Jose M. Seara
Founder and CEO
DeNexus

Secure Critical Infrastructure: Mitigating Cyber Risks

Manufacturing, energy and industrial sectors are witnessing a paradigm shift as chief information security officers (CISOs) take on the added responsibility of safeguarding both enterprise IT infrastructure and operational technology (OT) environments. With increasing connectivity between production facilities and company networks, there is a heightened risk of cyber incidents and ransomware, emphasizing the potential impact on production downtime, margin reduction, order delays and regulatory concerns.

facilities that are increasingly connected to company networks and internet for productivity improvement, operational excellence, production reporting and remote maintenance. This connectivity of applications and infrastructure increases the risk of exposure to cyber incidents and ransomware.

If IT/OT systems are targeted by threat actors or ransomware, their disruption can quickly lead to production downtime, margin reduction, delays fulfilling orders and reliability, as well as safety or regulatory concerns.

With highly integrated and just-in-time supply chains, small disruptions due to cyber incidents have immediate and lasting effects.

Main Drivers of Loss

Loss Event	Annual Expected Loss ($)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Loss Of Productivity	$3,815,210	5.1	63.9%	1.4%
Downtime	$1,406,060	1.9	23.6%	0.5%
Extortion	$296,295	0.4	5.0%	0.1%
Equipment Damage	$189,211	0.3	3.2%	0.1%
Forensic Investigation	$164,765	0.2	2.8%	0.1%

Source: DeNexus' DeRISK platform

Cyber risk is quantified for each type of expected loss, at the site or portfolio level, allowing manufacturers to rapidly identify where to allocate resources and budget to strengthen their cyber resilience.

CISOs now inherit the added responsibility of securing the enterprise IT infrastructure and OT/industrial controls systems (ICS) environment in production

Traps of Technology

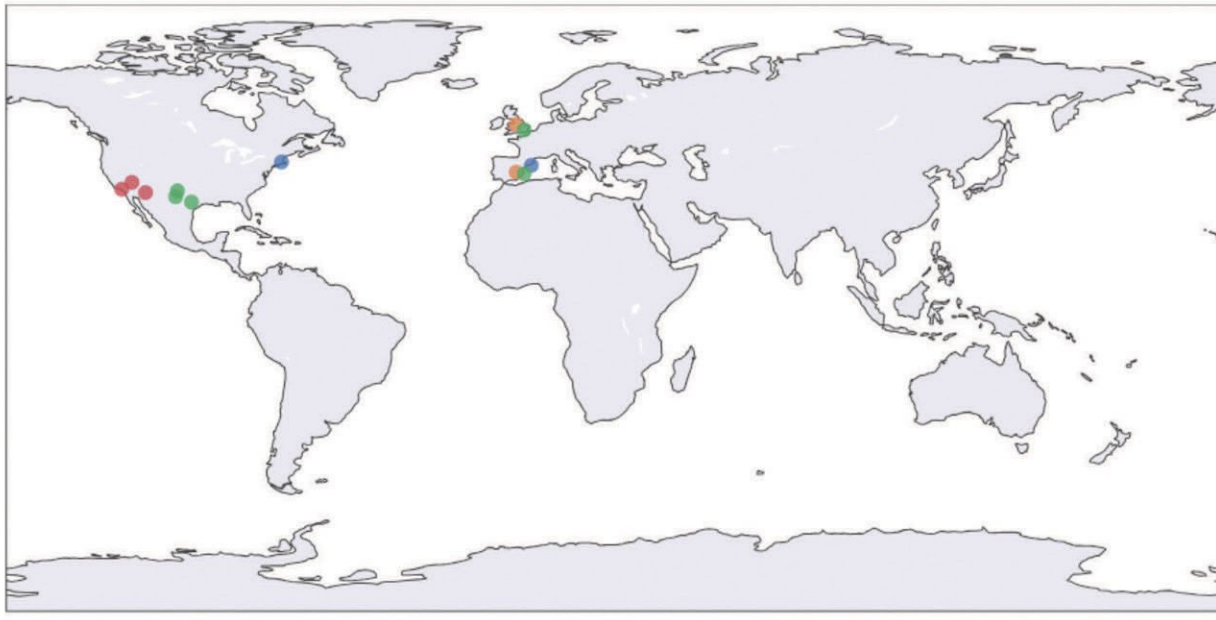
Many manufacturers are early adopters of technology to improve operations, driving increased connectivity between OT and corporate networks and cloud applications. This is both a benefit and a bane. While operations excellence and overall equipment effectiveness (OEE) are improved, pathways (aka initial access vectors) into OT are increased, as are dependencies between IT and OT.

