Deloitte.

MAPI

Cyber risk in advanced manufacturing

Contents

1 Executive summary **3**

2 Executive and board-level engagement **14**

3 Talent and human capital **22**

4 Protecting intellectual property **30**

5 Inherent risks in industrial control systems **34**

6 Implications of rapidly evolving connected products **40**

7 Cyber risk in the industrial ecosystem **44**

8 The changing nature of the cyberthreat landscape **46**

9 Conclusion **50**

10 Endnotes **51**

11 Authors and acknowledgements **52**

Executive summary

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 (IP) and exponential technologies[2]
- Exploration of industry 4.0 digital manufacturing[3] opportunities and increased interconnectivity of the industrial ecosystem[4]
- 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, and the recent enterprise risk study[5] 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 coalesced around the following key themes.

Executive and board level engagement

Talent and human capital

Intellectual property

Industrial control systems (ICS)

Connected products

Industrial ecosystem

We believe these themes 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. Key insights from the study include:

1. Executive and board level engagement

- Given its focus on innovation and an increasing reliance on connected products, those interviewed consistently shared their belief that manufacturing is an industry that is 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 risks, and in having the organizational ownership to do so effectively. 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.
- Due to the growing severity and sophistication of cyberattacks, only 52 percent of surveyed executives 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.
- In some cases, there are challenges with top leadership for funding, as cyber risk has not always been a top-of-mind topic. However, according to our survey, 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. When it comes to a board update, the following framework can help boards evaluate questions to ask to determine whether the scope of the update they are receiving is complete:

Cyber risk programs: a framework for leading practice board reporting

Traditional 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**

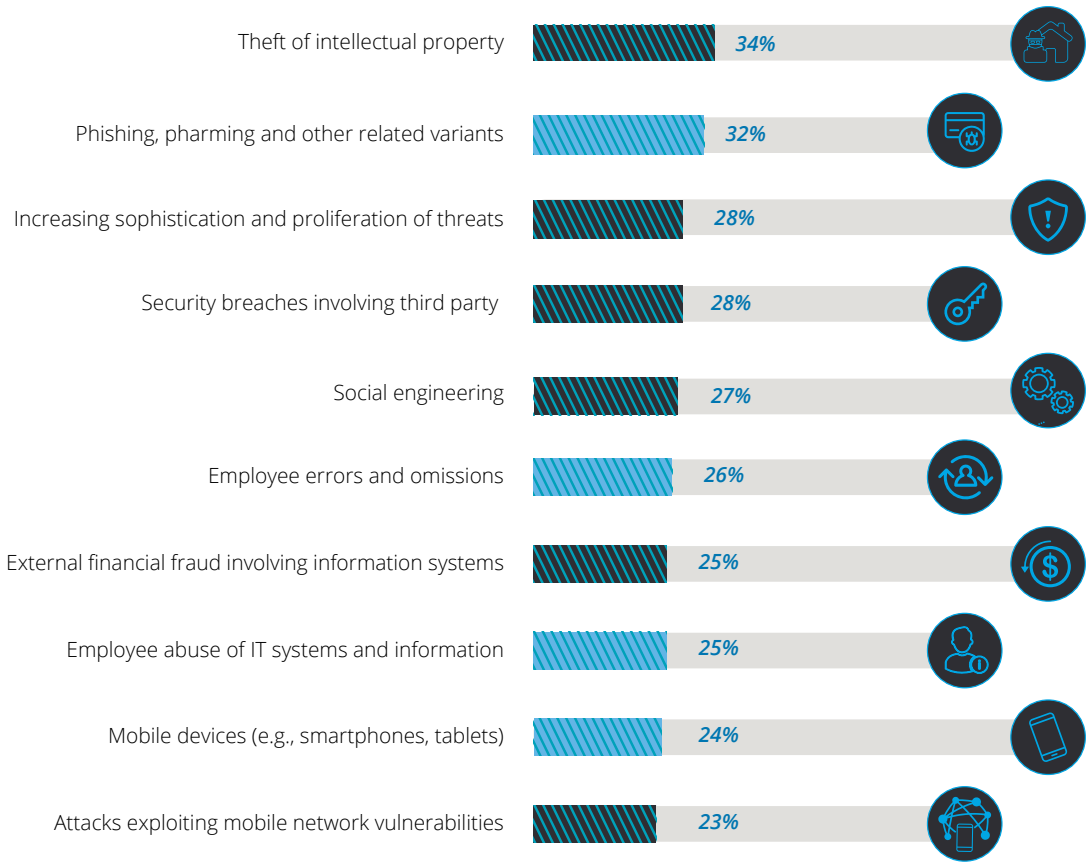
IT/OT gap **drives behavior**

	Enterprise Network & Business Systems	Industrial Control Systems	Connected Products
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	50% isolate or segment ICS networks 31% have not conducted an ICS assessment	**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** 28% 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

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

The top three near-term cyber initiatives cited by manufacturing executives are: (1) enterprise cyber risk assessments, (2) data loss prevention programs, and (3) increased employee training and awareness. Initiatives such as wargaming 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 2: Top 10 cyberthreats facing manufacturers (percent of respondents)



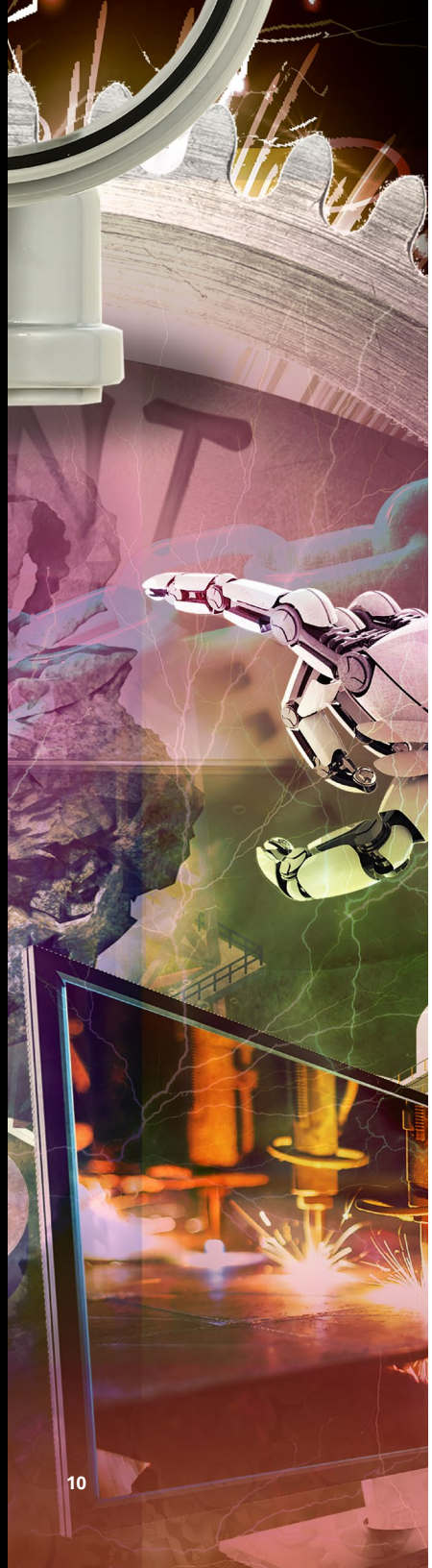
Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

2. Talent and human capital

- Manufacturing executives indicate that four of the top ten 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 midsize companies ($500M-$5B in revenue) are more concerned with IP 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 IP.
- The lack of skilled talent in the cybersecurity function represents a significant challenge for manufacturers, especially for midsize 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 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. 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 (R&D), 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 (ICS), R&D (IP, 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.

3. Intellectual property

- Over one-third (35 percent) of executives believe 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 of survey respondents). Many companies interviewed had not yet fully implemented data protection and data loss prevention programs to mitigate this risk.
- Theft of IP 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.
- In 42 percent of surveyed advanced manufacturing companies, 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.



4. Industrial control systems

- Almost one-third of manufacturers have not performed any cyber risk assessments specifically focused on the ICS 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.
- Half of all advanced manufacturing companies address shop floor related security vulnerabilities through network segmentation. Further, 43 percent of manufacturing executives said 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. Since many manufactures have not tested or monitored this control or conducted a thorough inventory of connected assets, 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 implementing a Secure Information and Event Management (SIEM) system or Security Operations Center (SOC) is a top near-term priority.
- Over one-quarter of companies' incident response programs have not included operational technology (OT) in those plans.
- One in four companies do not develop, implement or document ICS-specific policies and procedures so that stakeholders have a comprehensive understanding of the company's stance on ICS security.

10

5. Connected products

- Close to 50 percent of manufacturers have mobile apps associated with their connected product. In addition, 76 percent of companies choose Wi-Fi to enable data flows between their connected products, easily eclipsing the use of Bluetooth (48 percent).
- Over half of manufacturing executives (52 percent) 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.
- A significant number of manufacturing companies 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 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.

6. Industrial 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.
- There is also a growing desire among manufacturers to share knowledge and leading practices around cyberthreats as many companies operating in this space see the same kinds of challenges on a daily basis.
- A significant percentage (86 percent) of executives surveyed for this study 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 indicated they address third-party cyber risk through the contracting process, while 81 percent said they prefer to sign confidentiality and/or non-disclosure agreements.

The following content explores each of the six themes in greater detail, offering insights derived from both the online survey and interviews with cybersecurity leaders at manufacturing companies.

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:

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 company has already done 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 secure, vigilant, and resilient principles mentioned above.

3. Socialize the risk profile. Share the results of the enterprise cyber risk assessment, and recommended strategy and roadmap with executive leadership and the board. Engage in dialogue as a team relative 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. Build 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 sound strategies on the front end.

5. Remember data is an asset. It is important to change the mindset in manufacturing from a transactional mindset to the fact certain data alone may be an asset. This will necessitate 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 resides in the rest of 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.

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 wargaming 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 least, get employees on board. Ensure 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.

The detail in this study provides a new opportunity to engage in a deeper dialogue around core aspects of a company's cyber risk program, identify continuous improvement opportunities, and establish a road map for companies to become secure, vigilant, and resilient.

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

Executive and board-level engagement

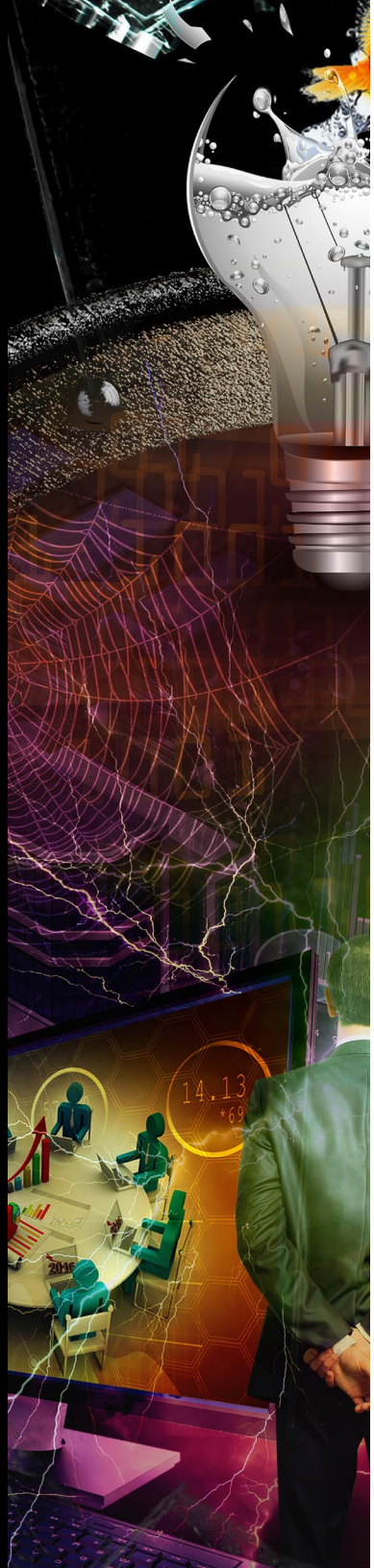
In March 2015, Deloitte released a study entitled Understanding Risk Assessment Practices at Manufacturing Companies in conjunction with MAPI, which focused on key risk factors spanning the manufacturing enterprise. One of the study's overwhelming findings was cybersecurity presents the largest IT risk. As such, additional research was conducted by Deloitte and MAPI to further explore this issue given its importance across the manufacturing sector, particularly as it pertains to ICS on the shop floor.

Moreover, from a corporate governance standpoint, cyber risk has become a more frequent topic of conversation at the board level. As manufacturing companies and their boards begin to pay closer attention to cyber risk, there is a need for a more holistic understanding of cyber risk trends and leading practices to enable them to be prepared to ask the right questions around the company's cyber risk profile, funding of key mitigation strategies, and how the cyber risk profile and threats are evolving over time.[6]

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.

