Why cybersecurity is the backbone of smart manufacturing

Keeping data safe and making it more effective

verizon

From SmartBrief

Today's manufacturers must be nimble and resilient, able to make near-real-time decisions using large stores of data without being limited by legacy systems and inflexible networks.

Having the right information and being able to act on it quickly requires fast connectivity, mobile edge computing, AI applications, IoT and the cloud.

But the corresponding explosion in smart products and equipment, industrial IoT sensors and other technologies has created new challenges around protecting intellectual property and protecting factory equipment. Verizon's 2022 Data Breach Investigations Report shows the manufacturing industry is increasingly targeted by cybercriminals for denial of service attacks, ransomware and credential attacks.[1]

Manufacturers must address cybersecurity vulnerabilities that can threaten production and supply chains, resulting in unplanned costs. They need computing and network bandwidth to support advanced encryption, continuous monitoring for intrusion detection and proactive response, safeguards that extend across IT and OT networks, and the security offered by private wireless.

In other words, they need an end-to-end cybersecurity strategy encompassing the entire organization.

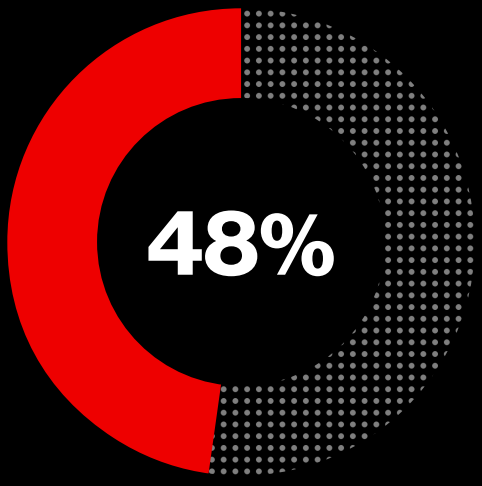
Challenges in manufacturing cybersecurity

The task of keeping proprietary manufacturing data secure, readily available and out of the hands of bad actors is growing more difficult.

Nearly half of the world's critical manufacturing industry is at risk of a data breach, according to a report from SecurityScorecard.[2] It found 48% of critical manufacturing providers in US government-designated "key sectors" received a C rating or below for cyberresilience.[2]

The adoption of smart manufacturing and the growing use of connected devices such as smart sensors and robotics equipment have created more potential intrusion points. These include manufacturing equipment, IT, operational technology like IOT, data stores, software and legacy systems.[3]

These vulnerabilities are not going unnoticed by bad actors, who target manufacturers using credential attacks, phishing, botnets and exploiting vulnerabilities. Experts at the World Economic Forum's Annual Meeting 2023 warned that cyberattacks are happening more often and becoming more sophisticated.[4] DDoS attacks increased 79% year-over-year in 2022, and other types of attacks are becoming more frequent as well.[4] Also, the number of ransomware attacks on industrial infrastructure nearly doubled in 2022.[5]



of critical manufacturing providers in US government-designated "key sectors" received a C rating or below for cyberresilience [2]

Further challenging manufacturers is the need for protection beyond their own organizations. The supply chain is a significant vulnerability and was responsible for 62% of system intrusion incidents in 2022.[1]

Manufacturers need to determine where they are vulnerable by conducting a thorough cybersecurity audit as they build the infrastructure of the future, and security must be a top priority in these transformations.

The consequences of falling short

Failure to properly secure data can bring significant consequences, including:

- Reputational harm and customer experience impacts.
- Lost revenue due to production shutdowns.
- Financial losses from ransom payments.
- Cost of work needed to diagnose and fix the problem, repair systems and bring them back online.
- The risk of proprietary data such as R&D and product plans being publicly exposed.[6]

Manufacturing breaches cost $2.8 million on average, and 98% of manufacturers that have been the victim of a breach or ransomware attack also experienced supply chain disruption.[7] Many find they need to temporarily shut down production lines because of a cyberattack.[7]

Unfortunately, these growing challenges and steep consequences come amid a shortage in cybersecurity talent, with 68 candidates on average applying for every 100 openings.[8]

Additionally, the economic uncertainty has created a "ripe environment" for hackers, said Merritt Maxim, vice president, research director for Forrester, on a recent webinar.[9] An increase in online employee interactions, coupled with large numbers of people leaving companies, means more vulnerabilities.

Maxim pointed to a resurgence of managed services that offer more value-add beyond standard monitoring, including more active detection. Managed services, such as those offered by Verizon, can play an important role for organizations that now need to do more with fewer resources. By leveraging cutting-edge technologies, they can get the most for their cybersecurity dollar.