Manufacturing execution systems (MES) are generally located on corporate networks separate from OT manufacturing systems. But when there are application dependencies between them (e.g., label printing, recipes, schedules), an isolated OT system doesn't matter anymore.

Ransomware on the corporate network can disrupt manufacturing without spreading to OT networks. A critical technology dependency is interrupted, or the production operations are shut down out of concern for caution or even uncertainty.

According to the ICS-STRIVE incident database, almost half of incidents in the past 10 years were in manufacturing. Recent ransomware

Portfolio of Facilities



Source: DeNexus' DeRISK platform

Large industrial companies often have facilities distributed around the globe. DeNexus quantifies cyber risk at the site and portfolio levels and any other grouping while also providing comparison to industry peers or adherence to specific security standards such as the NIST CSF.

incident data in 23Q4 from Dragos provides further evidence that the rate of ransomware affecting ICS/OT in manufacturing has risen over 65%.

Quantifying Risk

Manufacturing is vital to society. It is the food we eat, the components in our technology, the medicines we need, the boxes they ship in and so much more. With highly integrated and just-in-time supply chains, small disruptions due to cyber incidents have immediate and lasting effects, as evidenced by the supply chain issues during the pandemic.

CISOs and chief financial officers must develop the practice of quantifying their cyber risk in monetary terms and evaluate the ROI of mitigation strategies to drive effective decisions on cybersecurity investments that can thwart the current wave of ransomware attacks.

Conventional approaches, which involve assigning a criticality rating to a cyber asset or system and evaluating the severity of vulnerabilities, often fall short in persuading financial decision-makers. The prevalent scenario entails organizations seeking funds for cybersecurity projects by emphasizing the urgency of remediating high-severity vulnerabilities in highly critical systems. However, this approach neglects a crucial component: the financial repercussions of inaction—specifically, the probable financial loss in the event of a cyber incident today.

The transformational key lies in bridging this gap by quantifying cyber risk in monetary terms. By demonstrating that an investment of X amount can substantially reduce the probable loss by Y, organizations can create a solid foundation for cyber risk quantification and management.

This shift from a purely technical justification to a more financially oriented perspective not only enhances the case for cybersecurity investments but also aligns strategic decision-making with tangible financial outcomes.

How the ecosystem can combine efforts to secure the future of manufacturing

Jim Wetzel (left) and Conrad Leiva (right) leading an educational workshop at SOUTHTEC 2023, "Smart Manufacturing: Why It Matters and How to Achieve It," sharing insights on securing the future success of manufacturing operations. (Photo credit: David Butler II)

Set the Right Mindset for Smart Manufacturing

Conrad Leiva
VP of Ecosystem and Workforce Development
CESMII

Jim Wetzel
Co-founder
NxGen Group

The adoption of new technology plays an important role in the ongoing, competitive global manufacturing race. Many leading manufacturers are planning to compete as highly integrated ecosystems with highly connected digital supplier networks, and this race is fueling the drive to implement smart manufacturing (SM) technologies.

CESMII, the Smart Manufacturing Institute, is one of the national Manufacturing USA institutes helping manufacturers accelerate their efforts. Through our work with manufacturers, we have found that cultivating the right mindset and culture in the organization is a key factor to successful implementation and sustainment of smart manufacturing initiatives—a mindset that promotes the right set of attitudes and behaviors in the organization.

For example, if someone is walking around the plant without the proper eye protection, would people generally stop them and point it out or would they let it slip? If an organization has cultivated a safety mindset, the person would be more likely to be stopped and warned by multiple fellow employees along the way.

Mindset Matters

An organization can have multiple mindsets prevalent in its culture. Many have cultivated a lean mindset over the last decades that drove efficiency improvements by eliminating waste and focusing on customer value. However, the pace of technology innovation in products, supply chain logistics and customer services is creating new challenges for manufacturers that are beyond the manual lean methods of the past. There is a need to embrace a digital mindset without abandoning the lean mindset. In fact, studies have documented that when digital techniques are applied along with lean tactics the projects yield greater improvement—over 30% greater improvement.

The capability to work with rich insights, digitally orchestrate work and quickly act on new data is becoming the new norm. A digital mindset means that employees understand why the organization needs accurate, real-time data to stay competitive and deliver enhanced service to their customers. The right mindset and culture drives innovation in the organization. When employees see paper forms they wonder if there is a more efficient, paperless way to collect the data. If it takes days to investigate a customer complaint because employees are gathering data manually, they push for having digital data readily available, so root-cause analysis takes hours instead of days. Rethinking the process while applying lean principles with a digital mindset drives breakthrough performance.

