



**Cyber risk in
advanced manufacturing**
Executive summary

Introduction

Manufacturers drive extensive innovation in products, manufacturing process, and industrial ecosystem relationships in order to compete in a changing global marketplace.

Technologies utilized to drive the business are likely to include complex global networks, a myriad of back office business applications, generations of different industrial control systems (ICS) controlling high-risk manufacturing processes, and a variety of technologies directly embedded into current and emerging products. Further, manufacturers continue to drive extensive innovation in products, manufacturing process, and industrial ecosystem relationships in order to compete in a changing global marketplace.¹ As a result, the manufacturing industry is likely to see an acceleration in the pace of change in technology due to emerging trends, such as:

- Large scale investments in intellectual property and exponential technologies²
- Exploration of industry 4.0 digital manufacturing³ opportunities and increased interconnectivity of the industrial ecosystem⁴
- Rapid adoption of sensor technology, smart products, and Internet of Things (IoT) strategies and analytics to drive increased customer service and business efficiency

This existing technology footprint, along with its accelerating pace of change in business and manufacturing technology, is expected to have a dramatic impact on the breadth and complexity of the cyber risks manufacturers will need to address over the next decade.

Our exploration of these trends,⁵ and the recent enterprise risk study by Deloitte and The Manufacturers Alliance for Productivity and Innovation (MAPI), have highlighted the need for a broader and deeper understanding of

- The current state of cyber risks facing manufacturers
- Emerging risks likely to materialize as a result of rapid technology change

- An assessment of leading strategies manufacturers are employing to address these types of cyber risks

To that end, Deloitte and MAPI launched the Cyber Risk in Advanced Manufacturing study to assess these trends. We conducted more than 35 live executive and industry organization interviews, and in collaboration with Forbes Insights, we collected 225 responses to an online survey exploring cyber risk in advanced manufacturing trends.

The results of this study may help manufacturers engage their senior leadership teams and boards in a deeper conversation on how to make their businesses secure, vigilant, and resilient. Applying lessons learned from this study can help them:

- **Be Secure** – Take a measured, risk-based approach to what is secured and how to secure it. This includes managing cyber risks as a team and increase preparedness by building cyber risk management strategies into the enterprise and emerging technologies as they are deployed.
- **Be Vigilant** – Monitor systems, applications, people, and the outside environment to detect incidents more effectively. This includes developing situational awareness and threat intelligence to understand harmful behavior and top risks to the organization and actively monitoring the dynamic threat landscape.
- **Be Resilient** – Be prepared for incidents and decrease their business impact by improving organizational preparedness to address cyber incidents before they escalate. This also includes capturing lessons learned, improving security controls, and returning to business as usual as quickly as possible.

Key cyber risk themes

As a result of this extensive study, our own research, and an innovation lab that explored survey results and leading practices with manufacturing executives, we have coalesced around the following key themes.

We believe these are critical to manufacturers' abilities to capture the value associated with this new frontier of technology, while appropriately addressing the dynamic cyber risks, in order to protect and enhance value over the longer term. The top themes and associated statistics from our research are outlined in this summary.



Executive and board level engagement



Industrial control systems (ICS)



Talent and human capital



Connected products



Intellectual property



Industrial ecosystem

Engage the board and C-Suite to develop a business-driven cyber risk program



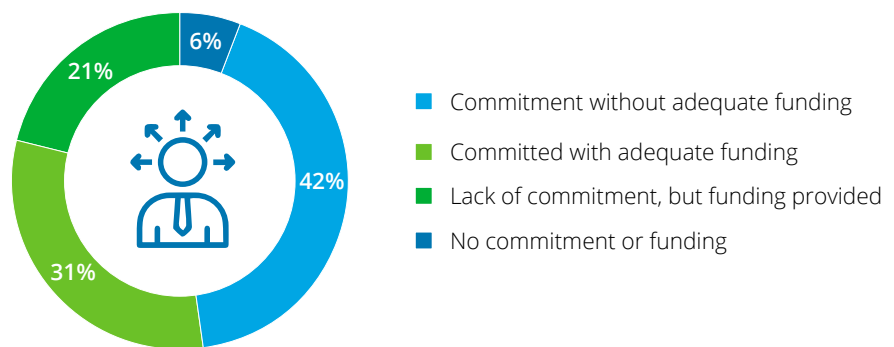
Understanding the landscape and need for organizational ownership

Given its focus on innovation and an increasing reliance on connected products, those interviewed consistently shared their belief that manufacturing is an industry highly vulnerable to cyber risk. In spite of new investments in IoT technologies and broad concerns with such risk, the manufacturing industry as a whole is still fragmented in its approach to managing cyber-related cyber risks, as well as the organizational ownership to do so. From a broad perspective, manufacturing is seen as lagging other sectors, such as financial services and retail in the maturity of enterprise cyber risk programs.

Budget increases are hard to secure

Due to the growing severity and sophistication of cyberattacks, only 52 percent of executives surveyed are either very confident or extremely confident their organization's assets are protected from external threats, meaning nearly half of manufacturing companies are only somewhat confident or less.

Figure 1: Description of senior level support for cyber initiatives



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

In some cases, there are challenges with top leadership for funding, as cyber risk has not always been a top-of-mind topic. However, senior executive and board support has increased considerably in the past couple of years as seen with the increased frequency of C-Suite and board briefings, more often occurring annually, with up to quarterly updates.

