CYBERSECURITY DIVE

OUTLOOK 2026

Cybersecurity 2026: AI, CISA, manufacturing sector all in the hot seat

Table of Contents

1 **5 cybersecurity trends to watch in 2026**
David Jones January 23, 2026

2 **CISA's 7 biggest challenges in 2026**
Eric Geller January 9, 2026

3 **Manufacturers fortify cyber defenses in response to dramatic surge in attacks**
Eric Geller and David Jones January 29, 2026

Cybersecurity 2026: AI, CISA, manufacturing sector all in the hot seat

A look at the most important trends and issues in cyber this year.

New year, new and more complex challenges for cybersecurity leaders, starting on the technology front: AI tools are revolutionizing ways of working for security operations teams while unfortunately also empowering cyber threat actors to amplify their attacks.

Meanwhile, the unprecedented wave of debilitating targeted cyberattacks that hit the manufacturing sector and disrupted operations at some of the biggest companies in the world over the past year serves as a stark wake-up call for critical infrastructure and other organizations to prioritize operational resilience.

At the same time, the very foundation of financial protection in the face of a cyberattack — cyber insurance coverage — has reached a tipping point. Insurers are now more closely scrutinizing policyholders' security postures, pressuring CISOs and executives to invest more in defense tools and potentially face higher premiums.

All eyes will be on the U.S. federal government agency tasked with protecting critical infrastructure and leading cybersecurity policy: the Cybersecurity and Infrastructure Security Agency, which is reeling after a year of massive workforce cuts and weakened private-industry partnerships. CISA's ability to adapt and lead will be critical to safeguarding national security and critical infrastructure.

But that is just a sneak-peek for 2026. Here is a deeper look at these and other critical cyber trends and issues to watch this year:



Getty Images

5 cybersecurity trends to watch in 2026

January 23, 2026

David Jones

Corporations across the globe are facing a dynamic risk environment, as AI adoption surges with few guardrails, business resilience takes center stage and the insurance industry raises major concerns about the U.S. cyber market.

The cybersecurity sector faced historic pressure in 2025. New AI tools changed the way we work, but at the same time posed new forms of cyber risk to organizations who adopt them.

Meanwhile, cybercrime groups employed an evolving menu of techniques to disrupt key industries, forcing businesses and government authorities to shift their emphasis toward operational resilience and managing the long-term financial impact of cyber incidents.

Here are five key trends that will shape cyber in 2026:

1. AI governance and guardrails now front and center

The adoption of artificial intelligence moved faster over the past year than most anyone could have anticipated.

An international arms race has commenced between major economic powers, led by the U.S. and China, over who will lead AI transformation. At the same time, companies are rushing to incorporate AI into their profit models, betting both on major gains in productivity as well as the technology supercharging their core product lines.

But this rapid embrace of AI brings growing concerns over whether companies have created the proper guardrails and governance structures to ensure their AI programs are secure and cannot be used by malicious actors to exfiltrate corporate data, exploit customers or compromise supply chains.

“There is a gap between how fast organizations are adopting AI and the maturity of their governance framework,” Morgan Adamski, cyber, data and tech risk deputy leader at PwC told Cybersecurity Dive. “Many are experimenting with agentic and generative AI to drive productivity or efficiency, but often, there are no guardrails in place from a security perspective.”

AI has moved quickly to become one of the top business cyber risks among global companies. A January report from Allianz Commercial shows AI risk jumped from number 10 to the second-leading business risk concern over the past year, based on a survey of more than 3,300 risk management professionals.

Look for AI risk to drive organizations in 2026 to focus more on establishing proper parameters and security for their AI programs.

2. Cybersecurity regulatory shifts shape disclosures

The regulatory environment for cyber has undergone significant changes in the past year. The Trump administration shifted toward a more nuanced approach, both in terms of oversight and implementation of cyber risk compared with how the Biden administration regulated it. That means oversight in the information security space is not going away but instead will allow markets forces more room to operate.

“Rather than uniformly pulling back or pursuing broad regulatory expansion, the government is continuing to assess where clearer expectations, coordination, or enforcement are warranted in response to a dynamic threat landscape,” said Haiman Wong, resident fellow, cybersecurity and emerging threats at the R Street Institute.

