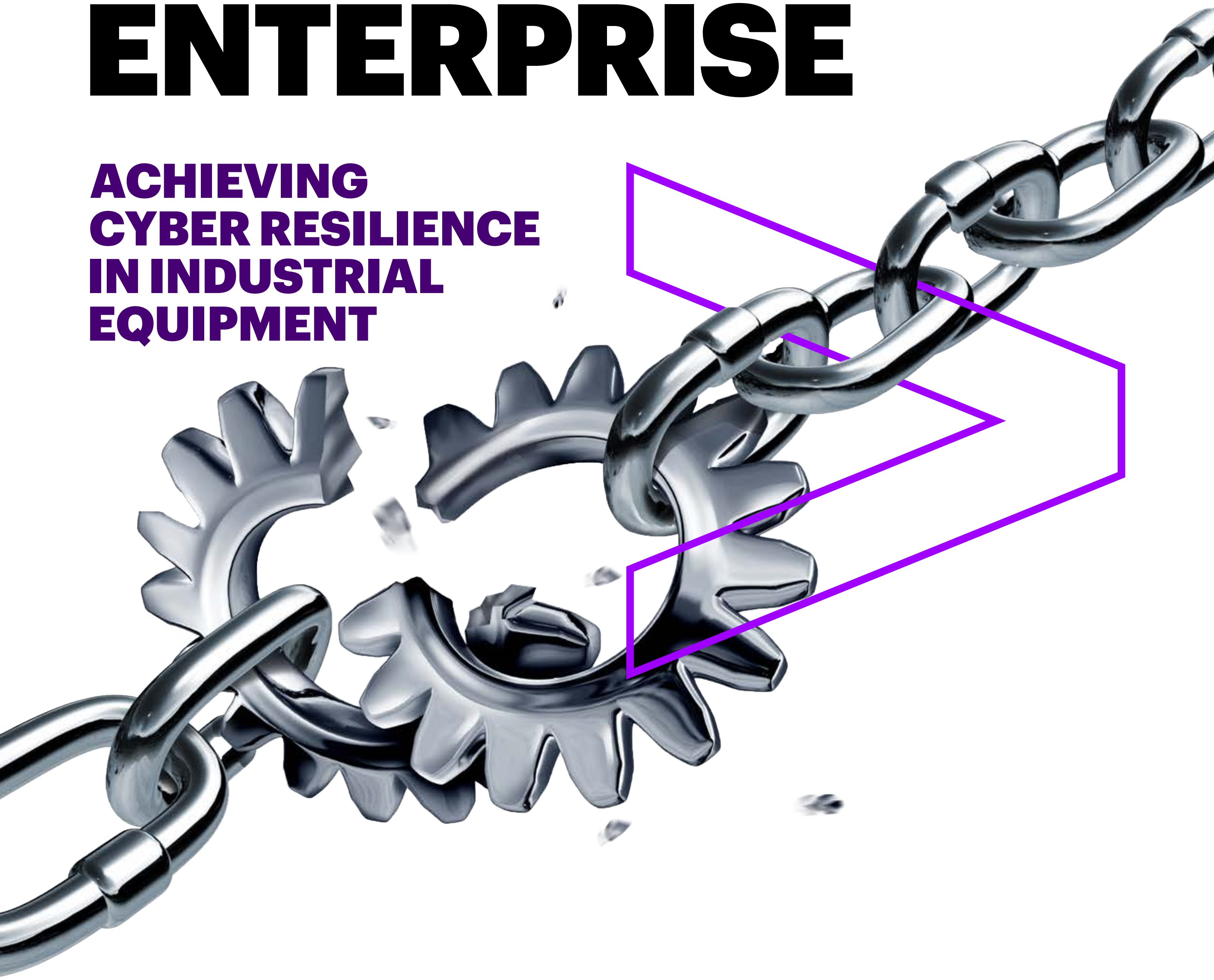
accentureconsulting

SECURING THE INDUSTRIAL ENTERPRISE

ACHIEVING CYBER RESILIENCE IN INDUSTRIAL EQUIPMENT



Confident in connectivity

Being connected is the new normal. Whether influencing people personally or professionally, connected devices mean that it is easier to know what is happening operationally and in real time. But those open channels also invite risk from nontraditional sources. Across all industries, the number of targeted cyberattacks has doubled in a year and threats are becoming more sophisticated and disruptive. And when asked what percentage of their organizations are actively protected by their cybersecurity programs, industrial equipment executives said just two-thirds (66 percent)—leaving one-third of the organization highly vulnerable. Indeed, 80 percent said that as their companies adopt innovative business models, ecosystems and liquid workforces—the lifeblood of connected economies—the risk and security attack surface increases exponentially.