Cyber risk in advanced manufacturing


Be Secure.Vigilant.Resilient™

Manufacturers are driving extensive innovation in products, manufacturing process, and industrial ecosystem relationships in order to compete in a changing global marketplace. As a result, the manufacturing industry is likely to see an acceleration in the pace of change in technology and associated cyber risks. The Deloitte Center for Industry Insights surveyed 225 manufacturing industry cyber risk executives, representing a diverse collection of companies from a variety of manufacturing sectors, to evaluate how manufacturing companies are confronting cyber risk issues. In collaboration with MAPI, the online survey effort was bolstered by a series of 35 executive interviews, and the following illustrates the overall findings.

Cyber risk programs: a framework for leading practice board reporting

Governance and Leadership Engagement

Nearly 50% of executives **lack confidence they are protected**

48%  **lack adequate funding**

Talent and Organizational Management



4 of top 10 threats involve employees

75% **lack skilled resources**

IT/OT gap drives behavior

Traditional board reporting

Enterprise Network & Business Systems

Be secure

Take a top down, risk based approach to implementing security strategies for the most critical networks, systems, and data



36% cited IP protection as top concern

Industrial Control Systems

50% isolate or segment ICS networks

31% have not conducted an ICS assessment

Connected Products



35-45% use sensors, smart products, and mobile apps

55% encrypt the data

Be vigilant

Implement routine monitoring mechanisms for high risk networks, systems, and data that will alert the company to abnormal activity and enable prompt action

A top executive concern is increasing sophistication/proliferation of threats



50% perform ICS vulnerability testing less often than once a month



77% had performed end to end product assessment

Be resilient

Plan ahead before a breach occurs so the entire organization is prepared to respond in order to quickly neutralize threats, prevent further spread, and recover from business impacts

39% experienced a breach in the last 12 months

38% had losses \$1 - 10m+

only 12% currently employ tactics such as **wargaming** exercises



27% do not include ICS in incident response plans



37% do not include **connected products** to incident response plans



What manufacturers can do to engage the board and C-Suite

Establish a senior management-level committee with board member representation that is dedicated to the issue of cyber risk.

Review cyber breach incident management framework and establish escalation criteria to include board members.

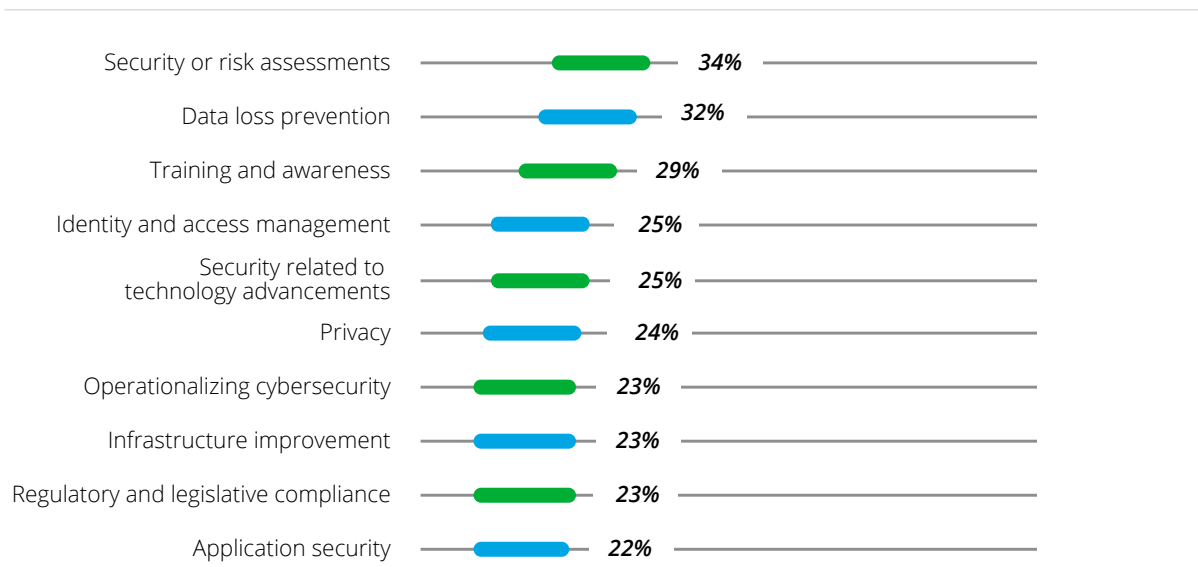
Share results of enterprise cyber risk assessments at the board level, including potential impact on key business outcomes in the areas of sensitive data protection, industrial control systems, and connected products.

Overall, one-third of manufacturers surveyed indicate their cybersecurity budgets have either remained flat or decreased over the past three years despite the growing concern posed by cyber risk. Two-thirds of executives said their cybersecurity budget represents between 3 percent and 10 percent of the company's annual information technology (IT) spend.

Initiatives and required resources to address concerns are diverse

The top three near-term cyber initiatives cited by manufacturing executives surveyed are: (1) enterprise cyber risk assessments, (2) data loss prevention programs, and (3) increased employee training and awareness. Initiatives, such as war-gaming simulations, are much further down the list with only 12 percent of manufacturing executives indicating it was at the top of their agenda for the balance of the year.