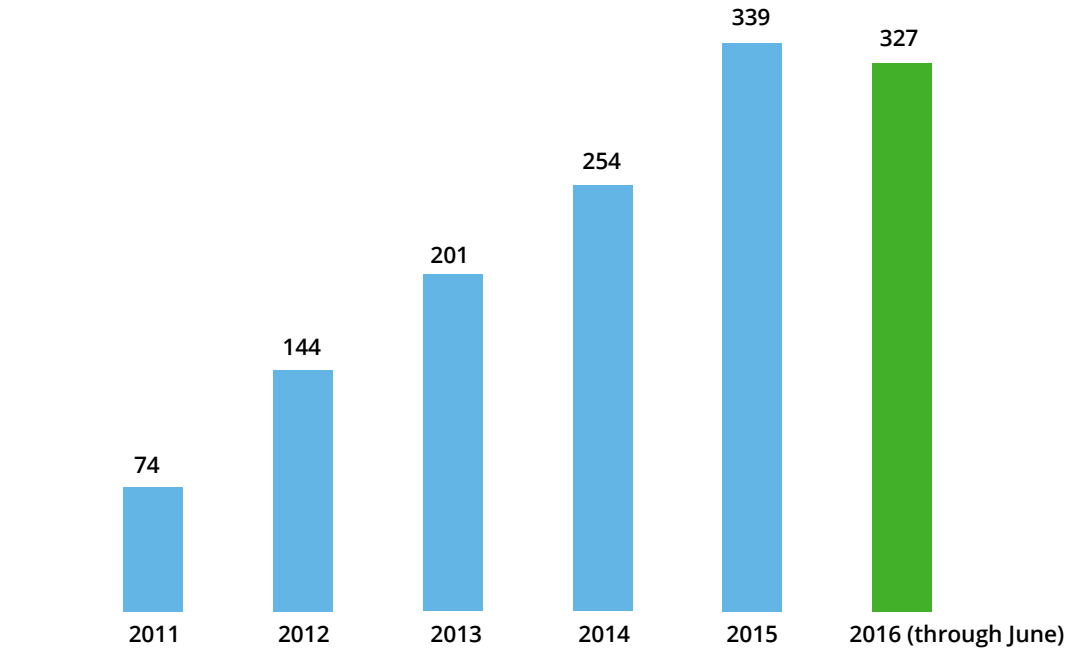
Top 10 questions[7] boards should be asking

1. How do we demonstrate due diligence, ownership, and effective management of cyber risk? Are risk maps developed to show the current risk profile, as well as timely identifying emerging risks we should get ahead of?
2. Do we have the right leadership and organizational talent? Beyond enterprise systems, who is leading key cyber initiatives related to ICS and connected products?
3. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
4. Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?
5. How do our cyber risk program and capabilities align to industry standards and peer organizations?
6. How do our awareness programs create cyber-focused mindset and cyber-conscious culture organization wide? Are awareness programs tailored to address special considerations for high risk employee groups handling sensitive intellectual property, ICS, or connected products?
7. What have we done to protect the organization against third-party cyber risks?
8. Can we rapidly contain damages and mobilize response resources when a cyber incident occurs? How is our cyber incident response plan tailored to address the unique risks in ICS and connected products?
9. How do we evaluate the effectiveness of our organization's cyber risk program?
10. Are we a strong and secure link in the highly connected ecosystems in which we operate?



It should be noted there is some evidence of a shift to prioritizing cyber risk. The term 'cybersecurity' has been increasingly cited as a key risk factor in 10-K SEC filings by manufacturing companies over the past five years (Figure 3). The number of citations has grown from only 74 in 2011 to 339 last year, and a 2016 figure (through June) suggests the sector will easily surpass last year's mark by a significant margin.

Figure 3: Cybersecurity instances in key risk factor section of 10-K filings—manufacturing sector (2011–2016 June YTD)



Source: Deloitte analysis.

According to some industry reports, the future is characterized by key cyber risk improvements, at least in the minds of executives surveyed. According to the Ponemon Institute© Research Report, 2015 Global Megatrends in Cybersecurity, postures regarding cybersecurity will improve as executives come to view their organization's cybersecurity as a competitive advantage, and briefings find their way to the board room.

In fact, although only 25 percent of those surveyed for the Ponemon report currently believe cybersecurity is a competitive advantage for their company, 59 percent of executives believe it will be regarded as such three years from now. Similarly, the percentage of executives indicating their organization's board of directors are being briefed on cybersecurity strategy is expected to grow from 22 percent today to 66 percent over the next three years.

"You need to educate your CEO and your CFO on the risks and threats. You need to make it personal."

Executive interviewee,
Deloitte and MAPI Cyber risk in advanced manufacturing study

Cybersecurity Disclosure Act of 2015

If passed into law, this piece of legislation will require all public companies to disclose the level of cybersecurity expertise embedded in the organization's board of directors (similar to financial expert proxy disclosures).[8] Specifically, companies will need to:

1) disclose whether any member of the governing body, such as the board of directors or general partner, of the reporting company has expertise or experience in cybersecurity and in such detail as necessary to fully describe the nature of the expertise or experience; and, if no member of the governing body of the reporting company has expertise or experience in cybersecurity,

2) describe what other cybersecurity steps taken by the reporting company were taken into account by such persons responsible for identifying and evaluating nominees for any member of the governing body, such as a nominating committee.[9]

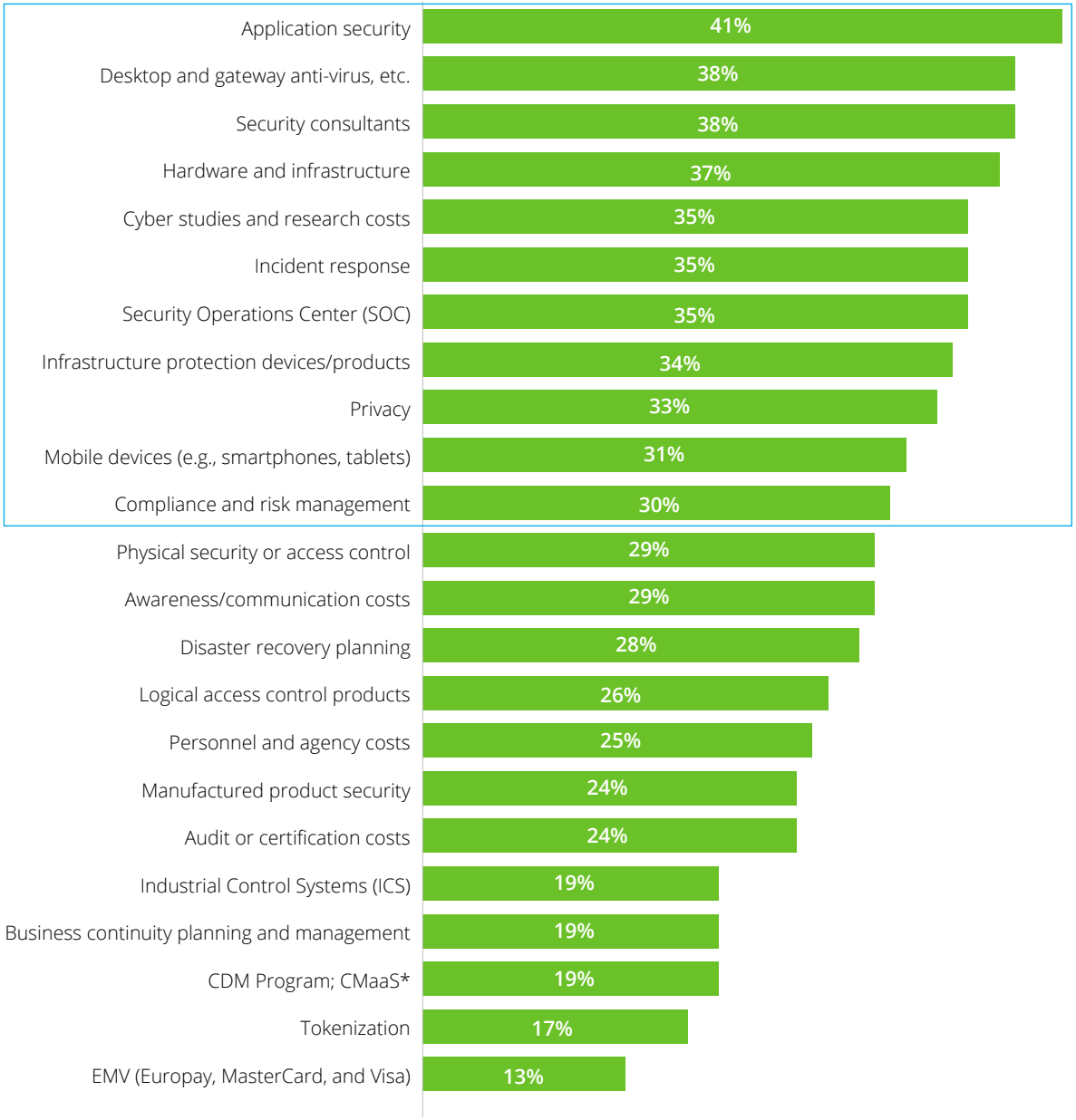
There still remains a strategy and implementation gap to close between now and the future. Board members may lack the technical understanding of cyber risk issues to fully evaluate the reported cyber risk profile and effectively assess the potential business impacts. Cyber leaders may struggle with fragmented organizational ownership and have difficulty clearly articulating to the board potential impacts associated with key areas of cyber vulnerability in the organization.

Further, manufacturers have traditionally taken a "transactional" approach to security, as opposed to viewing data as an asset to be protected. As many manufacturers do not have extensive data classification policies, board members are left with only a vague semblance of the cyber assets that need to be protected, including IP "crown jewels." As a result, board members may be more reluctant to support strategies for taking additional cybersecurity steps as it is not clear what needs to be protected.

Nonetheless, increasing prioritization of cyber risk at the highest levels of the organization has led some companies to review compliance requirements for established cybersecurity regulations. Study results show while only one in four manufacturers are reviewing the National Institute of Standards and Technology (NIST) framework, and plan to adopt it over the next six months, more than half of companies surveyed review and update their policies to be compliant with relevant cybersecurity laws and regulations.

Finally, due to fragmented organizational responsibilities, company boards and executive leadership teams may not hear a complete report of cyber risks beyond classic enterprise networks and business systems, to include ICS and connected products. For example, it may be surprising for a company board to hear study results indicate a third of manufacturers have not performed a cyber risk assessment focused on their ICS. Also, among companies surveyed that did perform such an assessment, 63 percent relied on internal resources to do so which limits a company's ability to generate unbiased results and make comparisons with its peer group.

Figure 4: Top initiatives funded in cyber budgets

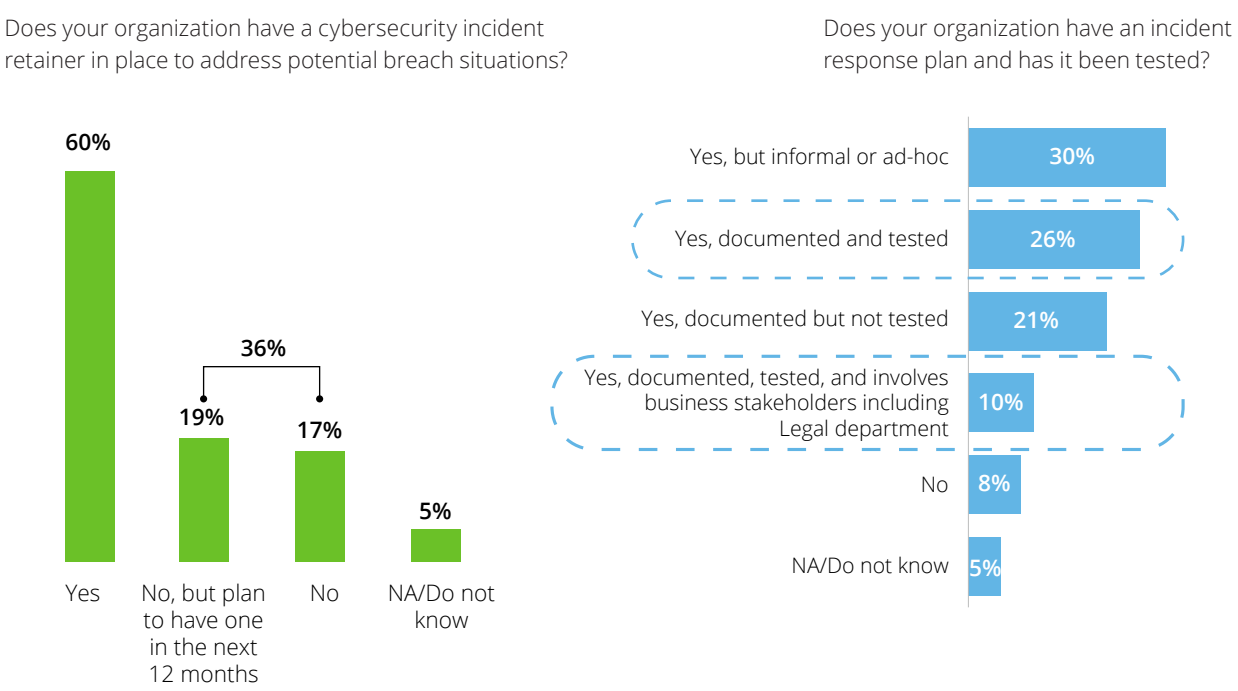


Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

A lack of comprehensive reporting and effective measurements may also lead company boards to discount potential safety and environmental risks, as there have only been a handful of documented occurrences where ICS systems were attacked in a way that impacted operations or caused physical damage. A lack of understanding regarding the state of a company's cyber readiness may also lead the board to discount the need for a cyber incident retainer and comprehensive response plan. In fact, study results show that 36 percent of manufacturers do not currently have a retainer in place and while 87 percent have a response plan, only 36 percent of manufacturers have it documented and tested.