But while one-fifth of our respondents in our research lack confidence in their ability to secure connected devices or Internet of Things (IoT) devices as they are deployed, the issues are accelerating. Research shows that the global Internet of Things market is expected to reach US$600 billion by 2022[1]—opening up fresh avenues of risk.

Yet, there is also an opportunity risk at stake here. Over the next five years, companies in the private sector risk losing an estimated US$5.2 trillion in value creation opportunities from the digital economy to cybersecurity attacks.[2]

Counteracting connectivity threats may require wholesale change—from handling hyper-connectivity, to managing fundamental security practices, and to the security officer's role—but it can also open the door to a new security paradigm that improves how industrial equipment organizations operate.

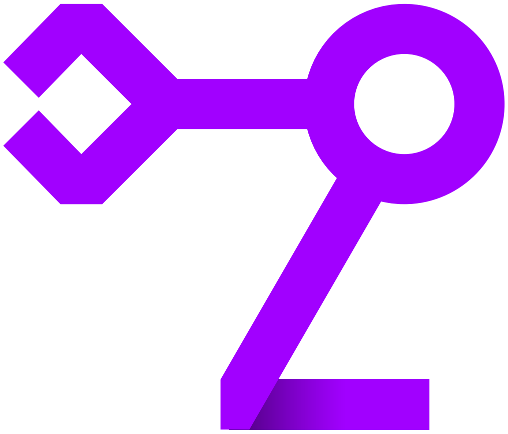
8 in 10

industrial equipment executives are confident about their cybersecurity capabilities; yet out of

33

cybersecurity capabilities, industrial equipment is high-performing in just

19



Spread the risk

Industrial equipment companies, the products they create, and the ecosystems in which they operate are becoming more connected by the day. Even their traditional factories, which may not have embraced the cloud yet, are more vulnerable to security risks due to missing basic security hygiene. Greater connectivity provides an opportunity for industrial equipment manufacturers to improve their service levels, be more responsive to the distribution network and their customers, and create new business value through data-driven services.

74% **of industrial equipment executives said that "cyberattacks are a bit of a black box, we do not quite know how or when they will affect our organization."**

Three steps are important for industrial equipment companies that want to achieve cyber resilience:

Protect the core assets

Make hyper-connectivity a security opportunity

CISOs must become a business enabler

Protect the core assets

Chief Information Security Officers (CISOs) need to be brilliant at the basics, by identifying, hardening and protecting their core assets and pressure testing resilience, if they are to gain the visibility they need across their operations. Industrial equipment manufacturers must consider the upstream elements (creating products and managing suppliers and the ecosystem) and downstream elements (such as managing distribution networks and servicing customers), for all relevant processes, products and related services.

Nearly half of industrial equipment executives recognize they need to improve on the "basics" of cybersecurity, such as security monitoring and network security. The definition of what good looks like has evolved over time as technologies have improved, attack impacts have risen and as threat actors have increased their capabilities and their savviness.

Industrial executives should ask themselves whether they have a comprehensive list of security capabilities and controls. They need to establish a product security incident response team (PSIRT). They should consider whether their manufacturing and connected products adheres to applicable regulation or industry standards. They need to ensure networks are properly segmented to protect critical operations, prioritizing implementation based on business purpose. And they need to question whether advanced security monitoring is being applied at the lowest levels of the architecture.

A majority of industrial equipment executives (83 percent) are putting their faith in new technologies such as artificial intelligence (AI), machine/deep learning, and blockchain, saying that they are essential to secure the future. Although there is little doubt that breakthrough technologies should be adopted in parallel to drive the next round of cyber resilience, this should not come at the expense of practicing the fundamentals.

46%

of industrial equipment executives recognize they need to improve on network security and

44%

on security monitoring—the "basics" of security programs.