This is particularly the case for critical infrastructure, which is largely owned by the private sector and already faces heightened cyber risk.

A November 2025 decision by the Securities and Exchange Commission to drop a landmark civil fraud case against SolarWinds was widely considered a welcome development for the business community. The 2023 suit alleged that SolarWinds failed to disclose known cyber risks to investors during the years leading up to the 2020 Sunburst cyberattacks.

A federal judge had previously dismissed most of the allegations on the grounds the SEC misapplied a Depression-era law to the company's alleged failure to implement security controls. That legal resolution was also seen as a win for the CISO community, as SolarWinds' CISO Tim Brown had also faced enforcement action by the SEC in the regulatory agency's case.

Sagar Ravi, a partner at McDermott Will & Schulte and a former chief of the Complex Frauds & Cyberscrime Unit at the U.S. Attorney's Office for the Southern District of New York, said the decision to drop the SolarWinds case hopefully signals a move to recognize companies should not be punished for falling victim to sophisticated cyber threat actors. It also emphasizes the need for cyber risk transparency, he said.

"I think the focus is going to be on [enforcing] cybersecurity disclosure rules" in material incident reports on form 8-K or additional disclosures of strategy in annual reports, Ravi told Cybersecurity Dive.

Ravi hopes the SEC instead emphasizes ensuring proper post-breach disclosure rather than conducting investigations that review pre-incident decision making.

3. Cyber insurance enters new phase in pricing, coverage

The insurance market has seen its share of turbulence as it struggled to address cyber risk. For years, companies struggled to obtain cybersecurity coverage amid the increased threat of ransomware and fears about the rise of state-linked hackers.

Most recently, global insurers have expanded their commitment to cyber risk, and recent legal cases involving war exclusions language related to the NotPetya attacks has provided greater clarity on coverage. Even so, the insurance industry has begun questioning its dependence on the U.S. market, and whether current premium levels for cyber insurance can remain over the long haul.

That could mean diversification of the cyber insurance market. Large corporations in the U.S. represent a significant percentage of U.S. policy holders in the cyber market, so insurance companies need to expand into new markets such as small- to midsized businesses**,** risk analytics firmCyberCube said in a September report. Specialist insurer Beazley late last year said it remains committed to the U.S. market, but warned of a weak pricing environment for cybersecurity coverage.

In order to maintain favorable coverage, insurers are now heavily scrutinizing enterprise security practices, according to risk experts.

"Not too long ago, you could get cyber insurance with basic antivirus and a firewall," Monica Shokrai, head of business risk and insurance at Google Cloud said. "Today, if you don't have phishing-resistant MFA, XDR and immutable backups, you won't just pay more. You may not get access to coverage."

4. CVE crisis resolved while patching challenges remain

One of the most pressing challenges for security teams in recent years has been how to identify,

prioritize and remediate critical flaws discovered in widely used software.

These security vulnerabilities are often the gateway used by hackers to launch malicious cyberattacks by abusing the very security tools and software that critical industries and government agencies rely on to manage and protect their IT networks and maintain operational resilience.

The security sector was thrown into crisis in April of last year when U.S. government funding nearly collapsed for the Common Exposures and Vulnerabilities (CVE) program. An agreement was eventually reached between CISA and the Mitre Corp. to maintain support for 11 months, and CISA officials in September pledged to back future funding, releasing a road map that outlines additional support measures.

"CISA is asserting our leadership role to modernize the CVE Program, broaden adoption of known exploited vulnerabilities and reduce the prevalence of vulnerabilities by driving adoption of Secure by Design principles," Nick Andersen, executive assistant director for cybersecurity at CISA told Cybersecurity Dive earlier this month. "In collaboration with the global cybersecurity community, CISA is working to deliver a well-governed, trusted, and responsive CVE Program aimed to enhance the quality of vulnerability data and global cybersecurity resilience."

Software security experts say the CVE funding crisis is a wake-up call for the industry to develop proactive measures to finally address insecure software.