Chris Novak, managing director for Verizon Cyber Security Consulting, added that organizations are increasingly taking a different approach to cybersecurity amid budget or headcount cuts. "Historically, we saw lots of organizations focus on trying to do it all themselves and now ... a lot of them are starting to say 'we need the same level of security but maybe doing it ourselves isn't always the answer.'"

Manufacturers need to determine where they are vulnerable by conducting a thorough cybersecurity audit as they build the infrastructure of the future, and security must be a top priority in these transformations.

Cybersecurity innovations for manufacturing

To address today's cybersecurity challenges, manufacturers can invest in:

- **Private networks** that provide greater speed and security to optimize facility operations and support technologies like augmented reality and automated guided vehicles.
- **Secure gateway solutions,** which are on-premise or cloud-based network security services that use company policies to approve or deny web requests from applications and websites.
- **Zero-trust frameworks** that verify every person and device every time, regardless of where they originate or whether they are already behind the corporate firewall.
- **Network detection and response** that can help flag and prevent intrusions before they occur. Managed detection and response flags anomalies as soon as possible so they can be addressed faster, potentially even catching a breach while it is still in progress.
- **IOT security and mobile device security,** such as credentialing, which prevents devices from being used as an access point and ensures each device and employee can access only the information necessary for a particular role.

The benefits of these technologies go beyond avoiding breaches. Manufacturers that prioritize digital innovation and security will also build smarter, more efficient and more agile operations.

How cybersecurity supports enterprise intelligence

The benefits of cybersecurity go beyond avoiding breaches. Tomorrow's successes will be achieved by healthcare organizations that prioritize digital innovation to build smarter, more efficient and more agile enterprises. Transformation starts by bringing together disconnected systems to create powerful, modular and intelligent solutions that can enable new functionality, smarter insights and faster decision-making. The result is Enterprise Intelligence.

For this, manufacturers need secure data at their fingertips and a real-time view across every access point on the network. For example, multi-access edge computing and 5G bring faster processing closer to the manufacturing facility. They offer ultra-low latency, helping companies gather more data faster to make better-informed decisions sooner. They can proactively monitor production equipment to avoid maintenance issues and reduce unscheduled downtime.[6]

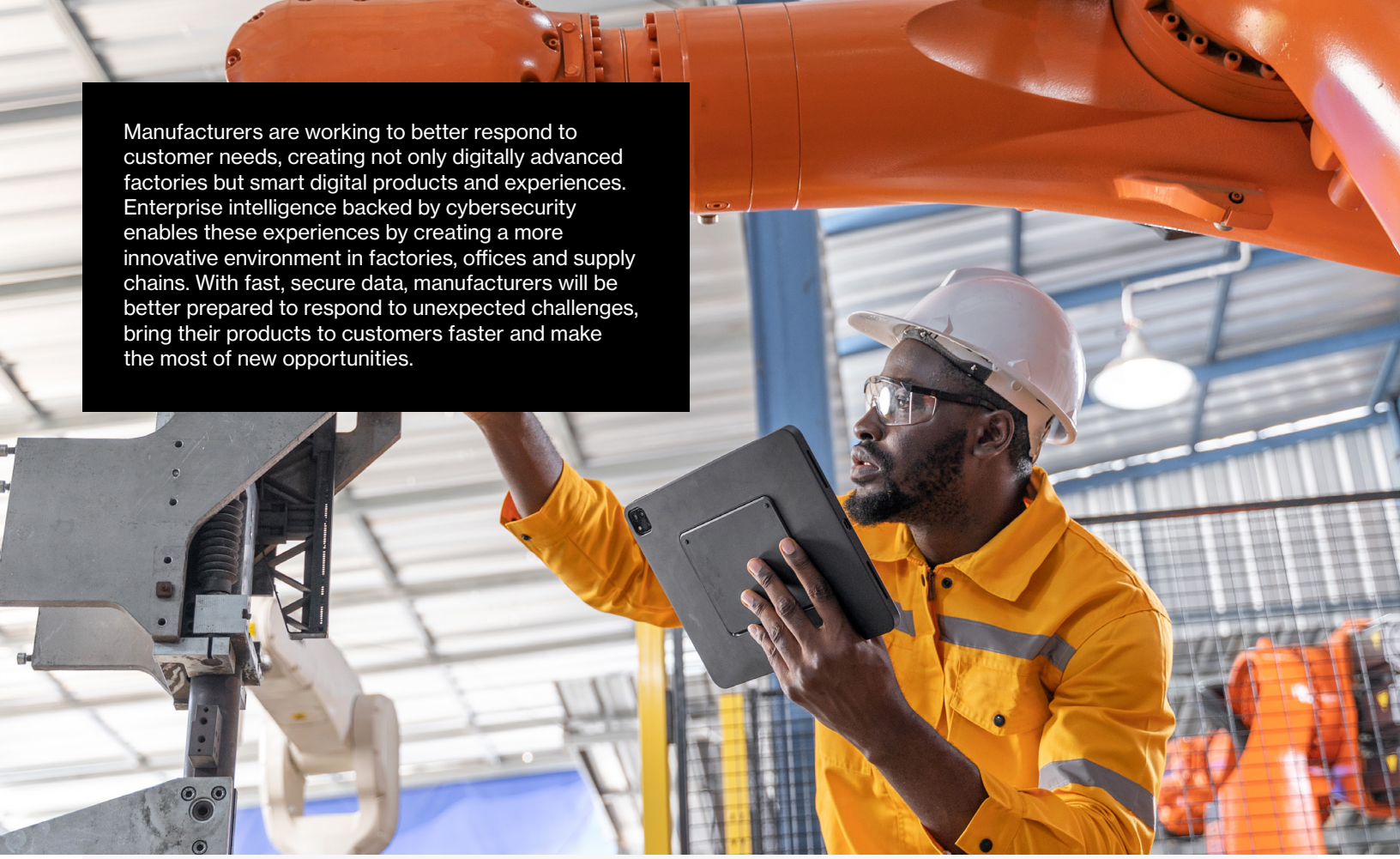
Faster data analysis also gives organizations maximum advance notice of global supply chain issues like semiconductor shortages, geopolitical instability, shipping bottlenecks, and mismatches between production and demand.