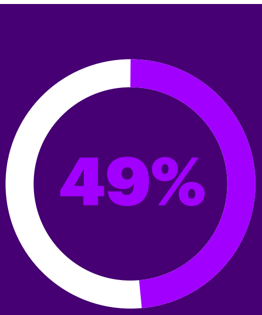
Make hyper-connectivity a security opportunity

Smarter products and connectivity bring value to distribution networks and the customers they serve—from condition monitoring to vehicle tracking to remote service or data analysis. But these benefits, if not well engineered, deployed, managed and monitored, can also lead to new risk. Cybersecurity is often seen as a "bolt-on" function—the result of an afterthought in the development process—rather than a core, upfront, integral and "built-in" input to the product development process, like a "security by design" principle.

Even customers are choosing hacking as a means to keep their equipment operational—farmers have resorted to using software from other countries to repair their equipment after manufacturers made it impossible to perform "unauthorized" repairs. With many farmers living some distance from a dealership and unwilling to absorb the cost of equipment lock down, they are faced with a stark choice—one that could affect the manufacturer and its entire ecosystem in the longer term.[3]

But the implications of connectedness are only likely to escalate in the future. New technologies and the use of the Internet of Things (IoT) or Industrial Internet of Things (IIoT) introduce a new hyper-connectivity that means the scale of security risk has also shifted. Overnight, the attack surface has tripled—not just products or systems, but a system of systems, involving inputs, outputs and communication networks. The hyper-connectivity of consumer devices and ecosystems to orchestrate faster and more meaningful work can ease the path to better, faster, more resilient products while introducing a data avalanche that also needs to be managed.

The situation seems to be worsening, with the number of cyberattacks rising year over year—industrial equipment companies, on average, experienced 177 security attacks in the last year, of which 17 percent succeeded in breaching defenses. Further, threat actors seem to be evolving the very nature of these attacks. Techniques such as ransomware-as-a-service and DDoS-for-hire combined with complex products (that incorporate many embedded, connected systems or systems of systems) accelerate risk to everyone, including those outside of the natural ecosystem. In addition, nation states are conducting targeted attacks to steal intellectual property or simply to disrupt. Recent research indicates that the number of these nation-state-sponsored cyberattacks has grown, and this is likely to continue.[4]



of industrial equipment executives intend to increase investments in monitoring and securing operational technology and manufacturing environments from cyberattack over the next two years.

We found industrial equipment executives are confident about their cybersecurity effectiveness and capabilities, but they are only high-performing in around half (19 out of 33 cybersecurity capabilities). With just 66 percent of industrial equipment executives saying that their organizations are actively protected by their cybersecurity program, and faced with greater connectivity, they need to think carefully about how such a program covers manufacturing, distribution and beyond.

Adopting a holistic approach makes their defenses more robust, helps them to take advantage of data for economic reward and enables their organizations to rotate to the new. Industrial equipment companies embedding a product security program can address gaps in product lifecycles end-to-end, starting with security requirements, to incorporate secure development lifecycle (SDL) practices into product design, build, operate and maintain elements through end-of-life.

CISOs must become a business enabler

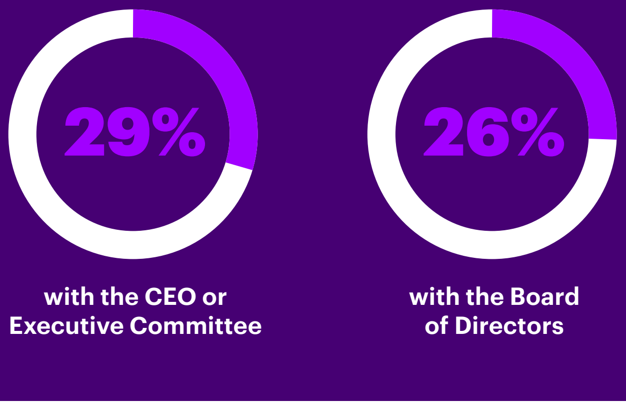
Security behaviors and roles must evolve. In this new world, it is not just about the CISO being technically competent. Traditionally, many CISOs have acted in a siloed manner, with a narrow focus on information security (with "information" being the key word) rather than the full digital value chain. In doing so, their organizations are not adequately protecting the business risks to their operations, including those of their own brand or intellectual property.