"Organizations need multisource, context-aware intelligence layered on top of CVE so each record reflects what actually matters: Exploitability, reach, prevalence in real dependency graphs, and whether there's a safe upgrade path," Brian Fox, co-founder and CTO at Sonatype told Cybersecurity Dive.

5. Operational resilience becomes the new watchword for cyberattack readiness

During much of 2025, companies around the globe were forced to confront a significant shift in cyber resilience. Cyber threat groups were no longer focused just on the exfiltration of data as their main objective, but instead on causing massive disruption to business operations.

A social engineering attack on UK department store Marks & Spencer, the hack of United Natural Foods and a crippling hack of automaker Jaguar Land Rover served as graphic examples in 2025 of how easily a successful cyberattack can disrupt production capacity, as well as major supply chains.

Security researchers said those cyberattacks were part of a deliberate strategy by threat actors to impose maximum pressure on major industries for monetary gain.

"Over the past year, we witnessed a fundamental shift in the attacker playbook, where financially motivated groups like Muddled Libra (Scattered Spider) moved beyond simple data theft to deliberate operational sabotage," said Sam Rubin, senior vice president, Unit 42 at Palo Alto Networks. "By exploiting the human element through sophisticated 'vishing' and manipulating

help desks, these actors proved they could paralyze entire enterprise networks and stop businesses in their tracks to maximize extortion leverage."

Corporate boards and C-suite executives are under pressure to ensure cyber risk is a key factor in their overall business resilience strategy, experts said security leaders will be tasked with developing specific plans on how to maintain operations and protect supply chains in the face of a catastrophic IT or security event.



The Cybersecurity and Infrastructure Security Agency's logo is seen at CISA headquarters in Arlington, Va., on June 11, 2025.

Eric Geller/Cybersecurity Dive

CISA's 7 biggest challenges in 2026

From infrastructure protection to improving morale, the cybersecurity agency has a lot on its plate — and it still lacks a leader.

January 9, 2026

Eric Geller

The beleaguered Cybersecurity and Infrastructure Security Agency faces a big test in 2026, with pressure mounting on the agency to clarify its approach to a wide range of security challenges.

As it reels from workforce cuts, lost resources and weakened partnerships, CISA will need to revitalize its support for critical infrastructure operators, craft an incident-reporting mandate that walks a tightrope of competing interests and develop a strategy to confront the Chinese government's increasing aggression in

cyberspace. The agency will also need to fix a morale crisis that threatens to further erode its operational readiness, as well as decide how much it intends to help state and local governments secure the upcoming midterm elections.

That many priorities would strain even a healthy agency, and since President Donald Trump took office a year ago, CISA has been anything but healthy.

"Losing 30 percent of your people in an unstructured drawdown is clearly a bad idea and this will hurt in every area," said Mark Montgomery, senior director of the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation.

From infrastructure protection to employee recruitment to whatever assignments it receives in Trump's new cyber strategy, CISA enters 2026 fighting an uphill battle, with a lot riding on whether it can turn itself around.

"We want CISA to succeed," said former senior agency employee Lauren Zabierek, "because their success strengthens our national security."

CISA's acting director, Madhu Gottumukkala, said the agency has "sharpened its mission" under the Trump administration.

"We will continue to work shoulder-to-shoulder with our trusted partners to improve federal network defense, empower small and medium businesses and critical infrastructure across the country to build resilience, and share timely and actionable threat information to assist in safeguarding the systems and networks Americans rely on every day," Gottumukkala said in a statement.

Here are the seven biggest challenges that CISA faces this year.

1. Protecting critical infrastructure with slim resources.

The biggest challenge CISA faces in 2026 is supporting critical infrastructure companies and state and local governments after losing thousands of employees and several key collaboration tools.

CISA has lost staffers focused on regional outreach, infrastructure security and strategic planning, making it harder for the agency to connect with infrastructure operators, deliver security services and guidance to them and collaborate with them on countering future threats.

"Our capacity to deliver our technical services has been significantly reduced in the past 11 months due to the cuts in programs and contracts, and we have to do more with less," said one CISA employee, who, like other staffers interviewed for this story, requested anonymity to speak freely.