Meanwhile, AI is increasingly being used in cyber programs to identify vulnerabilities and threats, predict attacks on data, and provide alerts and recommendations for response. An organization that is operating with Enterprise Intelligence can leverage AI to identify and respond to threats in "real time." This requires a special blend of connectivity, edge computing, AI capabilities, cloud technologies and the embedded security of private networks. Enterprises that adopt these new solutions will complement connected assets with analytics, AI and machine learning to allow autonomous, secure decision-making.

Manufacturers that want to tighten cybersecurity and make the most of the rich data and smart technologies available to them can begin with a few simple steps:

First steps

- Start with a security program assessment.
- Follow up with a workshop or consultation to assess current programs and tech stacks for vulnerabilities, using exercises like executive breach simulations to see where there might be holes in the response plan.
- Work with a trusted solutions partner to create a road map for streamlining the security portfolio and programs.
- Save time and resources by working with a partner on consultations; private networks; remediation, resolution and recovery services; or fully managed security services.



Manufacturers are working to better respond to customer needs, creating not only digitally advanced factories but smart digital products and experiences. Enterprise intelligence backed by cybersecurity enables these experiences by creating a more innovative environment in factories, offices and supply chains. With fast, secure data, manufacturers will be better prepared to respond to unexpected challenges, bring their products to customers faster and make the most of new opportunities.

References

1. 2022 Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/
2. Jones, D. Almost half of critical manufacturing organizations face significant risk of data breach. Cybersecurity Dive. Jan. 23, 2023. https://www.cybersecuritydive.com/news/critical-manufacturing-cyber-risk/640951/
3. Newton, E. We need to make smart manufacturing safer with better cybersecurity. IoT For All. Jan. 17, 2023. https://www.iotforall.com/we-need-to-make-smart-manufacturing-safer-with-better-cybersecurity
4. Feingold, S. Experts at Davos 2023 call for a global response to the gathering 'cyber storm.' World Economic Forum. Jan. 18, 2023. https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/
5. Zabeu, S. Ransomware: Attacks on industrial infrastructure nearly doubled in 2022. Network King. Feb. 22, 2023. https://network-king.net/ransomware-attacks-on-industrial-infrastructure-nearly-doubled-by-2022
6. Apte, P. The 5G manufacturing industry can be transformational, but how do we ensure security? Verizon. https://www.verizon.com/business/resources/articles/s/iot-and-5g-manufacturing-industry-security-challenges/
7. Columbus, L. The manufacturing industry's security epidemic needs a zero-trust cure. VentureBeat. Nov. 15, 2022. https://venturebeat.com/security/the-manufacturing-industrys-security-epidemic-needs-a-zero-trust-cure/
8. Benoit-Kurtz, S. Facing the cybersecurity workforce shortages. Mission Critical. June 28, 2022. https://www.missioncriticalmagazine.com/articles/94163-facing-the-cybersecurity-workforce-shortages
9. Maintaining strong cybersecurity in turbulent economic times. Verizon/Forrester. Jan. 26, 2023. https://www.brighttalk.com/webcast/15099/570308

sponsored by verizon