More than a third of companies do not have a cybersecurity incident retainer in place. A vast majority (87 percent) of companies have an incident response plan but only a third (36 percent) have it documented and tested.

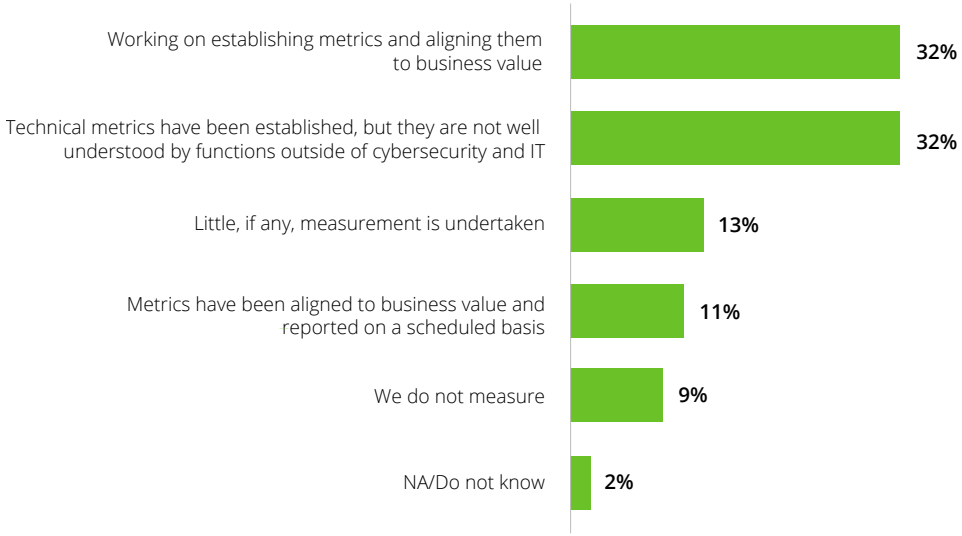
Figure 5: Readiness to tackle cyberthreats



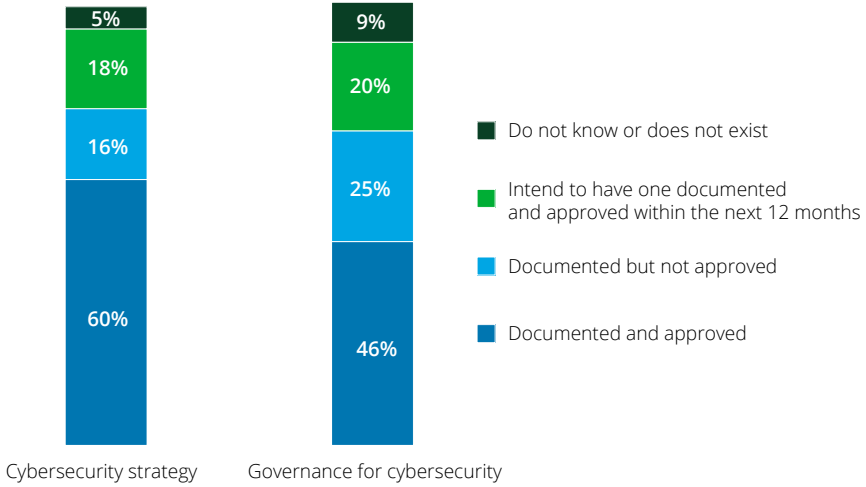
Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

Figure 6: Cybersecurity measurement and strategy

Which statement best describes how your organization measures your enterprise cybersecurity organization's activities?



Does your organization maintain the following strategy artifacts?



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

Executive and board-level playbook

- Establish a senior management-level committee with board member representation 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, ICS, and connected products.
- Establish a dashboard of key cyber risk indicators and trending to support continued dialogue around strategic investments designed to improve cyber maturity across the organization.
- Board updates on cyber profile should include results of broad employee awareness and resiliency efforts, including lessons learned from wargaming simulations and table top exercises. This should include transparency on the most likely cyber risk events a company may experience, key mitigation and incident response strategies, and continuous improvement opportunities identified.

Be purposeful in addressing talent-related challenges

Talent and human capital

Attracting, retaining and developing talent is a critical need throughout the manufacturing industry. Key findings from a recent Deloitte and Manufacturing Institute study[10] indicate 84 percent of executives agree there is a skills gap shortage in the US manufacturing sector. Adding to the complexity of this issue is finding workers with the individual skill sets required to meet today's advanced manufacturing requirements including cyber risk.

In a sector where cyber risk is growing at an exponential rate, human capital concerns such as bolstering an organization's cyber posture through the acquisition of qualified talent along with training and awareness throughout the employee base is critical. This section explores four key challenges:

- **Communication**—Bridging the gap between IT and C-suite
- **Fragmented cyber responsibilities**—The IT versus OT divide
- **Employee awareness**—The weakest link in the cyber chain
- **Insider threats**—Identifying and managing threats from within

Communication—Bridging the gap between IT and C-suite

Organizational structures among manufacturers can be as diverse as the products they produce. In fact, according to executives interviewed as part of the study, manufacturing companies, especially larger ones, are moving to a dedicated CISO, while some smaller / middle market companies do not have a CISO. Instead, they may have a variety of full-time resources aligned to cyber risk. They may even have particular people responsible for individual areas of enterprise cyber risk that are periodically pulled together to react to specific issues. Yet other companies have CISOs, but they have progressed through an IT environment and are ill-prepared to convey to the company's senior leadership the potential impact that cyberthreats can have on key business objectives.

In the first scenario, the reason companies do not have a CISO is, in part, organizationally driven and, in part, philosophically-driven. From an organizational perspective, some manufacturers prefer to consolidate the CISO function at a higher level in the command structure, usually with the CIO or Chief Technology Officer (CTO). The problem with this approach is by removing a key layer of management responsibility, the day-to-day vigilance required to maintain a sufficient cyber posture is often lost.

From a philosophical perspective, some companies believe addressing cyber risk should be the responsibility of the entire management team, if not the entire employee base. These companies are steadfast in their belief that it is detrimental to their overall objective of hardening the whole organization against cyberthreats by making only one person the sole security officer. In this case, the core argument is assigning just one person to the task tends to absolve everyone else of their duty to contribute to ongoing cybersecurity efforts.

The most impactful structure may lie somewhere in between these two approaches. It should be everyone's responsibility to understand how their actions can impact cybersecurity performance and the role they play. In addition, having a focused resource responsible such as a CISO may help to improve the maturity of the cyber risk program over the longer term by accomplishing the following objectives:

- Assessing changing cyber risks across the organization
- Developing and communicating policies and standards
- Monitoring effectiveness of key mitigation strategies
- Providing strategic advice on building in cyber risk mitigation to new investments and emerging technologies

There is also a very real communications gap between business leaders and cyber employees. While the business leadership is frequently not well versed in cyber risk, security professionals often do not have sufficient understanding of the priorities and decision models of the organization's business leaders. In addition, they may not fluently speak the language of business leaders. This communications gap may work against the effective funding and management of priority cyber risks. A great CISO can help bring teams together and bridge the gap between cyber risk and true business impact. To truly drive change, cyber leaders must articulate the "why?" behind key cyberthreats and initiatives, which is best done in terms of business risk to key investments, customers, operations, and cost.

Fragmented cyber responsibilities—The IT versus OT divide

In discussing different phases of maturity companies may have in addressing a broad range of cyber risks, it has become clear that organizational ownership responsibilities are a key driver in how employees are spending their time to address known and potential cyber risks to the company. According to the study results, this has been most clearly observed in relation to the organizational gap between IT (Information Technology or enterprise business systems employees) and OT (Operational Technology or shop floor operations employees). This gap in organizational ownership of the cyber risk issue may not be one of visibility, monitoring or identification of 'things gone wrong,' but more often may be about remediation of risk. For example, because a variety of OT groups own specific assets or ICS in the overall plant network, IT may have little control or influence over when or how issues get identified, remediated, monitored, or escalated to senior leadership.

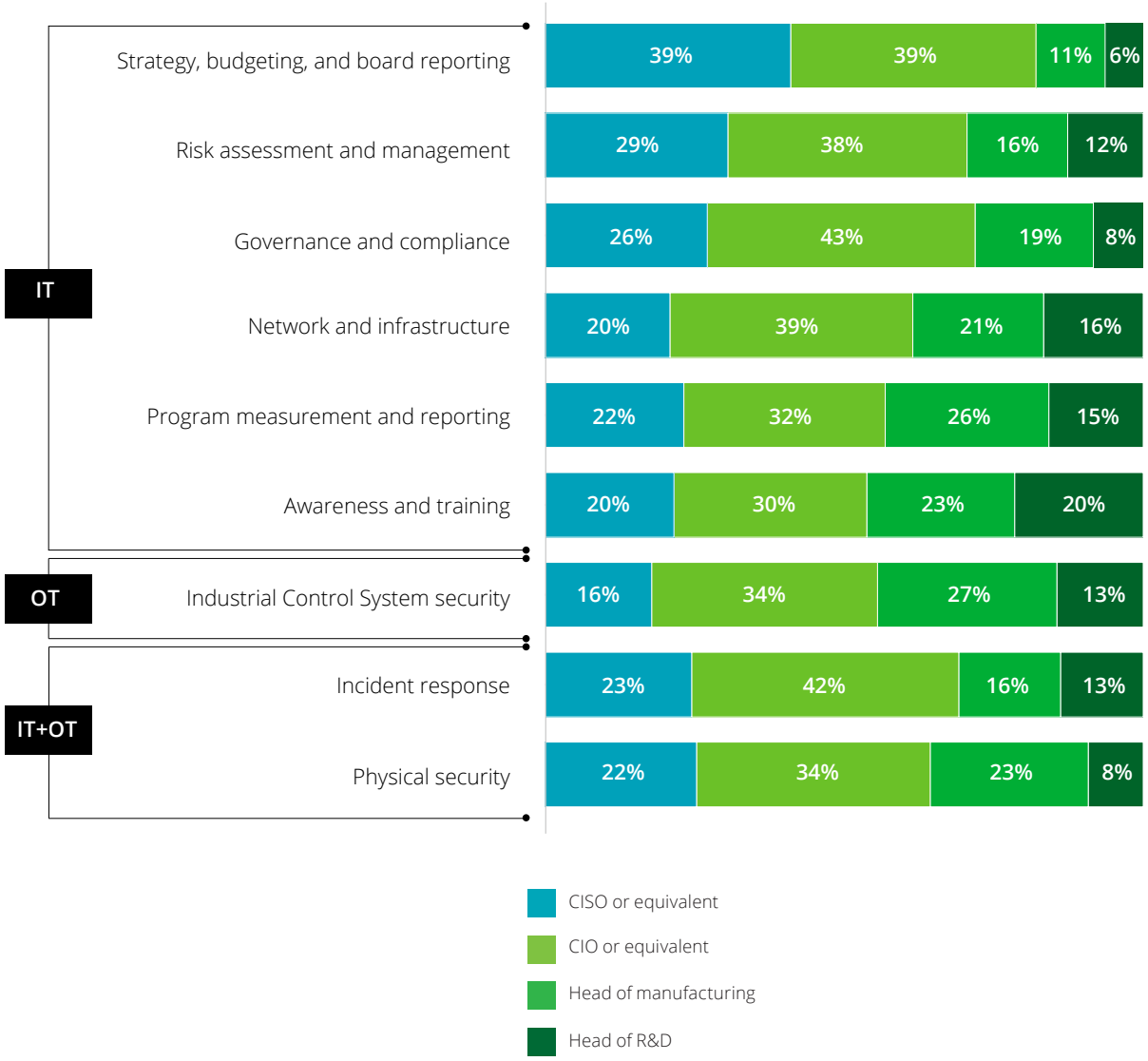
Further, in many cases, due to the high risk processing that ICS manage, operations personnel may be satisfied allowing that risk to remain unclear or resident with others in the organization, even if the CISO is unaware.