Figure 3: Top ten near-term cybersecurity initiatives



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

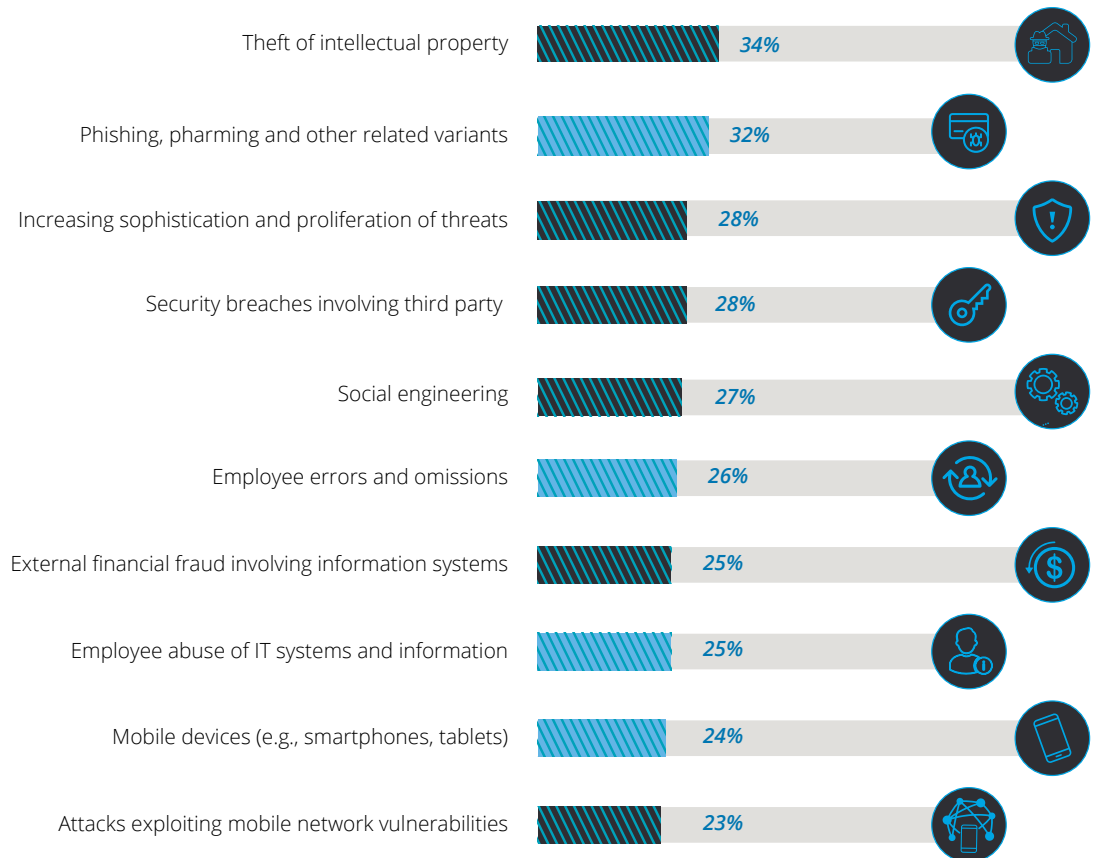
Be purposeful in addressing talent-related challenges



The weakest link in the cyber chain

Manufacturing executives indicate four of the top 10 cyberthreats facing their organizations are directly attributable to internal employees. These threats include: phishing/pharming, direct abuse of IT systems, errors/omissions, and use of mobile devices. Smaller companies (<\$500M in revenue) are more exposed to direct employee threats while mid-size companies (\$500M–\$5B in revenue) are more concerned with intellectual property theft and large companies (>\$5B in revenue) report their largest cyber risk concern focuses on phishing and pharming threats, which most often target financial gain or intellectual property.

Figure 4: Top 10 cyberthreats facing manufacturers



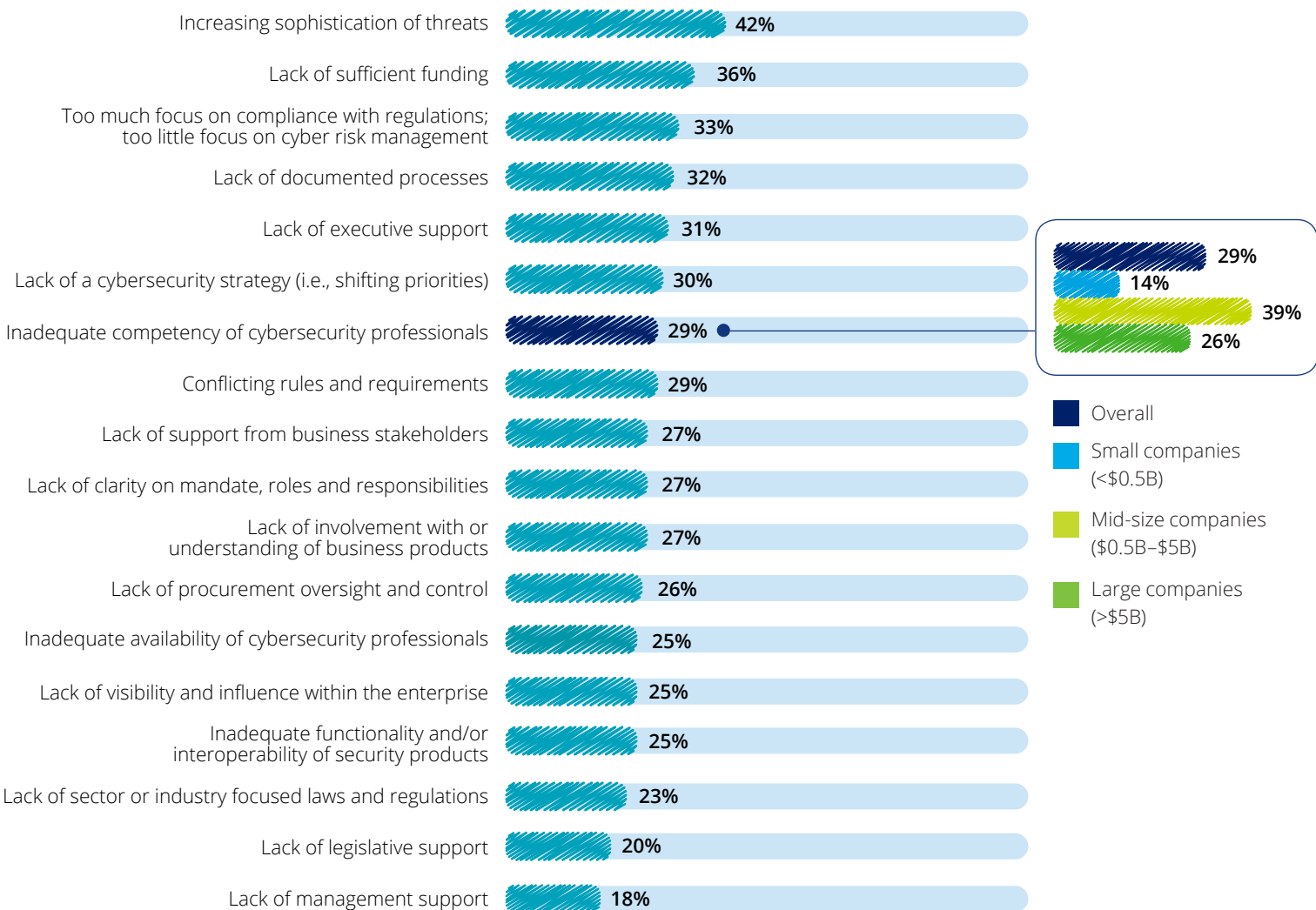
Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Talent and organizational challenges