Several of the agency's infrastructure partners agreed. "The essential mechanisms CISA needs to support critical infrastructure partners have been hollowed out," said Errol Weiss, chief security officer at the Health Information Sharing and Analysis Center. If a cybersecurity crisis hits healthcare or any

other sector, he predicted, CISA's "vital lifeline of coordination, support, and resource triage will be severely constrained, if not entirely severed."

Prior to the cuts, CISA had been trying to increase its support for the education sector, a community often overlooked in discussions about critical infrastructure despite weathering some of the most disruptive attacks. But "current events have absolutely set us back," said Doug Levin, national director of the K12 Security Information eXchange. Schools have noticed a stark difference, Levin said, "in state [and] regional [CISA] offices where personnel are simply not available to provide services anymore."

The agency's partnerships have also suffered as a result of the Trump administration both shuttering the Critical Infrastructure Partnership Advisory Council, which facilitated sensitive discussions, and eliminating funding for the Multi-State Information Sharing and Analysis Center, which provides vital intelligence and services to state and local governments. Cyber experts and industry leaders urged the government to reverse both moves.

The cuts have "created a dangerous void" and left U.S. critical infrastructure "fundamentally more vulnerable," Weiss said.

The recent changes have also eroded CISA's reputation as a reliable partner for the critical infrastructure community.

"The people that CISA should be supporting don't trust us, and right now they're absolutely right in that position," said a second CISA employee.

By cutting staff, collaboration forums and travel allowances, "DHS seems to be making it as hard as possible for CISA employees to have contact with the private sector," said Michael Daniel, president of the Cyber Threat Alliance, an industry collaboration group. "Over time, these restrictions will degrade CISA's effectiveness, reduce its understanding of the broader environment, and make its products … less relevant."

The Trump administration has said that the cuts at CISA are part of reorienting the agency toward its core protective mission. But infrastructure representatives rejected that framing. "You can't simply 'refocus' CISA on core defense without acknowledging that defense relies entirely on those external relationships," Weiss said.

2. China's aggressive cyber and geopolitical ambitions.

The looming potential of an armed conflict between the U.S. and China over Taiwan has further elevated the stakes of CISA's critical infrastructure protection mission.

Companies look to CISA for early warnings of threat activity and guidance on thwarting China-linked hackers, while policymakers rely on the agency to identify and prioritize critical national assets that need protection, such as the railways and ports used to mobilize military equipment. Those responsibilities will put CISA at the center of any conflict over Taiwan, given that China is expected to open such a conflict by hacking U.S. infrastructure to

delay an American response to the invasion. But many experts are pessimistic about CISA's current readiness to prevent or respond to those attacks.

A Chinese invasion of Taiwan "will be the geopolitical crisis of our time," but CISA is "ill-prepared" to play its part, said Brian Harrell, a former assistant director for infrastructure security at CISA. "I question current relationships and information sharing mechanisms."

China-linked infrastructure hacks are "akin to putting a gun to our head," said Suzanne Spaulding, who led CISA's predecessor at DHS for six years. "We need to take the bullets out of that gun by working to reduce the likelihood that China's cyber efforts will have the impact they seek."

3. Balancing the regulatory challenges of CIRCIA.

CISA is also racing to finalize a regulation requiring critical infrastructure operators to report cyber incidents to the agency. The 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) required CISA to publish the final version of the rule by October 2025, but CISA extended that deadline to this May. Companies and their lawyers are closely watching CISA's process of drafting what has become known as the CIRCIA regulation, which will be the U.S.'s first comprehensive cyber incident reporting requirement.

Currently, the vast majority of cyberattacks in the U.S. go unreported. The CIRCIA rule is expected to dramatically increase the government's awareness of cyber threat activity facing critical infrastructure companies. "It's essential, not just for CISA but for our security, to get CIRCIA in a working state," said Jeff Greene, a former executive assistant director for cybersecurity at the agency.

But CISA faces a difficult balancing act: preserving the rule's core information-gathering purpose while addressing businesses' complaints that the Biden administration's draft regulation is too onerous, broad and vague. Industry representatives say the draft rule overburdens companies in the middle of chaotic incidents, and some question CISA's ability to effectively use the ocean of data it will receive.