Additionally, the organizational mandates between these groups may be perceived as being at odds, with OT often wanting to keep production running at all costs, while IT may need "down time" to deploy upgrades, patches or other cyber remediation activities.

In order to ensure shop floor production operations strikes a balance between security and productivity, companies must create an ownership strategy among and between its employees that offers the greatest output while balancing risk at a tolerable level. A well-functioning internal cyber program has clear accountability established on multiple levels with special attention given to areas like responsibilities between IT and OT. A CISO might oversee the whole network and ensure connections are working, even when assets are individually owned/managed by others. Additional collaboration should occur between IT and OT when it comes to standard setting for cyber risk management for ICS systems in order to leverage knowledge and tools in the enterprise cyber space for the ICS world, as appropriate, or work together on alternate solutions that can achieve both uptime and cyber risk management objectives.

As organizations deploy their talent strategy in an environment with limited qualified resources, they often burden single individuals with the task of overall security. None know this burden more than the CIO, who typically takes on this responsibility; but as OT responsibilities become increasingly important, the head of manufacturing within a company is often the next to heed the call.

Figure 7: Primary responsibility for cyber functions



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

Employee awareness—the weakest link in the cyber chain

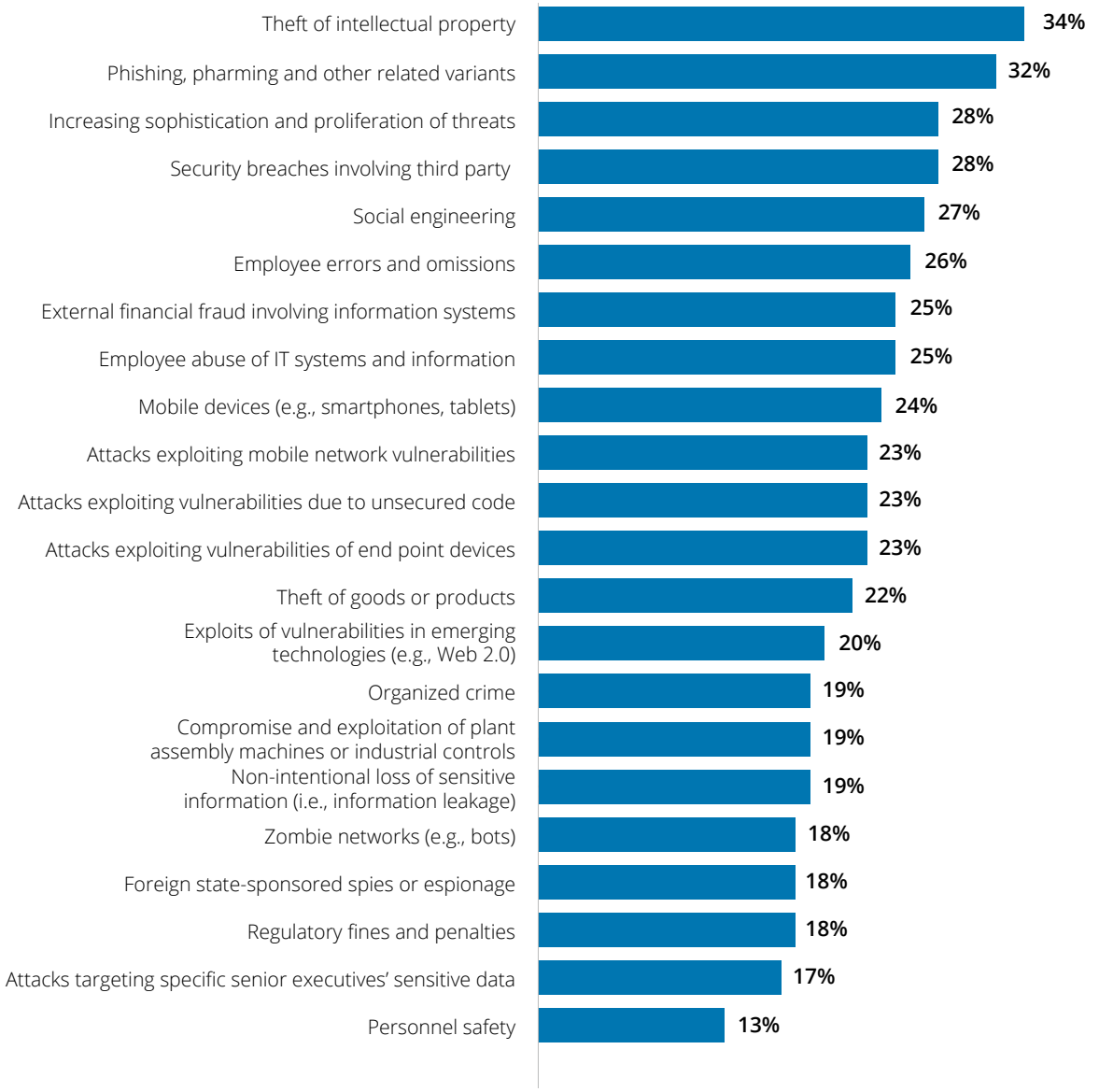
As digital transformation in the manufacturing space continues to accelerate, cyber has become a broad business risk rather than just an IT issue. It now encompasses nearly every aspect of a company's operations, from R&D to the factory floor, and the supplier to the customer. In other words, security concerns the entire enterprise ecosystem and the people that connect all these processes together.

Now, more than ever, manufacturers are exposed to a growing number of potential cyber breach points, spanning legacy control systems, connected ICS, and interconnected supply chains to name just a few. However, manufacturers also have to deal with threats posed by their own employees. In a world of increasingly mobile workforces, ever more ingenious phishing schemes, and a general lack of awareness regarding the security of digital assets, some manufacturers find their staff to be the weakest link in the cyber risk chain with four out of the top ten threats attributable to employees.

"In the last couple of years, our people have been one of our biggest exposures; whether the intent is malicious or not, it's always the weakest link."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

Figure 8: Top cyberthreats among manufacturers



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

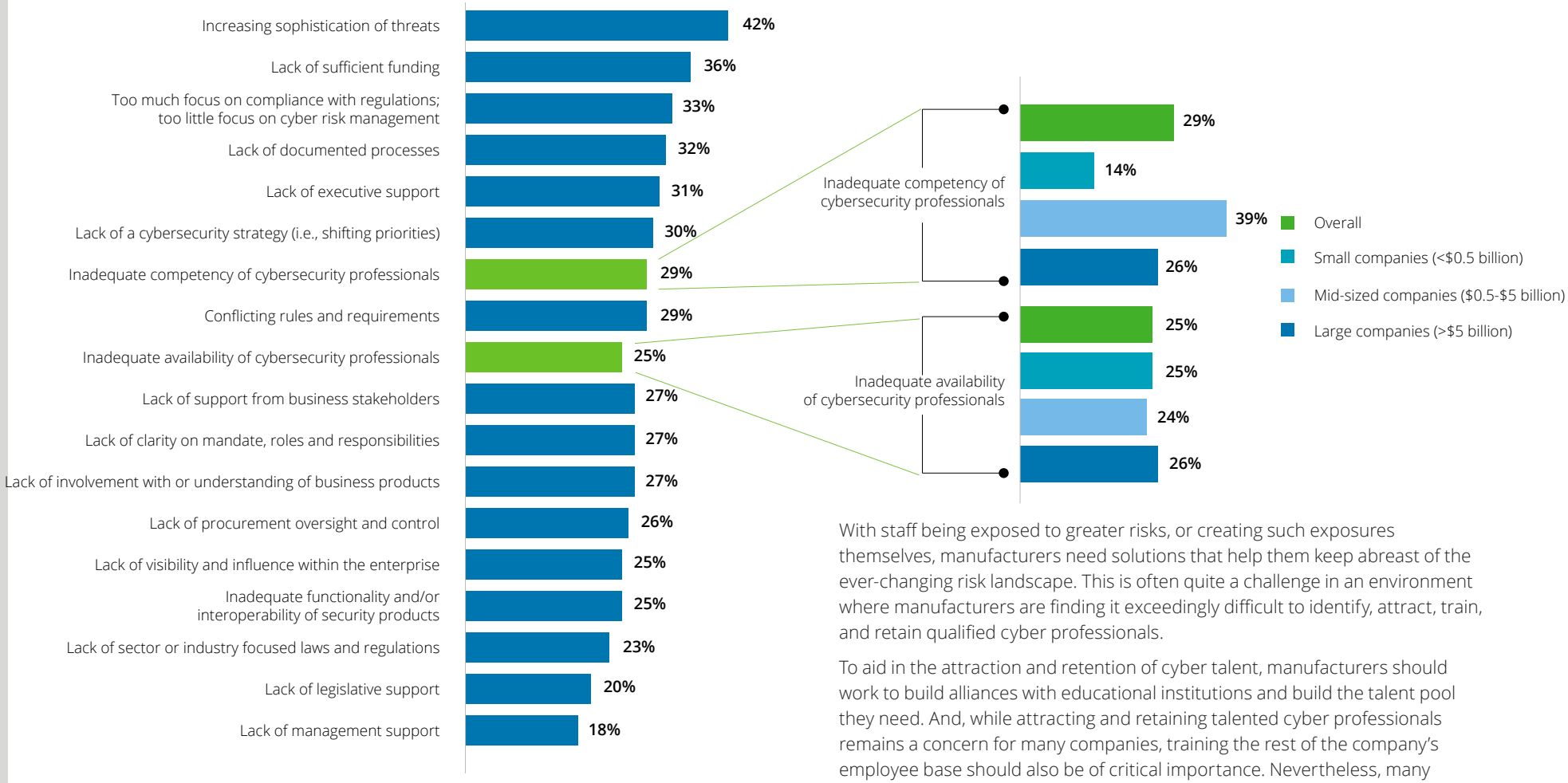
Every department and all levels of the workforce are exposed to cyber risk, as human touch points may serve as unwitting doorways for unauthorized or unsecure devices and users. When asked to characterize the nature of cyber-related incidents experienced in the last 12 months, surveyed manufacturing executives responded that the highest number of incidents—46 percent—originated within the organization with 39 percent deriving from external sources and 15 percent attributable to vendors or business partners.

Some of this concern with talent can be blamed on the lack of skilled professionals available to manage cyber risk. Two-thirds of executives interviewed for a recent Ponemon Institute© 2015 Global Megatrends in Cybersecurity Ponemon Institute© Research Report said their organizations need more knowledgeable and experienced cyber practitioners. Deloitte's own research supports this finding, with the further understanding mid-sized companies appear to be the hardest hit.