To develop a digital mindset, the team must be trained for the digital dexterity required to launch and obtain the desired outcomes of SM initiatives. In addition to basic skills in dashboards and metrics, training in areas like critical thinking, complex problem solving, adaptability, resilience and creativity are equally important to realize the full benefits of digital transformation.

Lean and digital are good grounding mindsets for smart manufacturing, but it is also important to cultivate an ecosystem mindset. The technology available today can help manufacturers tackle all kinds of problems and reduce costs within their organizations, but the big opportunities lie in optimizing the entire value chain. By leveraging an ecosystem, manufacturers can grow the business and deliver more value through more resources to more satisfied end customers.

Conrad Leiva (left) and Jim Wetzel (right) engage workshop participants at SOUTHTEC 2023. (Photo credit: David Butler II)

It has become increasingly hard for a single manufacturer to keep up with the pace of technological innovation and complexity in products and manufacturing processes. By focusing on specific specialties, partners in the ecosystem can target their capital and technology investments to fewer core competencies. While each company is optimizing and trying to "do more with less," the ecosystem shifts the culture to a more practical and scalable approach of "do more with more."

Better Together

Manufacturers have realized that the best way to provide personalized products and enhanced customer communications and services is through an integrated ecosystem of partners, suppliers, distributors and service providers. As these ecosystems become common place and expected, manufacturers must be ready to participate in these highly integrated digital networks to remain competitive.

The new manufacturing ecosystem is evolving to leverage digital connectivity and infrastructure for higher levels of orchestration and optimization in the manufacturing value chain. This evolution requires a culture that promotes collaboration and embraces higher levels of transparency, not only within the organization, but also across the supply chain.

Overcoming the challenge of digitally collaborating outside the company walls becomes paramount. Concerns about ownership and control of processes and systems can make departments reluctant to share information across organizational boundaries. However, the ecosystem mindset challenges the legacy of clearly defined areas of responsibility and siloed information systems and embraces streamlined integrated processes across the old departmental boundaries. Instead of relying on managers to make all decisions during weekly meetings, the organization empowers employees with the information needed to make better decisions on the spot when issues come up.

Manufacturers are opening to sharing data in the supply chain to get higher levels of visibility and resiliency in their ecosystems as long as they have security and governance. The information flow needs to be architected to limit and secure the data, so the right partners get the right data required for supply chain orchestration. Companies embracing a digital ecosystem approach are already realizing between 16% and 32% improvements in their speed of product introduction and revenue streams from new products and services.

Prior mindset movements like lean had big impacts on manufacturing during the last few decades. It is time for a new smart manufacturing mindset that combines lean, digital and ecosystem mindsets for the next big wave of productivity improvements. Organizations with this new mindset will be better positioned to drive future success.

The combination of the right mindset, principles and roadmap creates the recipe for a successful smart manufacturing journey. CESMII is providing resources like the "First Principles of Smart Manufacturing" and is helping manufacturers with a systematic approach to the development of a roadmap that aligns the team and links the business and technology strategy. To learn more about the many resources available from CESMII visit CESMII.org.

AD INDEX

SMART manufacturing

1000 Town Center
Suite 1910
Southfield, MI 48075
Phone: 313-425-3479

Jake Volcsko–VP, Integrated Media
Direct Line: 313-425-3260
E-Mail: jvolcsko@sme.org

Project Manager (MT Portfolio)
NICOLE SOTO
1000 Town Center, Suite 1910
Southfield, MI 48075
Phone: 313-425-3003
E-Mail: nsoto@sme.org

Central - Sales Manager
BILL LEPKE
529 Fairview
Elmhurst, IL 60126
Phone: 630-975-0185
E-Mail: lepkeb@sbcglobal.net

Western - Sales Manager
PAUL SEMPLE
2170 Red Setter Rd.
Rocklin, CA 95765
Phone: 916-880-5225
E-Mail: paul@semplemedia.com

Account Representative II
BEV HOGAN
1000 Town Center, Suite 1910
Southfield, MI 48075
Phone: 313-900-1463
E-Mail: bhogan2@sme.org

SMART MANUFACTURING
April 2024, Vol. 9, No. 2 is published by SME, 1000 Town Center, Suite 1910, Southfield, MI 48075. Telephone 313-425-3479 Fax: 313-425-3417. Canada Post Publication Mail Sales Agreement No. 40732015. Postmaster: Send address changes to Attn: CDC, Smart Manufacturing, 1000 Town Center, Suite 1910, Southfield, MI 48075.