"The agency is likely going to be under pressure to make the reporting system as minimalist as possible," said Daniel, who served as President Barack Obama's cyber adviser.

CISA will do its best to produce a rule that generates useful reports without impeding businesses, Greene said, but "you're not going to get something that everyone thinks is great and well-crafted."

The contours of the final CIRCIA rule will define CISA's relationship with the private sector in the coming years. "It is critical that CISA gets the implementing regulation right," said John Miller, a top executive at the Information Technology Industry Council.

4. Uncertainty over CISA's commitment to product security.

CISA's transformation over the past year has raised questions about its commitment to a major pressure campaign aimed at improving the security of the digital ecosystem.

During the Biden administration, CISA launched a "Secure by Design" initiative to encourage companies to build security into their products from the beginning and turn on secure features by default. Hundreds of companies have signed a pledge to make improvements in seven specific areas. But the key figures behind the initiative left CISA at the beginning of the Trump administration, and CISA has done nothing publicly with the project since then, raising questions about its fate.

Zabierek, one of the project's now-former leaders, said she hoped the Trump administration recognized its value and kept it alive, because "preventing cyberattacks through more secure technology is the most sustainable path to national cyber safety in the long run."

Secure by Design could dovetail with the Trump administration's unconventional political strategy, either through heavy-handed pressure on tech companies often criticized by conservatives or through praise of participating businesses as conscientious stewards of public safety. But either approach would require resources, staff and open communication with industry — all things the administration has taken from CISA.

Greene said CISA was "starting to have [a] real effect" with Secure by Design during the Biden administration. "We're starting to see companies go through the cycle that we had hoped to see."

5. Election cybersecurity.

With the midterm elections looming, security experts predict a resurgence in foreign influence operations designed to sow chaos and sway voters. In past election cycles, CISA helped state and local officials rebut misinformation and coordinated closely with the FBI and the intelligence community to track and disrupt foreign interference. But CISA's anti-misinformation activities prompted reprisals from the new Trump administration, casting doubt on the agency's attitude toward election security this year.

Trump "has weakened the nation's preparedness" for election threats, Jena Griswold, Colorado's Democratic secretary of state, told Cybersecurity Dive.

Caitlin Durkovich, a White House homeland-security official during the Biden administration, said the Trump team "has signaled that collecting on, exposing, and disrupting increasingly sophisticated hostile — or aspiring — foreign state actors will not be a priority."

Even if the White House allows CISA to reengage on the issue, staffers will likely be reluctant to take part in a mission that the administration considers radioactive. And whatever effort CISA does make will encounter skepticism from state and local officials who have lost trust in the agency. "Many no longer see CISA as an

honest broker," Spaulding said. "This is devastating and will take many years to recover."

6. Overcoming the agency's internal morale crisis.

CISA won't be able to achieve any of its goals, experts said, without addressing its crippling morale crisis and refilling hundreds of vital positions. In addition to firing many workers, the Trump administration has forced out othersby sending them to other Department of Homeland Security agencies, sometimes in unrelated roles across the country.

"Successful efforts to traumatize the federal workforce have decimated CISA," Spaulding said.

CISA has announced ambitious plans to fill critical gaps in its workforce this year, but the administration's attacks on CISA and the broader federal workforce will make it very difficult for the agency to recruit new employees and retain current staffers.

"It will take a long time to hire their way out of all firings and departures," Greene said. "Almost everyone I know who left is making more money and working fewer hours, so getting those people to come back … is not going to be super easy."

CISA might be able to find new workers in the months ahead, Greene said, but the hiring process is so slow that the agency may not see the benefits for a long time.

In the meantime, some employees say they're trying to make due with the agency's remaining capacity.

"We've got to pick up the pieces and still do our jobs," said a third CISA employee. "A lot of people are still committed to the mission, but it's going to be tough sledding."

7. Leadership vacuum.

CISA will struggle to improve morale, confront China and reestablish its trusted public presence without a permanent director. Trump's nomination of Sean Plankey to lead CISA expired at the end of 2025, and it is unclear if Trump will renominate him.