"IT talent and operations folks are not on the same page. The left hand doesn't talk to the right hand."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

Figure 9: Top barriers and challenges regarding cyber risk



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

Insider threats—Identifying and managing threats from within

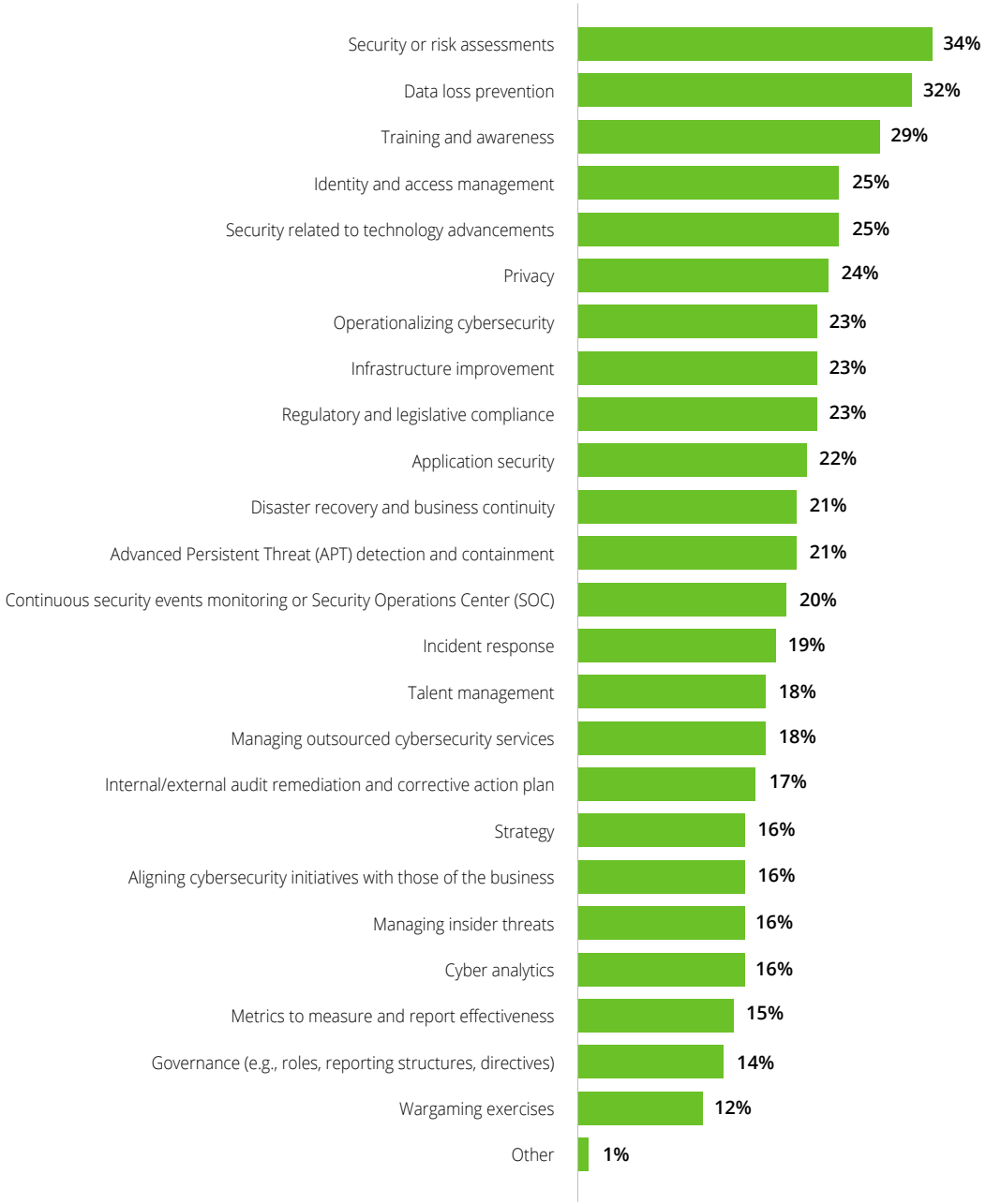
The most important part of any manufacturing operation is its people. In the new age of the IoT, and the frequency with which employees are permitted to Bring Your Own Device (BYOD), manufacturing companies are increasingly exposed to new and potentially more disruptive cyberthreats. The problem is a lot of these risks go unseen or are allowed to unduly impact the business due to the interconnectedness of legacy shop floor systems, a company's operations, and its processes.

With staff being exposed to greater risks, or creating such exposures themselves, manufacturers need solutions that help them keep abreast of the ever-changing risk landscape. This is often quite a challenge in an environment where manufacturers are finding it exceedingly difficult to identify, attract, train, and retain qualified cyber professionals.

To aid in the attraction and retention of cyber talent, manufacturers should work to build alliances with educational institutions and build the talent pool they need. And, while attracting and retaining talented cyber professionals remains a concern for many companies, training the rest of the company's employee base should also be of critical importance. Nevertheless, many companies report that providing training and raising awareness among their staff is not their top priority. In fact, not only should manufacturers focus more on training and awareness, but in general these programs should evolve and focus more on specific issues related to cyber risk (as most programs are too generic to be effective at altering employee behavior). In order to drive increased security awareness, companies should tailor awareness training to include specific objectives related to user populations that handle high risk data to increase their focus on what matters most.

While unwitting exposures resulting from carelessness or error may present one type of threat, many businesses have fallen victim to those with more malicious intent.

Figure 10: Top cyber risk initiatives among manufacturers

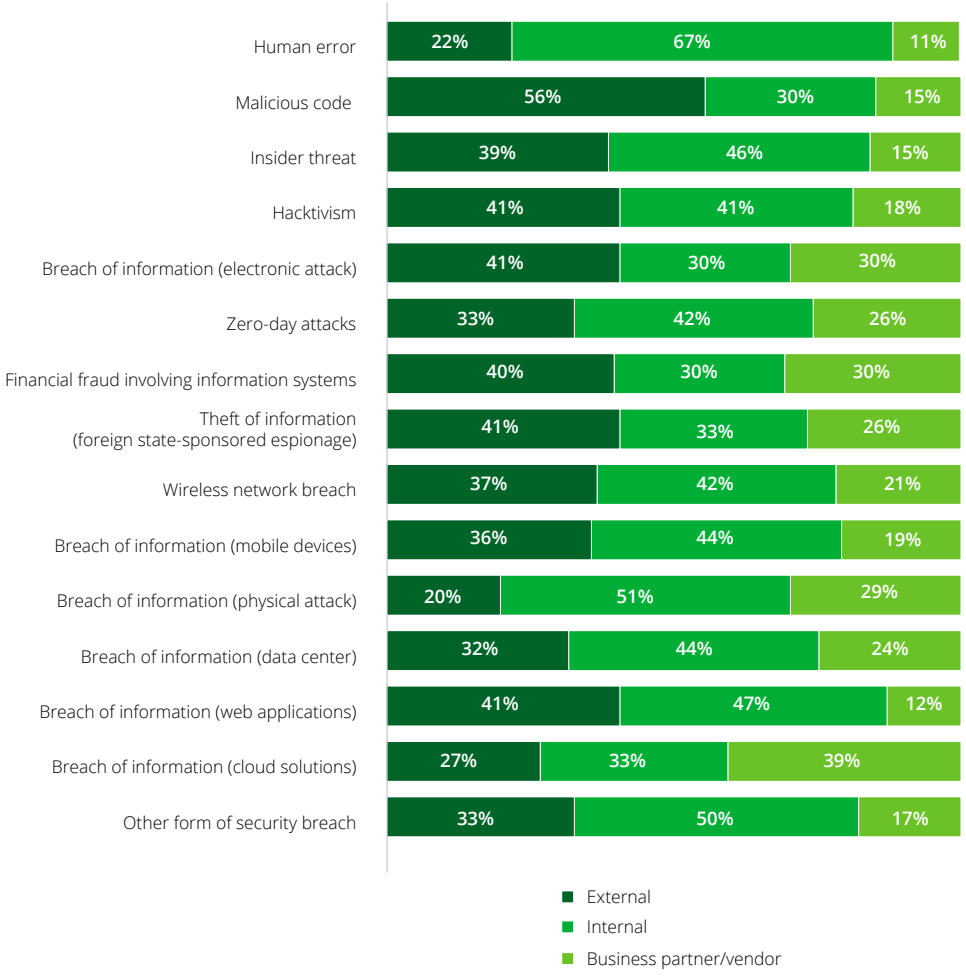


Source: Cyber risk in advanced manufacturing, Deloitte and MAPI.

"A combination of factors is dramatically reshaping OT security. More Internet connected industrial automation devices, and the convergence of OT and IT infrastructures, in addition to a shortage of security skills, means that accurate evaluation and mitigation of security risks is increasingly challenging."

Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT)

Figure 11: Types of cyber incidents in the past twelve months



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

Talent and human capital playbook

- Leadership sets the tone at the top and promotes a security culture through proactive, organizational-wide engagement and builds incentives for the entire workforce to be responsible for the cybersecurity posture. The organization implements a measurable cybersecurity learning and awareness program to reshape the corporate culture and daily behaviors of their associates needed to protect the organization and its people from a pervasive security breach.
- Establish a dedicated cybersecurity function led by the CISO with skilled cybersecurity staff in place to protect the business sensitive assets, monitor security threats and operations, and be ready to respond to any security incidents. The organization should develop its cybersecurity workforce strategies by assessing workforce needs and skills gaps, recruiting skilled talent for well-defined cybersecurity management roles, providing specialized trainings as needed to further enhance their skillsets and creating a productive, results driven environment to retain talent.
- Establish a cross-functional team of key stakeholders in the cyber program, including IT, 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.
- Perform regular internal phishing tests as an assessment and awareness tool to help employees better identify these attacks when they occur.
- Ensure the organization regularly recognizes key cybersecurity risk behaviors, trends, and cyberthreats to the organization.
- Implement threat, behavior and audience-based, concise learning programs with active user engagement to maximize attention and retention.
- Provide proactive learning and awareness opportunities in the form of frequent, small bites of information while leveraging different delivery channels (such as digital, class room based, etc.).
- 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. Evaluate results of various simulation tests to gauge effectiveness, and incorporate lessons learned into iterative awareness and learning programs.

Remain vigilant in protecting critical IP investments

Protecting intellectual property

IP is often a manufacturer's most valuable asset, requiring constant protection. In addition, the scope of responsibilities for CISOs is expanding, either directly or indirectly, to also include evaluation and management of cyber risks related to ICS and connected products. In fact, CEOs surveyed for a recent study[11] indicate a shift to higher value, advanced manufacturing will fuel their overall competitiveness going forward, and the creation of differentiating IP is critical to this transformation. However, manufacturers find themselves contending with increasingly connected systems, sophisticated spear phishing attacks, mobile device challenges, and state-sponsored attacks, each significantly elevating the risk of IP theft. This issue applies to where IP resides within enterprise networks and business systems, but also to how IP moves through a company's supply chain, including ICS systems, connected products, and third parties.

Manufacturers with a global footprint also have to contend with the never ending challenge to protect their IP. A majority of companies interviewed for this study indicated the problem of protecting IP is most acute in countries like China, Russia, India, and Mexico, where establishing and maintaining robust cyber risk measures to protect against IP theft proves to be complex and difficult. Companies must assess these risks not only in country, but also consider the growing threat of nation state-sponsored attacks on operations in the US.[12]

When evaluating risks related to IP theft, it is important to recognize this risk extends to the following:

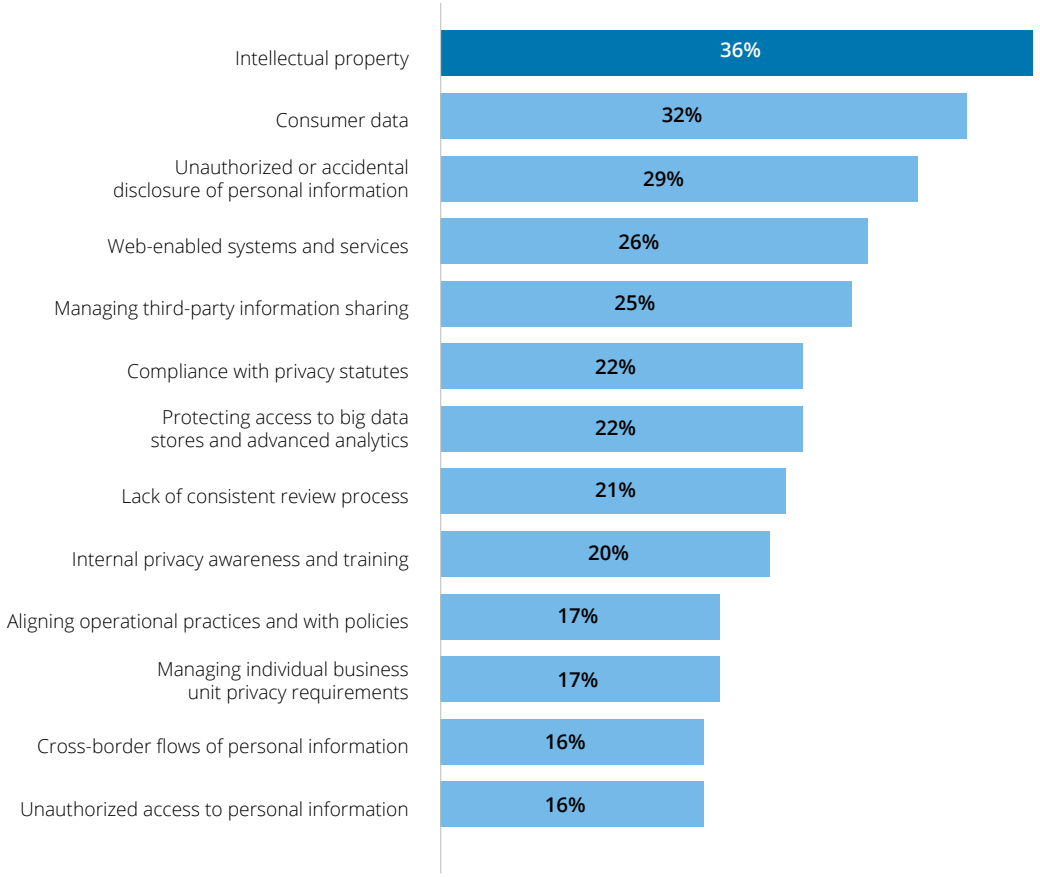
Data at rest

- How to protect large online stores of IP resident in R&D, Engineering, and Manufacturing Operations departments.

