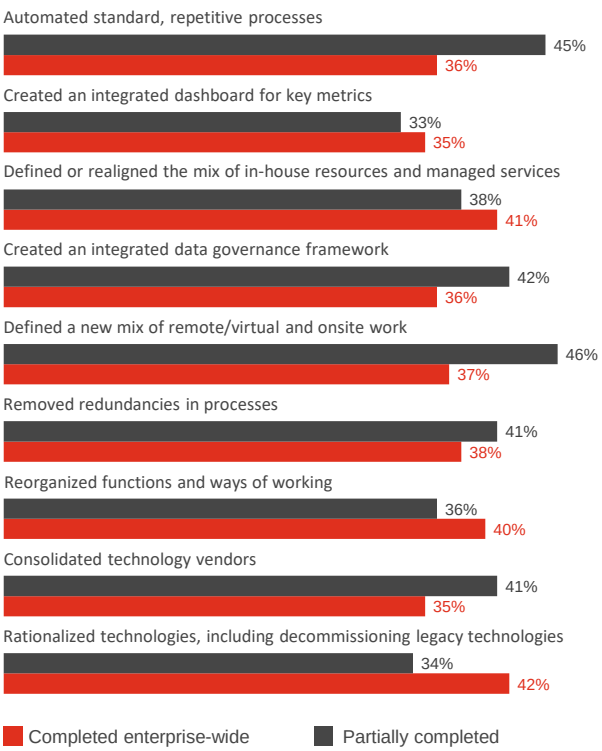
Is too much complexity now Industry 4.0's Achilles' heel?

Manufacturers face a quandary. In a race to adopt Industry 4.0 technologies, they run the risk of widening their attack surface − not only in their operations but also in their supply chain network and products and services. Even so, many are making headway by streamlining their operations in order to reduce their cyber vulnerabilities. Part of the increasing complexity for manufacturers lies in the sheer number of legacy assets they need to monitor, some of which require retroactive cyber-proofing or even retirement.

Still, industrials are well aware of the inherent exposure that complexity can create. Respondents cite financial losses due to successful data breaches or cyber attacks as the number-one consequence of complexity on business, followed by lack of operational resilience or inability to recover from a cyber attack or technology failure.

But manufacturers are on their way to reducing this complexity. Consider that 76% of our respondents, over the last two years, have either completely or partially completed enterprise-wide rationalization of technologies, including decommissioning legacy assets. An equal percentage tell us they've consolidated technology vendors as a path to reducing complexity.

Manufacturers streamlining operations to reduce complexity



Q. In the last two years, to what extent has your organization streamlined operations in the following ways?

Note: Respondents include US industrial products companies representing the following sectors:
Aerospace and Defense, Automotive, Chemicals, Engineering and Construction, Forest, Paper and Packaging, Industrial Manufacturing.

Number of respondents: 149

Source: 2022 PwC Digital Trust Insights survey, 2021

> Manufacturers have typically thrived on productivity. But now we need to accept that while building in cyber controls − such as installing patches − may cause a momentary slowdown in productivity, doing so may avert weeks or even months of low productivity.
>
> Rodney Masney, CIO, O-I Glass

> The older a plant is, the more difficult it can be to secure due to legacy hardware, software, networking, and architectural design. Acquisitions further increase the complexity, making it difficult to drive a consistent security strategy across all plants. The best way to get budget support behind OT cyber initiatives is to quantify the risks as best you can. How long would it likely take to recover a plant if it were hit by a cyberattack? If multiple plants were impacted, for example in a ransomware attack, priorities for recovery need to be discussed with and agreed to by company leadership since you will likely not have enough resources to recover all plants simultaneously. Plant managers have accurate productivity metrics − use those to calculate a rough estimate of the potential cost of a cyber breach in the company's OT environment.
>
> Dawn Cappelli, Vice President and Chief Information Security Officer, Rockwell Automation

> By its very nature, manufacturing can be far more complicated than other industries, which tend to be more homogenous. We also have 200 factories in 28 countries, so we need to centrally manage these facilities with the same rigorous cybersecurity standards around the globe. We contend with legacy equipment which can introduce vulnerabilities. Manufacturers have traditionally built lowering worker accident rates into their workplace culture. In the same way, we're prioritizing cyber hygiene and cybersecurity and building that into our culture.
>
> Tony Parrillo, VP Enterprise IT Global Head of Security, Schneider Electric