"Getting a CISA director confirmed is absolutely critical," Montgomery said. "No defense agency — whether it's CISA or NSA — should … go without a permanent leader for more than 10 days, much less 10 months."

Agencies without leaders struggle to make big changes and to advocate for themselves in strategy and budget meetings with the White House and other agencies. "The ability to put longer-term plans in place is really hamstrung," said Trey Herr, senior director of the Atlantic Council's Cyber Statecraft Initiative.

The mid-level officials currently steering CISA won't want to make big decisions on CIRCIA, election security and other issues without a director in place. That could force CISA to watch as other agencies take the initiative on cybersecurity.

Harrell said he admired the people currently running CISA, "but they need the autonomy and flexibility to lead without doing 'Mother, may I' to the DHS front office for every issue."



A Jaguar Land Rover employee works on an assembly line in the U.K. The company's recent cyberattack was one of the most disruptive in British history and came as manufacturers worldwide faced more hacks than any other sector.

Courtesy of Jaguar Land Rover

Manufacturers fortify cyber defenses in response to dramatic surge in attacks

IT/OT convergence and other trends are making the manufacturing industry's networks more vulnerable and more frequently targeted, but sector leaders are working to improve their cyber posture.

January 29, 2026

Eric Geller and David Jones

As U.S. manufacturing firms weather a constant barrage of cyberattacks, the various industries in that sector — which underpin everything from military readiness to everyday necessities — are banding together to learn from past incidents and boost their collective defenses.

Even as other critical infrastructure sectors like energy, healthcare and telecommunications receive more attention from most policymakers, cybersecurity firms have repeatedly found that manufacturing is the most targeted of the 16 critical infrastructure sectors recognized by the

U.S. government. Hackers see manufacturers as especially enticing victims, because they make and store sensitive intellectual property, operate businesses that can't afford interruptions and rely on complex supply chains. For those same reasons, industry leaders, cybersecurity experts and government officials increasingly warn that both U.S. national and economic security depend on protecting the heavily besieged manufacturing sector.

"Cyber disruptions can halt production, delay infrastructure projects, and create cascading supply chain impacts without causing physical damage," said Chris Grove, director of cybersecurity strategy at OT security firm Nozomi Networks.

Manufacturers would be important national assets to protect in any year. But amid growing tensions between the U.S. and China, experts see it as even more pressing to prevent hackers from crippling America's production capacity. And as technological and operational trends increase the vulnerabilities that these companies face, the risks of a catastrophic cyberattack are quietly growing.

"If the attack hits a key market component," Sean Tufts, field CTO at OT security firm Claroty, said, "it's like having a hurricane hit an entire industry at once."

Recent cyberattacks demonstrate the high stakes

Cyber threat intelligence reports of late have painted an alarming picture of the cybersecurity landscape facing manufacturers.

Ransomware gangs claimed more than 1,000 attacks on the sector over the past year, according to data from Palo Alto Networks. The average manufacturer faces about 1,585 attempted attacks per week, with overall attacks on the sector increasing by 30% year over year, the security firm Check Point Software said in an October report. And in the fourth quarter of 2025, manufacturing firms accounted for the largest share of claimed victims on dark web data-leak sites, according to researchers at Google Threat Intelligence Group.

Several major U.S. and international manufacturers suffered disruptive cyberattacks in 2025. Nucor, the largest steelmaker in the U.S., was forced to pause operations in May after an attack targeting its IT network. The company later confirmed that hackers accessed Social Security numbers, credit card information and other personal data, although it said the intrusion didn't materially affect it financially. A more crippling attack hit British automobile giant Jaguar Land Rover in late August, forcing JLR to shut down manufacturing for weeks, and ultimately costing the British economy some $2.5 billion.

The cyberattack on JLR, which led to the theft of company data as well, was the single most financially damaging cyberattack in British history, according to the U.K.-based Cyber Monitoring

Centre. The group estimated that the disruption affected more than 2,700 U.K. organizations.

"What makes the JLR incident notable is that the systemic impact arose from a single company's operational shutdown, rather than a piece of software or shared platform failing simultaneously across many organizations," Will Mayes, CEO of the Cyber Monitoring Centre, told Cybersecurity Dive after the group released its report on the incident.