Data in motion

- How to protect IP as it moves through the company's supply chain from enterprise business systems to ICS systems.
- How to protect IP as it moves in and out of the organization to third parties through routine processes such as subcontractor bidding processes, offshore manufacturers, and engineering or other service firms.

Figure 12: Top data protection concerns among manufacturers



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

In 2014, for the first time, a US grand jury indicted five Chinese military hackers for a variety of offenses including economic espionage against six manufacturers in the US nuclear power, metals and solar products industries.

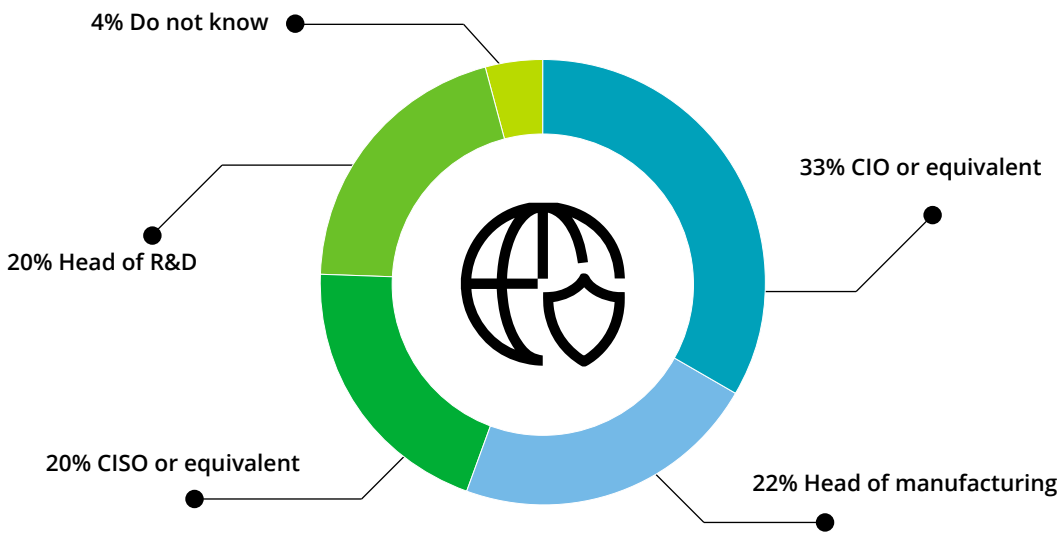
"Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets."[13]

U.S. Attorney General Eric Holder

Who's steering the cyber risk ship?

Protecting IP is a top concern among larger companies surveyed—a fair concern since study respondents cite IP theft among the most frequent reasons behind cyberattacks. Nevertheless, nearly half of manufacturing companies lack confidence that their assets are adequately protected. This should come as a concern to the CIO or CISO, more than half of whom are reported as the person primarily responsible for IP asset protection. There remains a significant portion of manufacturers where the responsibility for IP lies with either the head of manufacturing (22 percent) or the head of R&D (20 percent), signaling a lack of consistency regarding IP responsibility across the manufacturing sector.

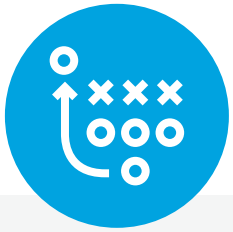
Figure 13: Responsibility for IP protection



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

"We were building a facility in China five years ago, and they acquired local equipment, cameras to show leadership back at headquarters live progress of construction. They put the live feed on the Internet, but did not realize this rendered it/us as a target. It was hacked. It was brutal."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study



Protecting IP playbook

Securing IP is a challenging area, and unfortunately there isn't a silver bullet that can solve this puzzle. History is witness that traditional security measures such as perimeter security are necessary, but not fully effective. A fundamental shift in approach is necessary to apply security controls in a layered fashion considering the risks and threats both external and internal to the organization. This approach should not only consider who might attack from the outside, and what techniques they may employ, but also consider insider threats and techniques that rogue employees or third-party contractors may employ to steal IP.

It is recommended that organizations apply security controls at the data layer itself ("inside out" security model), in addition to other basic capabilities such as perimeter security, vulnerability management, application security, etc. Data protection from the inside out focuses on three important principles: a) inventorying, classifying, and maintaining sensitive data and corresponding assets; b) implementing preventative and detective data protection capabilities at the data layer itself; and c) reducing the value of sensitive data, if and when it's compromised.

- **Inventory, classify, and maintain IP and corresponding assets**—Without knowing what crown jewels a manufacturer owns and where they are located, it is very difficult to apply any security approach to protect the crown jewels. It is extremely important to clearly define what is considered IP from a risk of loss standpoint. 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. Reducing the footprint of IP in the IT environment is a key strategy in protecting such information. Organizations across the industry have implemented tools such as Data Loss Prevention (DLP). The draw back from solely using a tool such as DLP is it is limited to what it knows is sensitive data (by default this would include well formatted information such as social security numbers or credit cards). The leading practice across the industry is to leverage tools such as data classification technology to classify or tag data as containing IP which enables DLP and other such tools to read that tag and understand how it should be protected and with whom it should be shared.
- **Implement IP protection capabilities at the data layer**—Once IP is identified and tagged, 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.
- **Reduce the value of sensitive data to the threat actors**—This is perhaps the most important principle, and it is based upon the premise it is not "if," but "when," someone gets their hands on IP. One way to reduce the value of such sensitive data is to encrypt or obfuscate the data to render it difficult to use when compromised. A second way to reduce the value of sensitive data is to securely destroy it when it is no longer necessary for legitimate legal or business purposes.

Protecting sensitive data is a complex challenge that requires a holistic and comprehensive data protection strategy, executive support, and investment of time, talent, and funding. Implementing individual data-centric solutions in a siloed manner, and without integration, can lead to critical gaps in an organization's security.

Additional strategies companies may employ to protect IP may include:

- global network segmentation strategies
- strong central guidance on IP protection policies and procedures
- continued monitoring for IP related threats
- tailored cyber awareness training of high risk employee groups that frequently handle sensitive IP
- secure sites to share IP as needed for key business processes, such as interaction with key suppliers and subcontractors, as opposed to sending the information out in an uncontrolled manner

Organizations may also need to make some strategic business decisions based on the risk tolerance, considering IP protection risks, when evaluating the types of business activities the organization may or may not be willing to undertake in emerging markets.

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

Inherent risks in industrial control systems

The need to constantly scan automated manufacturing processes for flaws that could open doors for hackers is clear. However, legacy systems, lack of complete inventories of ICS systems and their connectivity, and the need to limit production down time create their own set of risks and exposures.

Starting at the shop floor, IT and OT need to collaborate to strike a balance between managing a company's uptime, productivity and profitability and a company's known critical cyber vulnerabilities. Research conducted for this study has revealed that within the last six to 12 months, IT teams are starting to increase the use of cyberthreat monitoring techniques to detect unusual activity in control systems, with the intention to prevent:

- Loss of significant intellectual property
- Loss of life or other safety issues on the shop floor
- Significant negative environmental impact

In fact, companies at the leading edge of ICS security install real-time, automated 'audit' oversight tools to monitor and signal when systems are operating out of tolerance, so risk of event escalation can be mitigated and/or the system can "fail safer."

On the other end of the scale, almost a third of companies (31 percent) report they have not even performed an ICS specific cyber risk assessment. Among those who did perform this assessment, the majority (63 percent) did not use an independent third party for their assessment.

Integrating ICS into the larger enterprise network

In light of the increasing convergence of physical and digital manufacturing taking place, the need for ICS to be integrated into a company's larger enterprise network strategy has never been more acute. The good news is the importance of having a robust cyber risk strategy is recognized and supported by a majority of manufacturing executives. The more challenging news is securing adequate funding for enterprise cyber risk program remains a significant challenge for 48 percent of manufacturing companies.

Addressing the issue of legacy systems

Embedding cyber solutions within existing operational technology is a very challenging task, often prompting a reluctance to implement initiatives designed to improve the security posture of shop floor systems. This is due to either a fear of production disruption or an aversion to the large price tag generally associated with upgrade projects—or both. It should be noted that systems and networks used in industrial automation are designed to remain in production for much longer than enterprise business systems, and depending on how long they have been in service, may not have been designed or implemented with cyber risk in mind. Ironically, the information flowing through these antiquated ICS have, up until now, been somewhat protected by accident where the variety of dense data streams have historically been difficult for a hacker to understand and/or make use of in a malicious incursion scenario. It is only a matter of time before a determined hacker is able to unravel these data streams.

Still, many manufacturers find themselves in a precarious position of having outdated assets controlling integral parts of their manufacturing operations. Over time, these assets may represent more and more liability from a cyber risk perspective, and should be carefully weighed against the cost of bringing control systems up to modern standards. These issues are often exacerbated by frequent merger and acquisition (M&A) activities where acquired assets often bring their own problems in terms of legacy systems and hidden vulnerabilities. Cyber assessment is often left out of sensitive due diligence activities, but manufacturers would be well-served to include it in order to mitigate risk and properly assess potentially sizable infrastructure costs.

> The number of investigations carried out by the US Department of Homeland Security on cyberattacks against critical manufacturers doubled in fiscal year 2015 compared to the previous year, intensifying the need to double-down on efforts to find and fix cyber ICS vulnerabilities.[14]

For companies that take the next step to actually test whether their ICS systems are actually air-gapped, they frequently detect unauthorized connection points, which subject ICS systems (and their associated critical manufacturing processes) to direct attacks as well as indirect cyber risks such as malware that may have just as significant an impact.

According to survey respondents, electronic and physical access to critical cyber assets are also not well-managed. The process of updating anti-virus software, patching or changing configuration files on legacy systems in fragmented OT environments remains a significant challenge. Similarly, network segregation and remote access are big challenges for manufacturers. For example, networks should be segregated based on criteria such as:

- Sensitivity of data
- The business purpose
- Business intelligence requirements
- End-to-end supply and demand process management
- Integration with ERP systems
- Internet access requirements

Acknowledging the air-gap fallacy

History shows even facilities that are thought to be fully "air-gapped" (i.e., ICS or plants that are prevented from connecting to an enterprise network, third parties, or the Internet by means of a physical or logical barrier) can fall victim to cyberattack through either the use of portable storage media, wireless access points, or low-priority systems (e.g., heating, ventilation and air conditioning) that have been overlooked and are actually connected to the outside world.

Air-gapping a production facility can also subject a manufacturer to an unintended drop in productivity as barriers to the free-flow of critical information are deliberately erected. This situation often results in manufacturers becoming more susceptible to competitive threats over the longer term. As the manufacturing sector moves closer to an "Industry 4.0" paradigm, where an ever increasing number of devices involved in the production process are connected to each other and the outside world, manufacturers that are resistant to the inevitability of this digital transformation risk being left behind.

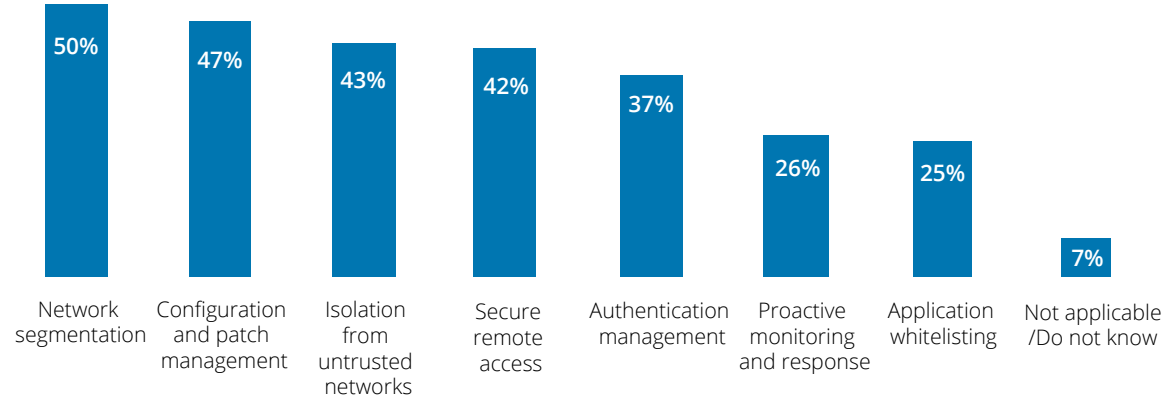
There are also clear cost advantages in upgrading to new shop floor systems that are much easier to understand and are much more standardized. It is interesting to note while there may be a strong desire to leave legacy systems alone for fear something will break, the risk of component failure also grows over time. In fact, the longer these systems are left untouched, the greater the risk a component will fail, and a replacement part will be harder to find, thus introducing a significant business continuity concern. Many manufacturers with successful implementation stories approach legacy systems with a risk-based methodology where the response to an issue is based on the level of risk that each component in the ICS environment represents. It is important to involve engineers or manufacturing operations employees in this exercise to appropriately identify and articulate the risks and associated business impact.