Securing against the most important risks to business

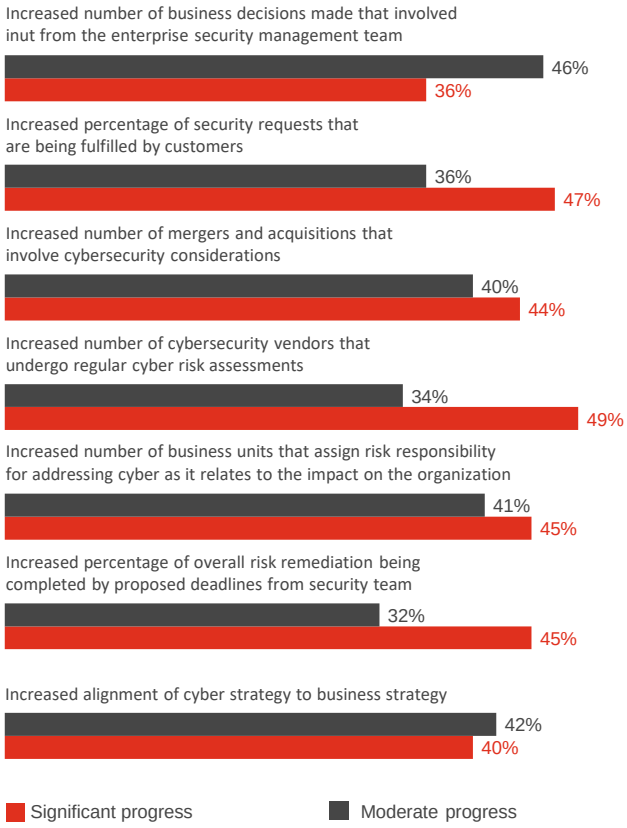
Nearly three in four manufacturing executives agree that strengthening cybersecurity to protect hybrid work arrangements brings about “some or significant” improvements for their business. Likewise, two-thirds (67%) report that building security into cloud adoption and migration would support their organization. The challenge is how to optimally allocate limited resources.

Monitoring and quantifying risk today is a constant battle. While manufacturers know that there is no such thing as too much security, they also know that they only have so many resources − both human and technological − at their disposal to secure and defend their businesses, customers and supplier partners. With so many areas of potential vulnerability, businesses need to quantify the risks they may be exposed to in order to prioritize the right resources to confront the most critical threats. When asked about the most important reasons to quantify risk, our respondents said their top two were both related to validating their investments in cybersecurity.

How are manufacturers typically monitoring cyber risk and threats? On many fronts. About four in five are using a two-pronged approach to make investment decisions and to monitor use of real-time threat intelligence:

- Implementing generally accepted standards and frameworks (e.g., NIST, CMMC, ISO), and
- Using autonomous threat detection, including cognitive security.

Manufacturers making progress in aligning cyber with overall business strategy



Q. How much progress in alignment between cybersecurity and overall business goals has your organization made in the past two years?

Note: Respondents include US industrial products companies representing the following sectors: Aerospace & Defense, Automotive, Chemicals, Engineering & Construction, Forest, Paper and Packaging, Industrial Manufacturing.

Number of respondents: 149

Source: 2022 PwC Digital Trust Insights survey, 2021

Cyber now sits at the core of business. As cybersecurity becomes more pervasive, industrials are integrating it into core business aims. For example, 82% of respondents agree that over the last two years, they’ve seen an increased alignment of cyber strategy with business strategy. Cyber has also affected deals, with 82% of industrials saying that recent key mergers and acquisitions have involved cybersecurity considerations.

Mind the IT/OT gap. Manufacturers continue to more closely align the cybersecurity efforts of their IT specialists with that of their operational technology (OT) team. This is a challenge especially germane to the manufacturing sector, and 76% of manufacturers agree that the crossover from IT to operational technology itself presents concerning intrinsic levels of risk.