A threat actor affiliated with the cybercrime groups Scattered Spider, Lapsus$ and ShinyHunters — whom researchers linked to a wave of social engineering attacks last year — eventually claimed credit for the attack.

While JLR and Nucor's were the highest-profile cyberattacks in the sector, hackers have breached many other manufacturers over the past few years, including tire maker Bridgestone Americas, cleaning products giant Clorox, medical device-maker Masimo, aerospace and automotive-sensor supplier Sensata and building control system-maker Johnson Controls.

The disruptive effects of many of the recent attacks underscore the precariously configured manufacturing sector's unique inability to tolerate downtime.

That fact has led to "a market consensus among threat actors … that manufacturing is the most reliable place to extract a profit," said Anna Chung, principal threat researcher at Palo Alto Networks.

Moody's analysts concur that manufacturing firms face a higher risk of ransomware attacks because they have limited ability to withstand significant disruptions.

"Attackers … see that as an added incentive for their victims to find a solution that would put them back online as fast as possible," said Lesley Ritter, vice president at Moody's.

Growing cyber risk of opportunistic and targeted attacks

The manufacturing sector faces major technical and economic challenges that complicate efforts to defend against cyberattacks.

One of the biggest challenges is the increasing convergence of information technology and operational technology networks. Manufacturing firms' computer networks often encompass functions like payroll on the IT side and industrial functions like machinery operations on the OT side, as well as Internet of Things devices like surveillance cameras. It's not difficult for hackers to jump between systems in those environments if they are not properly secured and segmented. "That convergence expands the attack surface and creates multiple entry points," Grove said.

Manufacturers' growing use of cloud platforms, mobile applications and Internet of Things devices also drives this convergence, as businesses connect devices and systems in untested ways, often without prioritizing the security of those links.

At the same time, visibility gaps between the security teams managing IT and OT sometimes make it harder for companies to quickly react when they discover hackers conducting reconnaissance or other early-stage cyberattack activity.

Manufacturers also face significant third-party risk, given their vast networks of suppliers and contractors. The JLR cyberattack began when hackers penetrated a major global outsourcer to which the carmaker had delegated many of its digital operations. "This happens all the time," said Timothy Chase, the program director for the MFG-ISAC, the sector's information-sharing group, which is housed within the nonprofit Global Resilience Foundation.

Manufacturing firms are also grappling with the dangers of legacy OT devices that vendors no longer support and that may be quietly accumulating security vulnerabilities.

"In some cases, there are no patches, because manufacturers don't replace and update their systems at all," said Sergey Shykevich, threat intelligence group manager at Check Point Software.

But a modernization rush carries its own risks: As companies rush to adopt artificial intelligence and cloud platforms, they are not always integrating security into those technologies.

Even when companies understand their security risks, they cannot always address them. Decades-long offshoring trends mean that U.S. firms have tighter financial margins than ever before. "Cyber is expensive, with limited ROI," Claroty's Tufts said. "CFOs are hesitant to spend."

Bureaucracy can also hamper progress. Companies often assign the security of their corporate networks to experienced personnel at headquarters while leaving OT security in the hands of factory supervisors without "the expertise or investment to make the needed security upgrades," Tufts said.

All of these challenges make cyber defense more difficult for the manufacturing sector, even as the threats grow more sophisticated.

"Manufacturing attacks are increasingly opportunistic, automated, and IT-originated, then moving laterally into OT," Nozomi's Grove said.

The year ahead is likely to bring even more serious threats. China is expected to increase its penetrations of U.S. critical infrastructure as part of a deterrence strategy to keep the U.S. from repelling its invasion of Taiwan. In the context of that strategy, manufacturing firms are prime targets for China because of their strategic importance.

"Cyber vulnerabilities in manufacturing directly affect U.S. national and economic security because the sector underpins critical supply chains, defense readiness, and industrial competitiveness," Grove said.

But Chinese cyberattacks wouldn't be limited to sabotaging weapons production or stealing fighter-jet blueprints. The manufacturing sector is also vital to everyday life, so even a

prosaic attack could have devastating consequences. “A nation-state actor could target several of the [U.S.’s] paper pulping and toilet paper manufacturers to bring down operations,” the MFG-ISAC’s Chase said, “and for some time it could look like early days of the pandemic, with shortages, hoarding, et cetera.”