Manufacturers have also reported success in testing upgrades to their ICS in controlled lab environments as a way to contain exposures while limiting the risk of production disruption. Once the upgrade has proven successful in the test environment, it can be efficiently implemented in production during routine scheduled downtime.

Figure 14: Assessment of ICS cyber risks

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

Figure 15: Solutions for ICS connectivity



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

Security vs. production: finding harmony between the left and right hands

The issue of balancing the need for cybersecurity against the need to maintain operational efficiency is often viewed as an "either/or" dilemma, but it needs to be embraced pragmatically by top executives and proposed as a unified vision spanning the entire enterprise. In a manufacturing sector characterized by hyper competition, shrinking margins, supply chain interdependencies, two-way data streams entering the shop floor, and embedded but unmanaged endpoints, senior management should recognize the importance of collaboration and transparency across departments and functions.

To be sure, IoT and connected systems can offer significant benefit to manufacturers (and some are certainly headed in this direction), but most companies interviewed are still very cautious when they consider the fact that improving the flow of data and information might mean giving suppliers remote access to machinery on the shop floor (even though by doing so, manufacturers might extend the operating life of critical machinery, etc.). However, regardless of the intended benefit, adding new access points to critical machinery on the shop floor represents a new level of risk. Suppliers that are granted such access must, themselves, be monitored and offer clear policies and processes that protect the systems to which they connect.

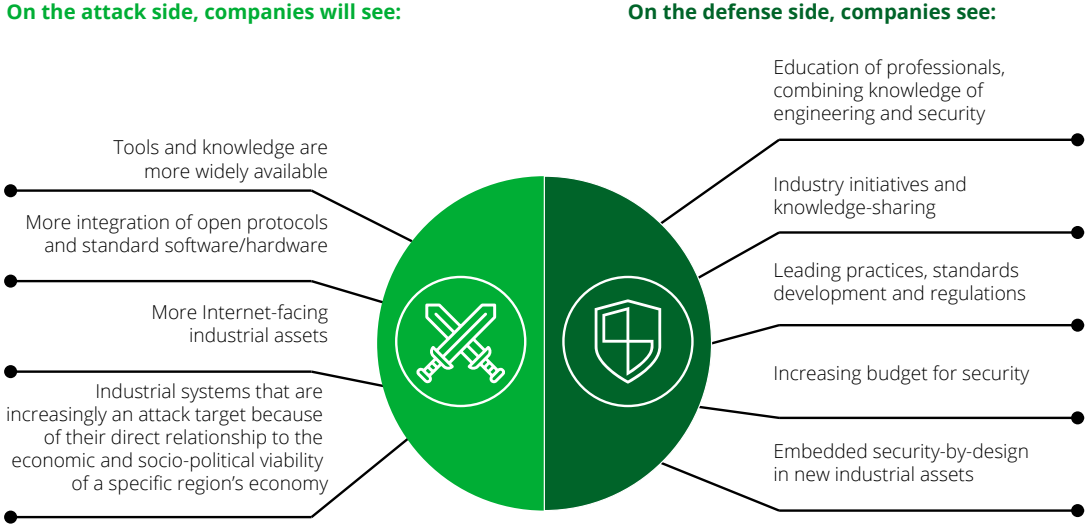
Left and right hands meet – now what?

Automation will play an increasingly important role in the manufacturing space. Nevertheless, 30 percent of surveyed companies do not have an automated tool in their network to secure remote access to their ICS network. In more than 10 percent of companies, the remote access tool is not configured to allow for interactive user access or implementation of strong passwords. This lack of foresight only amplifies the security concerns of an enterprise, particularly as ICS become more intelligent and more autonomous. These systems and other control systems such as building automation, car systems, and medical devices that were once disconnected from networks, are now becoming part of a networked society. Future developments will bring greater risks, and more potential tools to guard against adversaries.

"Bad guys can pull up in the parking lot and cause a lot of problems."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

Figure 16: Attack vs. defense



Source: Deloitte: Cyber Risk & Resilience: Secure.Vigilant.Resilient.™ | May 2015

ICS playbook

- The first step in understanding risks at the shop floor and engineering levels is creating a holistic inventory of all connected devices including ICS that are attached to those network segments. This can be accomplished through a combination of passive scanning and physical observations. Forms of active scanning are not recommended as this can cause operational issues including production downtime resulting from the instability of the aging technologies supporting many ICS coupled with their intricate designs.
- A cross-functional security team should be formed, including, but not limited to representatives from global information security, engineering, and operations. The control system vendor should also be included as appropriate. 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, and improves overall visibility into the decision making process across departments.
- When securing ICS, organizations should consider how the technologies are used within the production processes and the systems the ICS is sending information to or receiving from (one-way communication or two-way communication). ICS are often designed to operate for 10+ years, which differs significantly from the expected lifecycle of other IT systems. As a result, ICS often cannot always be patched and/or are running on technologies including operating systems that are no longer supported by a vendor. Organizations should determine the appropriate response to reduce the risk of these technologies being connected to their networks including:

  1. Removing the connection completely if direct communication is not needed;
  2. Leveraging next generation firewall capabilities such as application control, identity awareness and ICS protocol specific capabilities;
  3. Whitelisting (i.e., establishing a list of applications that have been granted permission to operate on the network)[15] the ICS to prevent unauthorized programs from running;
  4. Porting the ICS to a more stable and secure technology that can be patched when security vulnerabilities are identified;
  5. Containerizing/virtualizing (i.e., encapsulating an application in a container with its own operating environment)[16] obsolete or unsupported technologies, and
  6. Replacing the existing ICS entirely, which will often be the most expensive option and is not always required.

- While "defense in depth" is an important consideration with relation to ICS, trends in the manufacturing space are moving toward 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, which in turn decreases the risk of significant production downtime, impacts to production quality (i.e., corporate espionage), loss of IP and/or safety events.
- IT security policies and trainings have not traditionally considered ICS security, development, operations and ongoing support. Security policies, procedures, training, and educational material that apply specifically to ICS and other connected devices, should be developed and disseminated to those employees within the organization who are responsible for ongoing support or using these technologies as a component of their job responsibilities.
- It is important to also evaluate the scope of other enterprise efforts, such as cyberthreat monitoring and wargaming simulations / resiliency exercises to determine whether they are comprehensive enough to cover top ICS cyber risks.

Design cyber risk management mechanisms into connected products before deployment

Implications of rapidly evolving connected products

For an advanced manufacturing business to remain competitive, understanding and investing in connected devices—and the systems that protect them—is critical. In fact, recent study results indicate smart, connected products are the second most important advanced manufacturing technology for creating and maintaining competitiveness, as ranked by US and European manufacturing executives.[17] Nevertheless, as various technologies mature, merge and evolve, so too do their associated risks associated. As a result, manufacturers should take special care to ensure their connected products are not put at risk.

To understand the cyber risk implications of rapidly evolving connected products, manufacturers should:

1. Bifurcate risks related to connected product data collection vs. remote control
2. Engage cyber talent in key innovation initiatives to make sure the company is building in cyber risk management strategies up front
3. Engage the legal team around ownership of connected product data, responsibilities for product breach incidents, and customer responsibilities topics
4. Evaluate whether "fail safe" techniques have been implemented to detect anomalous product functioning, and remediate or shut down gently to keep products and their users safe

As manufacturers are led by market forces, the quest for competitive advantage, and the relentless pursuit of emerging digital technologies and features, they need to take stock of the implications and risks of prolific connectivity.

Connectivity can mean vulnerability

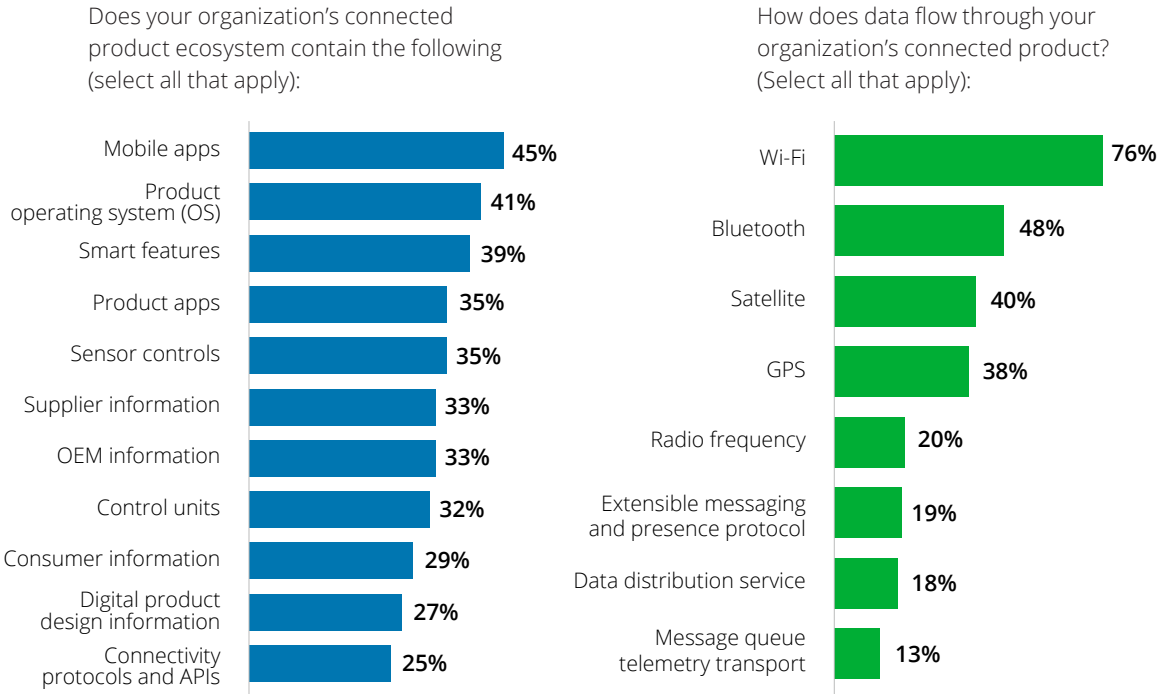
According to Deloitte's latest analysis, nearly half of all companies report the presence of mobile apps for their connected products, and more than three-quarters of companies report their connected product data flow is facilitated by Wi-Fi. This wireless gateway to free-flowing information has proliferated quickly and, though it represents advancements in product capability and increases in service effectiveness, it may also present an unprecedented vulnerability.

"We make controls that go into big equipment [but] if there is no customer need for connection why give it to them? Disable the Wi-Fi so as not to allow exposure. We just need to think of security exposure. If you don't need it, don't include it."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

The IoT market is expected to grow from an estimated $1,928 billion in 2013 to $7,065 billion in 2020.[18]

Figure 17: Mobile and Wi-Fi connectivity



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

This vulnerability is particularly concerning when one considers that:

- Seven in 10 companies store or transmit private information like "unique identifiers" in their connected products.
- Only 55 percent of those are encrypting such data captured from connected products.
- From a risk perspective, one in four companies do not have legal protections in place to cover their organization's responsibility for risk and ownership of product data and transfer (if this has not been legally defined, it can prove especially difficult to determine accountability in the event of a breach or significant cyber-related product issue).

Such vulnerabilities, both systemic and procedural, represent risk to the overall enterprise that, in many cases, can be managed by adopting a secure, vigilant, and resilient approach.

Avoiding the disconnect between production and protection

There is certainly no shortage of hyperbole when discussing the scale and exponential proliferation of networked devices the world is currently experiencing. Many product engineering, development and marketing departments are laser-focused on developing the best connected products, and producing them faster and more efficiently than their competitors. For instance, IoT technologies are all about developing products that rely on embedded sensors and network connectivity to create, share, and act on that information. As a result, cyber leaders should be ever-present during development of these products to assess potential vulnerabilities and offer considerations so risks may be effectively managed before downstream efforts are impacted. Further, it is critical that security assessments be regularly conducted, with particular focus on newly introduced technologies and processes.

"...Our customers may not be asking for sensors in products; from our products; but we may feel the need to make our products capable of being connected even if not needed, but because our competitors are going there."

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

Rapidly evolving connected products playbook

- Assess the 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. The value add must outweigh the cost burden to secure these features, otherwise security appetite may fall short of the standard required.
- 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.
- Consider 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 often times 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.
- Remember previous data protection hygiene still applies to the new age of connected products. A significant portion of the information collected by products today is deemed private and/or confidential. Data must be protected upon collection, while in transit, and in storage on both the device and the data store. Additionally, privacy and data use policies, including cross-border transfer, should be updated to reflect the new age of 24/7 data collection in homes, on roads, on persons, and otherwise.
- It is important to also evaluate the scope of other enterprise efforts, such as cyberthreat monitoring and wargaming simulations / resiliency exercises to determine whether they are comprehensive enough to cover top cyber risks related to connected products.