The lack of skilled talent in the cybersecurity function represents a significant challenge for manufacturers surveyed, especially for mid-size companies (\$500M–\$5B in revenue). The difficulty in attracting and retaining cybersecurity talent makes it hard for companies to maintain an adequate defense against cyber adversaries’ intent on penetrating enterprise networks.

Chief information security officer (CISO) reporting structures vary significantly within manufacturing organizations as 30 percent of executives surveyed indicate their company’s CISO reports directly to the chief executive officer (CEO), while a further 31 percent report to the chief information officer (CIO), leaving nearly 40 percent of CISOs reporting to someone else in the organization.

Figure 5: Organizational barriers to cybersecurity



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.



What manufacturers can do to address talent-related changes

Establish a cross-functional team of key stakeholders in the cyber program, including IT, operational technology (OT), R&D, Finance, and Risk. Identify and socialize the risk framework with this team to define key mitigation strategies, and clearly identify ownership for implementation.

Implement engaging learning programs focused on identifying and reporting potential threats.

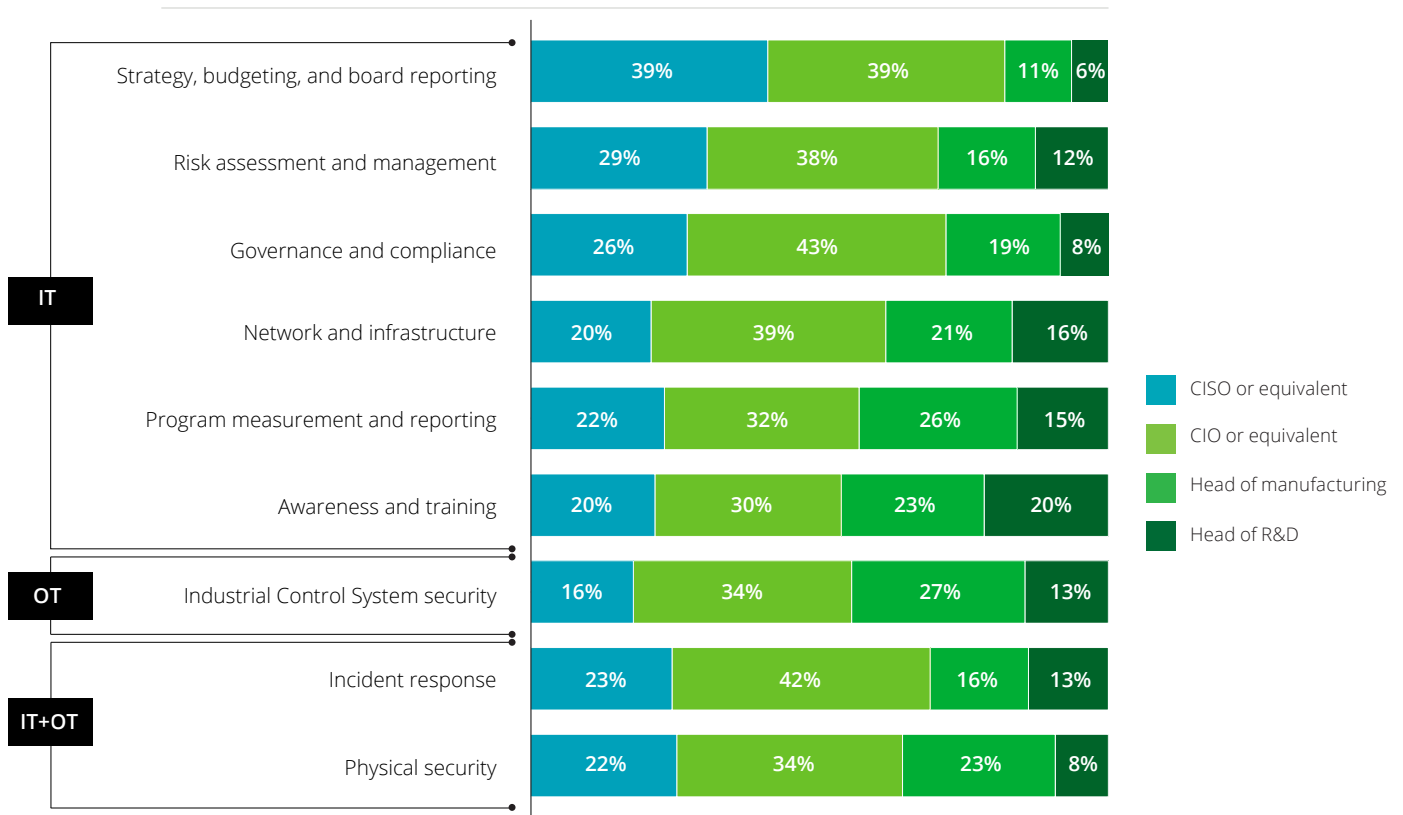
Simulate real-life threat scenarios with a cross section of the executive leadership team to perform knowledge checks periodically and assess real threat management preparedness. Assess results of various simulation tests to gauge effectiveness and incorporate lessons learned into iterative awareness and learning programs.