Secure IoT products and services. As more manufacturers offer connected products and services, they will need to anticipate the potential for those offerings to be breached, thus opening a new and expanding attack surface. Monitoring, patching and event-reporting of IoT products and services, then, will become increasingly important.

> It's important to prioritize your cyber risk and protect your crown jewels such as intellectual property and customer information. What's at risk? What's the cost to mitigate against that risk? What's the damage that can be done if there is a breach? You need to know the answers to these questions. How fast can you detect it and how quickly can you recover?
>
> Tony Parrillo, Schneider Electric

> The role of the CISO is growing wider. We need to deal with security and privacy issues for our own organization as well as for our vendors and customers, and even our dealerships. Our relationships and communication with all these stakeholders has grown. OT [operational technology] is becoming a bigger priority, and we are leveraging what has worked well in securing the IT environment in the OT environment.
>
> Stephen Roberts, Division Manager for Information Security and Risk, Honda

> These are criminals we're talking about. We have to be smarter, faster and better than them. Simply spending more money on cyber security tools is not enough. You need to get the most out of all the tools at your disposal. The tool itself really doesn't matter. It's how well you use it, and how much you get out of it.
>
> Rodney Masney, O-I Glass

> Most large companies have the resources to build cybersecurity into their products. But I am concerned about the small and medium- sized enterprises which may not have the resources or expertise. So, as a community, we all have to work together to help support these companies because we are only as strong as our weakest link. It is imperative that we raise the security posture of the entire ecosystem.
>
> Dawn Cappelli, Rockwell Automation

The next big thing for industrials: Third-party and supply-chain risks

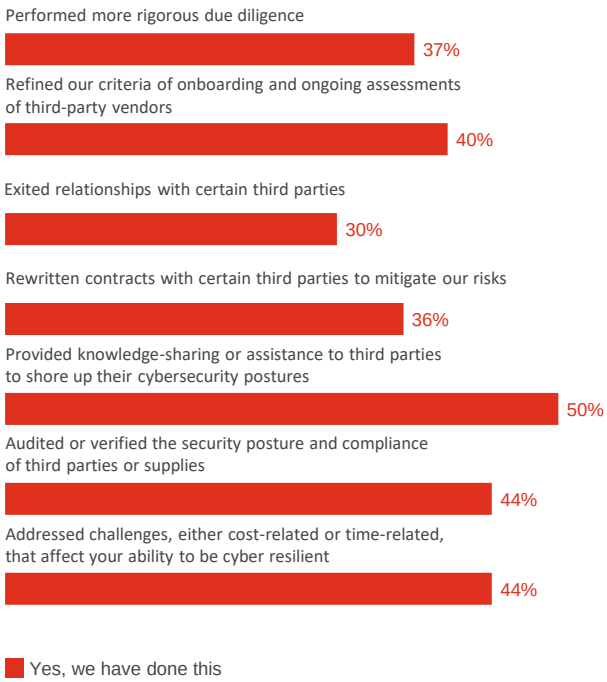
How well do industrials grasp the risks posed by their suppliers? Half (50%) of respondents say they have a high understanding (from formal, enterprise-wide assessments) of data breaches in their supplier network. In other areas, their understanding of third-party risk appears more opaque, with only about one-third (34%) agreeing that they have a high understanding of nth-party risks and 59% saying their understanding of software supply chain risk is "moderate" or "low."

Chasing supply chain risk? Supply chain risks are very much on the radar, with 63% of industry leaders expect that third-party threats will increase in 2022 over 2021, and with 58% expecting to see an increase in reportable incidents occurring at the supply chain software level.

As supply chain disruptions and acute shortages of some materials, parts and components persist, manufacturers are increasingly collaborating more closely with their supply chain partners. Such collaborations typically involve greater data sharing and other internet-enabled connections. This increased digital connectivity with suppliers significantly expands new entry points that cybercriminals can attempt to exploit, thus also expanding the manufacturers' attack surface.

As a result, manufacturers are taking action. In the last year, for instance, one in two manufacturers provided information-sharing or assistance to third parties to shore up their cybersecurity postures. Nearly four in ten respondents (36%) have rewritten contracts with certain third parties to mitigate risk, and 30% altogether exited partnerships with third-party vendors (presumably as a result of unacceptable cybersecurity risks attached to them).