The next-generation CISO needs to be business savvy—going beyond information security, aligning with the business, and leading the business in terms of cyber-risk-associated technology, ecosystems and the overall operating environment. CISOs must be agile, support business objectives, and understand the broader scope of security—including connected products, smart services, and supplier and distribution ecosystems—to demonstrate the art of the possible to the CTO or CIO.

To take ownership of risk throughout the organization, CISOs must understand and safeguard the business ecosystem in which they operate—and if they do not adapt, other roles will fill the gap. Consider two new roles in industrial equipment organizations, the Chief Products Officer (CPO) and the Chief Operational Security Officer (COSO). CPOs are operating at the highest levels in the organization, often creating a bridge between the CISO and the Board so that the organization can build business-enabled security. COSOs are on the same level as the CISO, taking the business lead for operation technology (OT) security. Their work is to enable cyber resilient operational environments and to build bridges between IT and OT infrastructure.

Our research "Gaining ground on the attacker: 2018 State of Cyber Resilience" found that cybersecurity budgets often rest at the top, so speaking to C-level peers in their own language can make a huge difference to the impact and success of the security function.

Cybersecurity budgets rest at the highest levels of the industrial equipment organization.



Seize the day

Industrial equipment executives need not feel daunted. They can achieve cyber resilience by taking the following three actions:

01

Secure core assets

CISOs must prioritize establishing visibility into the network. Focus on the fundamentals. Regularly harden and protect core assets and pressure-test resilience. Bring new realism to your testing with coached incident simulation with a technique known as Purple Teaming—a combination of Red Team adversarial actions with real-time Blue Team dynamics. Above all, make sure that cybersecurity basics are baked in to the fabric of the organization.

02

Establish a security-by-design culture

Security must be practical and keep pace with the changing nature of connected environments. Develop a more proactive security posture that is fully operational from the outset. Understand the value chain upstream and downstream environment where your assets are connected to better manage hostile behaviors.

03

Evolve the CISO role

As well as being tech-savvy, next-generation CISOs should be business-minded and adept at communicating effectively across all levels of the business. Take the lead as a champion of the broader business ecosystem, not just a protector of information.

20% of industrial equipment executives lack confidence that their organizations can protect connected devices/Internet of Things devices as they are deployed in factories, warehouses, or equipment.

Manufacturing change

At both ends of the spectrum—from an individual employee's perspective, all the way up to strategic corporate decision making—cybersecurity represents an opportunity to improve and enhance the business. Industrial equipment executives have a window of opportunity in the next couple of years to succeed where others have failed—by employing cyber resilience to make their business bigger, faster and stronger and meet the threats of today, while planning to counteract the threats of tomorrow.

Authors

Tilak Mitra
Managing Director
Industrial Equipment Technology Lead
tilak.mitra@accenture.com

Bradford Hegrat
Principal Director
Security Consulting
bradford.hegrat@accenture.com

Wayne Dennis
Senior Manager
Security Consulting
wayne.dennis@accenture.com

Stay Connected

@AccentureConsult
@AccentureInd

/showcase/accenture-industrial
/showcase/accentureconsulting

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks. Information regarding third-party products, services and organizations was obtained from publicly available sources, and Accenture cannot confirm the accuracy or reliability of such sources or information. Its inclusion does not imply an endorsement by or of any third party. The views and opinions in this article should not be viewed as professional advice with respect to your business.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at **www.accenture.com**.

Note

Unless otherwise stated, the statistics in this point of view represent industrial equipment respondents in the survey report "Gaining ground on the attacker: 2018 State of Cyber Resilience," Accenture 2018.

References

[1] Internet of Things Technology Markets, Global Forecast to 2022, Markets and Markets. https://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html

[2] Securing the Digital Economy, Accenture. https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf

[3] Why American Farmers Are Hacking Their Tractors with Ukrainian Firmware, Motherboard, March 21, 2017. https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

[4] Cyber Threatscape Report 2018, Midyear cybersecurity risk review, Accenture. https://www.accenture.com/us-en/insights/security/cyber-threatscape-report-2018