The IT/OT divide

Further, ownership of key areas of cyber risk, such as ICS and connected products may be unclear or fall outside the responsibilities of the CISO/CIO to manufacturing operations, research and development, or other departments, which may not be as high a priority or mature in identifying and addressing cyberthreats.

Ownership of enterprise cyber risk is often fragmented across an organization to include leaders in Operations (industrial control systems), Research and Development (R&D) (intellectual property, smart products), or other departments or business units resulting in varying levels of maturity and approaches in handling cyber risk. This may leave CISOs with a limited visibility of the enterprise cyber risk landscape and limited ability to influence policies, risk management strategies, and remediation activities for these important parts of the business.

Figure 6: Ownership of cybersecurity functions



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Remain vigilant in protecting critical investments in intellectual property

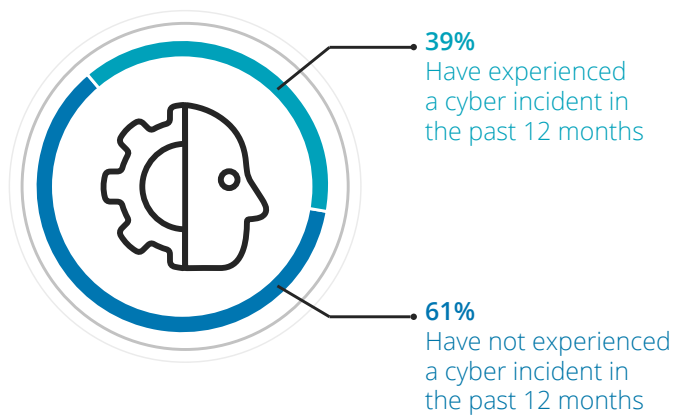


Intellectual property is top data protection concern

A significant percentage (35 percent) of executives surveyed believe intellectual property (IP) theft was the primary motive for the cyberattacks experienced by their company in the past 12 months—second only to financial theft (45 percent). Many companies interviewed had not yet fully implemented data protection and data loss prevention programs to mitigate this risk.

Theft of intellectual property is the most frequently cited cyberthreat (34 percent of surveyed executives) facing manufacturers, followed closely by phishing and pharming attacks (32 percent). IP theft also ranks closely with consumer data as the top sensitive data concern for manufacturing companies. (see Figure 4).

Figure 7: Percent of manufacturers that have experienced a cyber incident in the past 12 months

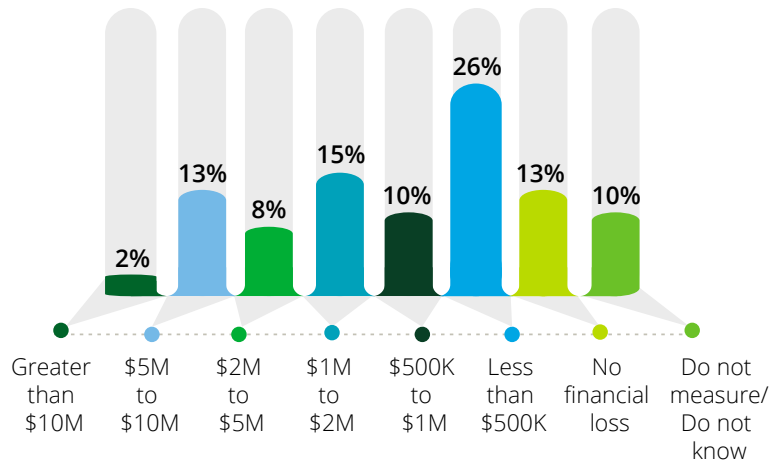


Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Who is responsible for IP protection?

In 42 percent of advanced manufacturing companies surveyed, the responsibility for IP protection falls to someone other than the CISO (20 percent) or the CIO (33 percent). In fact, 20 percent of executives indicate IP protection falls under the head of R&D, while a further 22 percent of executives said this responsibility falls to the head of manufacturing.

Figure 8: Average monetary damages of cyber incidents in the past 12 months



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Figure 9: Top motives for cyber incidents



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.