The next frontier in cybersecurity: honing in on supply-chain risk



Q. Has your organization done any of the following actions in the past 12 months to minimize third-party or supplier risks in your ecosystem?

Note: Respondents include US industrial products companies representing the following sectors: Aerospace & Defense, Automotive, Chemicals, Engineering & Construction, Forest, Paper and Packaging, Industrial Manufacturing.

Number of respondents: 149

Source: 2022 PwC Digital Trust Insights survey, 2021

The layers of third-party risk definitely exist − not only in the hardware but also when there is software embedded in products and components. Every chunk of software needs to be checked and confirmed that there is no corrupt code. It's an enormous undertaking. We're in constant conversations with our suppliers and are synergistic in carrying out cyber controls and sharing information not only with the suppliers but also with our customers. We have open and frank conversations. It's so important to have mutual trust.

Tony Parrillo, Schneider Electric

We look at cybersecurity through the prisms of threat management and vulnerability management. We're constantly adding potential risks into our risk registry. We have hundreds of suppliers, and are constantly assessing risks of what we procure, and actually rate our vendors. If a given vendor receives a low rating, then we work with them to make improvements and work through issues. And, if for whatever reason they cannot improve, then we will look for another vendor.

Stephen Roberts, Honda

It's a challenge for any company to secure their supply chain, and it's especially difficult in a converged IT/OT environment. Consider the increasing number of connected products, suppliers needing remote access to plants, and suppliers with access to confidential information, including trade secrets. We need to strengthen our relationships and partnerships with vendors to ensure that their security posture is as strong as ours. But even when you do this, one must also contend with the nth-party risk, which can be trickier. Most large Industrial Control Systems vendors like Rockwell have been obtaining IEC 62443 security certifications, which require secure development lifecycle processes. To be certified at increased maturity levels, our software suppliers must also implement a secure development life cycle. We've been working for years with our hardware and software suppliers to make sure that they have a strong security posture and secure development lifecycles. This is especially important because our products are used in every one of the nation's critical infrastructures. So, our cyber security controls in our products become a human safety issue.

Dawn Cappelli, Rockwell Automation

Bracing for the (formidable) future

Looking ahead, manufacturers are continuing to up their cybersecurity game. Top goals for the next three years include achieving more successful outcomes for their organization's transformation, preventing attacks and gaining more confidence of leaders in their ability to manage current and future attacks.

To help them hit these and other goals, industrial enterprises plan to expand budgets to bolster their cyber acumen and capabilities − an expansion that exceeds the average across all other industries. Seventy percent of manufacturers plan on increasing their cyber budgets in 2022, including nearly half (49%) planning increases of between 6% and 14%.

Which threat vectors do industrials expect to increase in activity in 2022 compared to what they experienced in 2021? According to our survey, 70% expect increased threats through mobile technology, followed by 69% who anticipate them to come through IoT devices and cloud service providers.

In terms of the rise in types of reportable incidents that manufacturers are expecting for 2022 (compared to what they experienced in 2021), 69% anticipate an increase in incidents at cloud-service levels followed by cryptomining (60% expecting increases) and attacks on supply chain software (58%).

> OT security is the next frontier. IT and OT have traditionally had very different cultures and environments. But at Rockwell we pulled together the IT and security specialists along with plant managers and plant engineers in early 2017 to develop a strategy together. They have joint ownership of the strategy and have been working in tandem ever since to execute and learn from each other. We need OT security to be as sophisticated as IT security. They should − and can − be at the same level of sophistication − if IT and OT will work together. This will be particularly challenging for small manufacturers that do not even have a strong IT security program.
>
> Dawn Capelli, Rockwell Automation

Contacts

To have deeper conversations about how this subject may affect your business, please contact:

Aaron Schamp
Principal, Consulting Solutions, PwC US
aaron.j.schamp@pwc.com

Harshul Joshi
Principal, Consulting Solutions, PwC US
harshul.joshi@pwc.com

Joseph Nocera
Cyber and Privacy Innovation Institute Leader, PwC US
joseph.nocera@pwc.com

www.pwc.com