Identify and address emerging cyber risks in the industrial ecosystem

Cyber risk in the industrial ecosystem

In much the same way as a healthy body requires having healthy functioning vital organs, blood stream and cardio-vascular system, so too does a manufacturing company need to ensure its cyber program develops and evolves inside a broader industrial ecosystem—with all its broader aspects and components functioning in unison.

This conceptual approach takes on even more meaning when considering: (1) the digital transformation taking place across the manufacturing sector, (2) the mass "sensorization" of the manufacturing process and the products being generated, and (3) the pace of innovation required to maintain a company's core competitiveness. Indeed, innovation and risk go hand in hand and that amount of risk gets multiplied when cyberthreats can arise from a wide variety of origin points along the company's external value chain.

Keeping the industrial ecosystem healthy

Given the interconnectedness of the modern industrial ecosystem, it stands to reason one might take the "inoculation" metaphor further—treating the entire value chain as a living entity in need of constant care. As such, businesses not only need to consider their own internal cyber risk posture, but also their suppliers, outsourcers, service providers, vendors, partners and customers (referred to as 'third party') as well.

Indeed, today's ever-changing business environment can be characterized by increasing expectations of cyber preparedness from suppliers, customers and regulators. It is also accompanied by new cyber standards and requirements being placed on suppliers. This is particularly true for manufacturing, with new technologies and processes constantly being applied to the industry, from R&D, to operations, to distribution. As enterprise security becomes more and more of a hot topic from the boardroom down, higher expectations are being put on manufacturers to keep on top of the changing threat landscape.

Cyber risk in the industrial ecosystem playbook

- Most organizations are mandating consistent third-party governance standards amidst increasing decentralizations of operating units.
- Define requirements for third-party cyber risk management up front in key contracts. Make sure there is a right to audit against those requirements.
- Increasing monitoring and assurance activity over third parties is believed 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.
- Visits to third-party locations are considered the most effective method to gain assurance over third-party management.
- The drivers for third-party engagement are progressively shifting from a focus on cost to a focus on value, reflecting organizational recognition of the strategic opportunity that third parties can create for them.

As many departments are involved with their company's industrial ecosystem like IT, Security, and Procurement, it is important they effectively communicate and collaborate on a regular basis. For cyber risk matters, Security should take the lead related to its third party's security aspects, especially if those third parties access the company's network, systems or data. Additionally, Procurement should ensure cybersecurity requirements are fulfilled by third parties early in the third-party management lifecycle as they are brought into the company's industrial ecosystem. When breaches occur, the sharing of information between relevant companies operating within an industrial ecosystem can help eliminate silos and make the invisible threats not only visible, but also manageable, thus reducing future risk across the entire value chain.

Since 2011, The US Department for Homeland Security (DHS) has called for a more collaborative application of cybersecurity to include a broad spectrum of companies working together as an ecosystem. "Rather than focus on the security of individual organizations, the proposed idea was that we should work as a community to address threats as they arose. By inoculating the community to these threats, we would only have to suffer the disease once before we all grew stronger." – Davis Hake, Palo Alto Networks[19]

The changing nature of the cyberthreat landscape

There is no doubt the number, sophistication, and severity of cyberthreats is increasing in the manufacturing sector.

IP theft is the biggest cyber concern, but IP is often dispersed throughout the business, attracting the skills and resources of foreign state-sponsored actors to penetrate, locate, and extract the intellectual assets. A recognition that external, global attackers are very real and they are specifically targeting manufacturing IP would be a good first step (but not sufficient) for companies that have traditionally believed this will not affect them.

The truth is every manufacturer is at risk.

Spear-phishing methods are now among the most prevalent forms of cyberattack and are often motivated either by a desire to expose and target high-net-worth individuals (i.e., senior company executives), and/or those in the organization who can authorize significant monetary transactions (e.g., fraudulent notifications using trusted company executives' emails instructing customers to make changes in bank account remittance). In some cases, cyberattacks are not even specifically targeted, as employees often unwittingly download malicious "malware" that can impact functionality or "ransomware" that holds company data hostage until the hacker's demands are met. Spear-phishing is also used as a frequent entry point for the IP theft as well.

In other cases, seemingly benign systems can be hacked and used for alternate purposes. For example, a manufacturing company was expanding its global footprint by constructing a production facility in China. In order to keep an eye on the construction progress, the company installed a series of cameras they could control from a remote location. However, it was discovered these connected cameras had been hacked, and the images were being used to covertly monitor the facility.

Cyber risk in the manufacturing space is not just a concern for information or financial theft, as there is a large and growing concern for personal safety. Hacked systems on the shop floor could be manipulated to cause a number of catastrophic events. To date, the most high-profile example of this type of incursion is the steel mill in Germany where hackers effectively disabled the fail-safe governing one of the plant's blast furnaces, causing wide-spread damage and endangering the lives of plant workers. To be sure, there is all manner of connected machinery involved in the manufacturing process that could be used to disrupt the flow of production, affect the safety of company employees, alter a product's specifications, or change quality testing tolerances, creating a risk to the end consumer. There are also potential environmental risks or threats to IP as well.

Another way in which cyber-risk is changing at an accelerated rate is through the adoption of cloud computing. Even as some manufacturers look to leverage the efficiency and scale of cloud computing, many executives question how they can be assured that these service providers are keeping up with necessary system upgrades and security patches necessary to keep individual company data safe and secure. Nevertheless, smaller companies could actually realize some benefit from moving their data to the cloud as they may not have access to modern security tools otherwise. This will increase the need to engage service providers in a coordinated dialogue on management and monitoring of key cyber risks, focused on the needs and unique issues of the manufacturing sector. Effective third-party risk management standards and monitoring are key to managing this risk.

Study results indicate 40 percent of companies were affected by cyber incidents in the past 12 months. In terms of monetary impact, 36 percent of these incidents resulted in damages of $1 million or less. Having said that, 38 percent of identified cyber breaches resulted in damages in excess of $1 million. It is also interesting to note 13 percent of cyberattacks resulted in no financial damage and a further 13 percent of incidents are either not quantified or not tracked in terms of potential financial impact to the company. These statistics are likely to represent the hard dollar costs associated with a breach, but not fully representative of other indirect costs.[20]

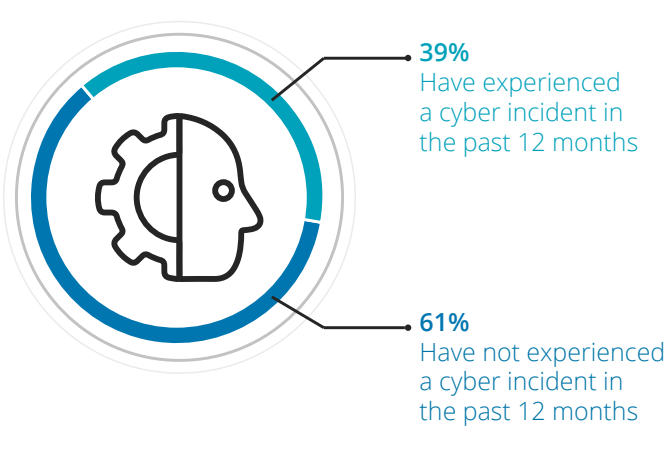
"We think like the bad guys and use the tools that the bad guys use to help us plan and implement changes."

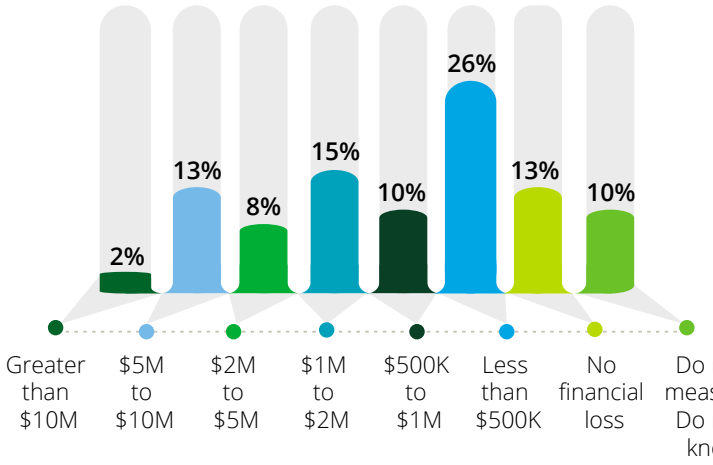
Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

"How can I be sure that the cloud providers are keeping up with the vulnerabilities in their environments?"

Executive interviewee,
Deloitte and MAPI
Cyber risk in advanced manufacturing study

Figure 18: Number of cyber incidents and damages





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

Conclusion

Although there is a tremendous amount of product and process innovation occurring in the manufacturing sector as digital and physical paradigms continue to evolve, there is also much variability among cyber risk approaches which leaves individual companies vulnerable to attack and loss of critical data. Manufacturers face a plethora of challenges as they strive to get a handle on complex issues such as upgrading legacy ICS while maintaining production output levels to more fundamental human capital concerns such as the scarcity of critical talent.

Cyber risk is also climbing ever higher on the list of priorities for senior executives and company boards. Nevertheless, establishing effective cyber strategies remains challenging as many boards still do not have enough information about the company's cyber profile, initiatives, and/or specific vulnerabilities to raise the right questions.

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.

A few thoughts on where to begin:

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

It is our hope that the detail in this study will provide a new opportunity to engage in a deeper dialog around core aspects of your company's cyber risk program, identify continuous improvement opportunities, and establish a road map for your company to become secure, vigilant, and resilient.

Endnotes

[1] Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, *2016 Global Manufacturing Competitiveness Index Study*, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-gmci.pdf.

[2] Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, *Advanced Technologies Initiative: Manufacturing & Innovation*, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-indprod-deloitte-and-council-on-competitiveness-advanced-tech-report.pdf.

[3] Ibid.

[4] Articulating Cybergovernance, NACD Directorship, September/October 2016.

[5] https://www.congress.gov/bill/114th-congress/senate-bill/2410/text.

[6] Irfan Saif, Sean Peasley, and Arun Perinkolam, *"Safeguarding the Internet of Things: Being secure, Vigilant and Resilient in the Connected Age," Deloitte Review 17, Deloitte University Press, July 27, 2015*, http://dupress.deloitte.com/content/dam/dup-us-en/articles/internet-of-things-data-security-and-privacy/DUP1158_DR17_SafeguardingtheInternetofThings.pdf.

[7] Deloitte LLP and MAPI, *Understanding Risk Assessment Practices at Manufacturing Companies, 2015*, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-mfg-mapi-risk-assessment-paper-single-page-040715.pdf.

[8] Deloitte Advisory, *Assessing Cyber Risk: Critical Questions for the Board and C-suite*, 2016, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-assessing-cyber-risk.pdf.

[97] Ibid.

[10] Deloitte LLP and The Manufacturing Institute, *The Skills Gap in US Manufacturing: 2015 and Beyond*, 2015, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-pip-the-manufacturing-institute-and-deloitte-skills-gap-in-manufacturing-study.pdf.

[11] Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, *2016 Global Manufacturing Competitiveness Index Study,* http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-gmci.pdf.

[12] The National Bureau of Asian Research, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, May 2013.

[13] Source: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[14] Source: The Hill, *DHS: Cyberattacks on critical manufacturing doubled in 2015*, January 15, 2016.

[15] Source: http://searchsecurity.techtarget.com/definition/application-whitelisting.

[16] Source: http://www.webopedia.com/TERM/C/containerization.html.

[17] Deloitte Touche Tohmatsu Limited and US Council on Competitiveness, *2016 Global Manufacturing Competitiveness Index Study*, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-gmci.pdf.

[18] IDC market in a minute: Internet of Things, IDC, http://www.idc.com/downloads/idc_market_in_a_minute_iot_ infographic.pdf.

[19] Source: http://researchcenter.paloaltonetworks.com/2015/06/where-is-our-cybersecurity-ecosystem-today/.

[20] Deloitte Advisory, *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts*, 2016, http://www2.deloitte.com/us/beneath-the-surface-of-a-cyberattack.

Methodology

To assess cyber risk in advanced manufacturing trends, Forbes Insights, on behalf of Deloitte and MAPI, conducted a survey of 225 cyber risk executives at leading manufacturing firms who responded to a proprietary online survey. Respondents represented a diverse collection of companies from a variety of manufacturing sectors, including: industrial equipment, computer hardware, electronics, automation technology, and consumer appliances among others. The online survey effort was bolstered by a series of 35 executive interviews where participants provided a broad point of view on how manufacturing companies are confronting and discussing cyber risk issues.

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

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*.

Deloitte.

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.