What manufacturers can do to protect IP

Inventory and classify the IP at the source and corresponding systems that store/process such IP. Determine who uses the IP in the organization and how widely it is distributed, including other departments and third parties.

Reduce the value of sensitive data by encrypting or obfuscating the data to render it difficult to use when compromised or securely destroy it when it is no longer necessary for legitimate legal or business purposes.

Apply security controls at the data layer itself whether IP is stored in documents or in databases. These capabilities include preventative solutions, such as digital rights management (DRM), as well as detective solutions, such as DLP, data access governance, and database activity monitoring. Develop an overall strategy to protect the IP and select tools that complement each other and cover the risk holistically.

Harden security, implement monitoring, and incident response for industrial control systems



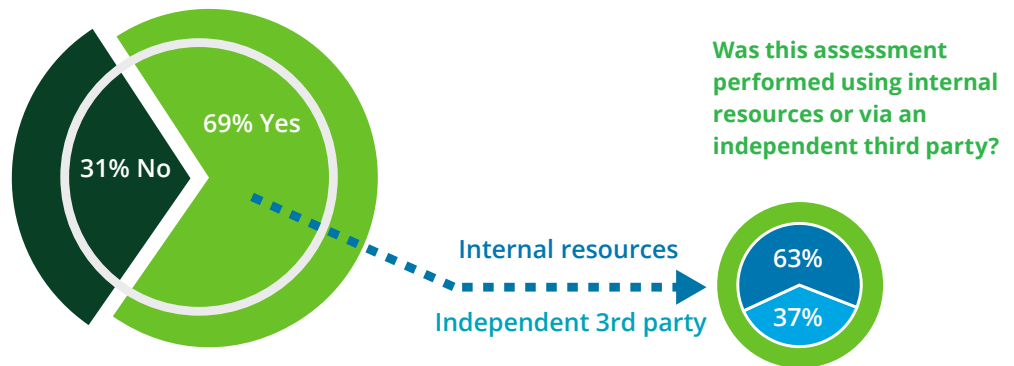
Cyber risk assessments need improvement

Almost one-third of manufacturers have not performed any cyber risk assessments specifically focused on the industrial control systems operating on their shop floors, resulting in a potentially significant risk to their operations.

Further, nearly two-thirds of companies that have performed an ICS cyber risk assessment used internal resources, potentially introducing organizational bias into the assessment process.

Figure 10: Risk assessments focused on ICS

Has your organization performed a cyber risk assessment specifically focused on your plant or manufacturing ICS?



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Half of all advanced manufacturing companies surveyed address shop floor related security vulnerabilities through network segmentation. Further, 43 percent of manufacturing executives surveyed indicate they isolate their facilities from outside networks (air-gapping).

Although air-gapping is a common approach to ICS security, when companies actually take the next step to test that strategy, they often find it is a fallacy.

This can lead to at least two significant concerns:

- 1 Many manufactures have not tested or monitored this control or conducted a thorough inventory of connected assets. As such, live network access points, especially easy to install wireless access points, can remain hidden from view.
- 2 In an ever more increasingly connected business environment, simply cutting off access to the outside world can severely limit a company from accessing key advanced technology cost savings and efficiency benefits.

Half of the manufacturing executives surveyed indicate their companies perform targeted vulnerability or penetration tests on their ICS less often than once a month. Further, only one in five manufacturers indicate that implementing a secure information and event management (SIEM) system or security operations center is a top near-term priority.

Over one-quarter of surveyed companies incident response programs have not included OT in those plans.



One in four companies surveyed do not develop, implement, or document ICS-specific policies and procedures, so stakeholders have a comprehensive understanding of the company's stance on ICS security.



What manufacturers can do to secure ICS

Create a holistic inventory

of all connected devices, including ICS that are attached to network segments. This can be done through a combination of passive scanning and physical observations.

Create a “zero trust network”

(i.e., “never trust, always verify”) that extends to all layers of the enterprise. This reduces the exposure of vulnerable systems, including ICS, while decreasing the likelihood of lateral movement in the event of a breach.

Form a cross-functional security team,

including, but not limited to representatives from global information security, engineering, operations, and the control system vendor. Providing all relevant groups a seat at the table consistently improves the organization’s ability to respond to risks while also considering operational issues that could arise as a result. It also can improve overall visibility into the decision-making process across departments.

Design cyber risk management mechanisms into connected products before deployment





Rapidly evolving connected products environment

Close to 50 percent of manufacturers surveyed have mobile apps associated with their connected product. In addition, 76 percent of companies surveyed choose WiFi to enable data flows between their connected products, easily eclipsing the use of Bluetooth (48 percent).

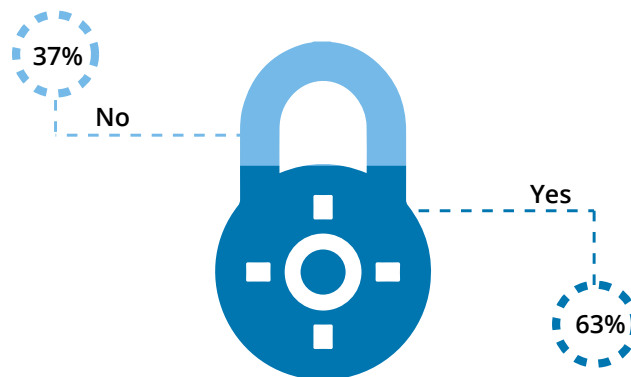
Over half of manufacturing executives (52 percent) surveyed said the connected products their companies produce are able to store and/or transmit confidential data, including social security and banking information.