A major cyberattack on the manufacturing sector “could result in significant national economic impact and lengthy disruptions that cascade across multiple critical infrastructure sectors or regions,” Nick Andersen, the Cybersecurity and Infrastructure Security Agency’s executive assistant director for cybersecurity, said in a statement. Andersen said CISA “routinely engages” with manufacturing firms to discuss issues like the IT/OT convergence.

Joining forces across diverse market segments

To confront growing threats, manufacturing companies have teamed up through the MFG-ISAC, which hosts events and distributes guidance to members.

“Customers view peer collaboration as one of the most effective defenses they have,” Grove said. “Manufacturers trust information coming from peers who face the same operational realities.”

In 2025, the MFG-ISAC partnered with Google Cloud on an in-person tabletop exercise, convened a working group that produced a cyber-incident response playbook and co-organized an OT training course with the security firm Dragos. Dozens of companies have participated in that program, Chase said. The ISAC also manages an OT discussion group through which member firms can plan shared responses to sector-wide challenges, such as the difficulty of securely monitoring remote facilities.

This year, Chase said, the ISAC is planning another in-person tabletop exercise, as well as an expanded range of guidance documents and services for managing OT threats. The organization is also creating new working groups to address the priorities of its growing membership base. One of the groups will bring together manufacturers who need to meet the Defense Department’s new Cybersecurity Maturity Model Certification standards and want to discuss implementation challenges.

Within the manufacturing sector, “there’s a strong understanding that collaboration benefits everyone,” Tufts said. “MFG-ISAC provides a trusted environment where even competitors can share failures and success.”

That collaboration will be essential for improving the security posture of a highly diverse sector, in which many different industries share overlapping vulnerabilities and concerns. The MFG-ISAC’s members include everything from pharmaceutical giants and food companies to businesses that make home heating and plumbing appliances. A recent Dragos report tallied 26 distinct manufacturing subsectors. “The diversity in manufacturing … can make it a challenging sector to help facilitate collective defense,” Chase said.

Cyber readiness varies widely throughout the sector as well, according to Chase. Some companies still don't realize that they could be the target of nation-state hackers, while others recognize that they are vulnerable but misunderstand the risks they face, whether ransomware or intellectual property theft. In some cases, Chase business leaders also underestimate the impact of certain threats — for example, seeing a ransomware attack as mostly an IT concern, without realizing how their production environment depends on those IT systems.

"The recognition of the importance of both IT and OT cybersecurity is increasing across the manufacturing sector," Chase said, "but there is much more work to be done in education and in helping resource security teams with relevant threat and vulnerability information to secure their own environments."

In the U.K., the National Cyber Security Centre has strengthened its commitment to help vital industries better prepare for malicious attacks by state-linked adversaries and criminal hackers. Its latest annual review, released in October 2025, warned that critical infrastructure sectors were under increased threat of disruptive cyberattacks.

In connection with the report, authorities wrote directly to top corporate executives at the Financial Times Stock Exchange (FTSE) 350, urging them to take board-level action to prepare for cyber threats and protect their supply chains.

NCSC also meets regularly with cybersecurity leaders from key sectors, including manufacturing and automotive, to share threat intelligence and best practices, officials familiar with the process told Cybersecurity Dive.

Experts said manufacturers would benefit immensely from implementing a handful of key network improvements, including expanding asset visibility across IT, OT and IoT; prioritizing the most impactful vulnerabilities; segmenting networks to limit the consequences of a single attack; and minimizing the internet exposure of unpatchable systems. Security specialists also recommended that manufacturers restrict and supervise third-party suppliers' network access and develop and test incident-response plans.

That final recommendation, often neglected by busy companies, could prove to be the most important one. "You must have a plan ahead of time," Chase said," and you must exercise that plan with all relevant stakeholders."



Stay ahead with Cybersecurity Dive



Operated by Informa TechTarget, part of a global network that informs, influences and connects the world's technology buyers and sellers.