The most common method of securing this information as it flows through connected products is data encryption, cited by 55 percent of executives surveyed.

A significant number of manufacturing companies surveyed use internal resources rather than external, third parties for product-related security assessments. This is particularly true for both applications (57 percent) and network assessments (49 percent). This can be seen as a potential missed opportunity for manufacturers to take advantage of unbiased, fresh thinking that comes from working with external partners.

In cases of product-related cyber breaches, nearly 40 percent of manufacturers surveyed do not incorporate those products within the company's broader incident response plan, signaling a need for a more holistic approach to cyber risk when it comes to connected products.

Figure 11: Percentage of incident response plans that encompass connected products



Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.



What manufacturers can do to address connected product risks

Assess value add for new connected product functionality prior to release. Each new feature set brings additional risk to the consumer and the organization that requires protection from malicious intent.

Engage actively with legal to make sure customer agreements clearly reflect roles and responsibilities with respect to connected product data ownership, responsibilities for product breach incidents, and other customer responsibilities to manage cyber risks.

Security by design principles and strong application security is paramount to connected product security. Firmware is sometimes not able to be updated by consumers/ customers and oftentimes is neglected even when updates are available. Organizations today have an expectation to produce secure products off the assembly line or potentially face negative impacts in operations, brand, regulatory compliance, or functionality.

Identify and address emerging cyber risks in the industrial ecosystem



Increasing connectivity in the ecosystem

In terms of the broader value chain, today's ever-changing business environment sees increasing digital expectations from clients and customers and new cybersecurity requirements being put on suppliers. Many manufacturers are just beginning to assess cyber risks related to key third parties in their innovation network, subcontractors, supply chain, and other critical business partners.

Strength in numbers

There is also a growing desire among manufacturers to share knowledge and best practices around cyberthreats as many companies operating in this space see the same kind of challenges on a daily basis.

A significant percentage (86 percent) of executives surveyed indicate the preferred method of managing the adequacy of third-party cyber practices is through identification of any material risks as part of the normal assessment process. Further, 84 percent of respondents also indicated they address third-party cyber risk through the contracting process, while 81 percent said they prefer to sign confidentiality and/or nondisclosure agreements.



What manufacturers can do to engage the industrial ecosystem

Define requirements for third-party cyber risk management upfront in key contracts. Make sure there is a right to audit against those requirements.

Increase monitoring and assurance activity over third-parties to significantly reduce overall cyber risk. Organizations should consider third party risk management programs to help ensure that third parties that access the network, systems, or data fulfill cybersecurity requirements.

Visiting third-party locations are considered the most effective method to gain assurance over cyber risk management.

Be Secure.Vigilant.Resilient.™

Top 10 next steps

In order for manufacturing companies to capture the business value associated with emerging exponential technologies, address the dynamic cyber risk landscape, and increase preparedness should a cyber breach occur, they must remain secure, vigilant, and resilient. To start this journey, manufacturing executives should consider the following top 10 action items:

1. Set the tone. Set the right tone at the top for cyber in the organization. The CISO cannot be an army of one. He or she needs to be appropriately supported by the leadership team and management to accomplish key cyber risk objectives for the company.

2. Assess risk broadly. Perform a cyber risk assessment that includes the enterprise, ICS and connected products. If the organization has already conducted one in the last six months, review the scope to confirm it was inclusive of advanced manufacturing cyber risks, such as IP protection, ICS, connected products, and third-party risks related to industrial ecosystem relationships. Make sure this risk assessment addresses the principles around being secure, vigilant, and resilient.

3. Socialize the risk profile. Share the results of the enterprise cyber risk assessment and recommended strategy and road map with executive leadership and the board. Engage in dialogue as a team related to the business impact of key cyber risks and discuss how to prioritize resource allocation across the secure, vigilant and resilient areas to address those risks commensurate with the organization's risk tolerance, risk posture and capability for relevant business impact.

4. Remember data is an asset. It is important to change the mindset in manufacturing from a transactional mindset to the fact that certain data alone may be an asset. This likely necessitates a tighter connection between business value associated with data and the strategies used to protect it. In addition, it is important to assess not only where valuable data is at rest in the organization, but also how its risk profile changes as it moves throughout the organization, from business systems, to the shop floor, through the supply chain, and to third parties and back.

5. Build in security. Evaluate top business investments in emerging manufacturing technologies, IoT, and connected products, and confirm whether those projects are harmonized with the cyber risk program. Determine whether cyber talent is resident on those project teams to help them build in cyber risk management and fail safe strategies on the front end.

6. Assess third-party risk. Inventory mission-critical industrial ecosystem relationships and evaluate strategies to address the third-party cyber risks that may coincide with these relationships.

7. Be vigilant with monitoring. Be vigilant in evaluating, developing, and implementing the company's cyberthreat monitoring capabilities to determine whether and how quickly a breach in key areas of the company would be detected. Remember to extend cyberthreat detection capabilities to the shop floor and connected products.

8. Always be prepared. Increase organizational resiliency by focusing on incident and breach preparedness through table top or war-gaming simulations. Engage IT as well as key business leaders in this exercise.

9. Clarify organizational responsibilities. Be crystal clear with the executive leadership team on the organizational ownership responsibilities for key components of the cyber risk program and make sure there is a clear leader on the team with responsibilities to bring it all together.

10. Drive increased awareness. Last, but certainly not the least, get your employees on board. Make sure they are appropriately aware of their responsibilities to help mitigate cyber risks related to phishing or social engineering, protecting IP and sensitive data, and appropriate escalation paths to report unusual activity or other areas of concern.

Cyber risk is, and always has been, more than just a concern for the IT department. It remains a critical part of every manufacturing environment and concerns every employee, contractor, partner, or customer with whom a company interacts. As manufacturing processes and technologies continue to advance, with such progress comes new threats and new opportunities. The question every manufacturer must ask is whether they wish to make cyber risk an advantage or a disadvantage for their company. Given the pace of today's competitive climate, manufacturers cannot afford to slow innovation simply because it cannot be perfectly secured, but neither can they innovate without appropriate regard for the inherent risks being generated. Cyber risk and innovation are inextricably linked and rather than subordinating one to the other, senior executives should harmonize these important elements of business performance through a program to become secure, vigilant, and resilient.

Acknowledgements

Authors

Trina Huelsman

Vice Chairman
US Industrial Products and
Services Leader
Deloitte & Touche LLP

Ed Powers

US Managing Principal
Cyber Risk Services
Deloitte & Touche LLP

Sean Peasley

Partner
Cyber Risk Services Consumer and
Industrial Products Leader
Deloitte & Touche LLP

Ryan Robinson

Industrial Products and
Services Research Leader
Center for Industry Insights
Deloitte Canada

Contributors

Stephen Gold

President and CEO
MAPI

John Miller

Council Director
MAPI

Maria Negron Kneib

Council Director
MAPI

Gina Pingitore

Executive Director
Center for Industry Insights
Deloitte Services LP

René Stranghoner

US Industrial Products and
Services Marketing Leader
Deloitte Services LP

Barbara Mroczynski

Sector Specialist
Deloitte Services LP

Michelle Drew Rodriguez

Manufacturing Research Leader
Center for Industry Insights
Deloitte Services LP

Endnotes

¹ Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, 2016 Global Manufacturing Competitiveness Index Study

² Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, Advanced Technologies Initiative: Manufacturing & Innovation

³ Ibid.

⁴ Deloitte LLP, Safeguarding the Internet of Things: Being secure, Vigilant and Resilient in the Connected Age, 2015

⁵ Deloitte LLP and MAPI, Understanding Risk Assessment Practices at Manufacturing Companies, 2015

Sincere thanks and special acknowledgement to the professionals who informed the insights related to the key emerging themes in the cyber risk study:

Talent and human capital

- **Sharon Chand**, Advisory Principal, *Deloitte & Touche LLP*
- **Kirti Tidke**, Advisory Senior Manager, *Deloitte & Touche LLP*

Intellectual property

- **Dan Frank**, Advisory Principal, *Deloitte & Touche LLP*
- **Vikram Rao**, Advisory Senior Manager, *Deloitte & Touche LLP*

Industrial control systems

- **Mo Reynolds**, Advisory Principal, *Deloitte & Touche LLP*
- **Jason Hunt**, Advisory Senior Manager, *Deloitte & Touche LLP*
- **Ramsey Hajj**, Advisory Senior Manager, *Deloitte & Touche LLP*

Connected products

- **Russell Jones**, Advisory Partner, *Deloitte & Touche LLP*
- **Arun Perinkolam**, Advisory Principal, *Deloitte & Touche LLP*
- **Tyler Lewis**, Advisory Senior Manager, *Deloitte & Touche LLP*
- **Nick Sikorski**, Advisory Senior Consultant, *Deloitte & Touche LLP*

Industrial ecosystem

- **Adam Thomas**, Advisory Principal, *Deloitte & Touche LLP*
- **Jayee Hegde**, Advisory Manager, *Deloitte & Touche LLP*
- **Karan Kartikey Singh**, Advisory Manager, *Deloitte AERS India Pvt L*

Deloitte and MAPI would like to also thank the following professionals who have contributed to the research and this publication:

Matthew Zaruba, Advisory Senior Manager, *Deloitte & Touche LLP*, **Jonathan Chan**, Advisory Senior Manager, *Deloitte & Touche LLP*, **Sandeepan Mondal**, *Deloitte Support Services India Pvt. Ltd.*, **Beth Ruck**, Senior Manager, *Deloitte Services LP*, **Karen Ambari**, Senior Manager, *Deloitte Services LP*, **Elizabeth Schmidt**, Manager, *Deloitte Services LP*, and **Whitney Garcia**, Manager, *Deloitte Services LP*.



About the Deloitte Center for Industry Insights

The Deloitte Center for Industry Insights in the United States leads Deloitte's extensive industry research that informs stakeholders across the consumer business and manufacturing ecosystem of critical business issues including emerging trends, challenges, and opportunities. Using primary research and rigorous analysis, the Center provides unique perspectives and seeks to be a trusted source for relevant, timely, and reliable insights. To learn more, visit www.deloitte.com/us/cb and www.deloitte.com/us/manufacturing.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

About MAPI

The Manufacturers Alliance for Productivity and Innovation (MAPI) is a member organization focused on building strong leadership within manufacturing, and driving the growth, profitability, and stature of global manufacturers. MAPI contributes to the competitiveness of US manufacturing. MAPI provides the timely and unbiased information that business executives need to improve their strategies, boost productivity, and drive innovation. For more information, please visit www.mapi.net/about.

About Forbes Insights

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, publisher of Forbes Magazine and Forbes.com, whose combined media properties reach nearly 75 million business decision makers worldwide on a monthly basis. Forbes Insights conducts primary research designed to support both strategic and tactical decisions for business leaders.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this publication contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.