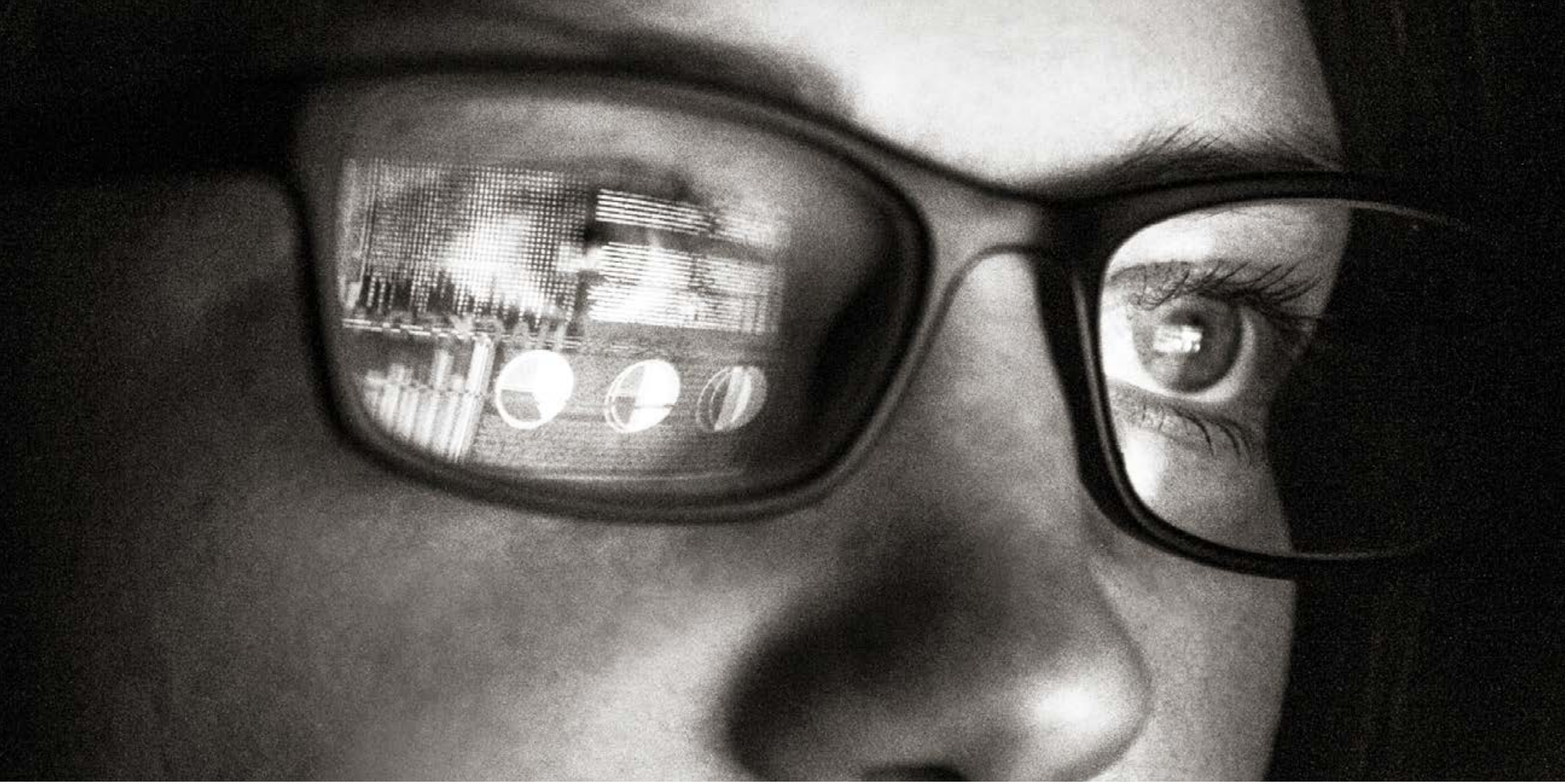


Electronics Industrial IoT cybersecurity

As strong as its weakest link

IBM Institute for Business Value

Benchmark Brief

Electronics

In this report

IBM capabilities

Connecting systems that monitor and control physical environments to the internet without securing them adequately is risky and potentially expensive. A successful cyberattack in IoT-enabled electronics operations can have catastrophic consequences. However, many of these risks can be addressed or mitigated. IBM helps electronics executives manage the growing amount of attack surfaces. We bring our cognitive approach to security disciplines that help protect equipment, production lines and provide new services that support platforms and ecosystems. Our strength in manufacturing and the depth of our global electronics experts can address quality while helping to protect assets and processes. IBM applies cognitive approaches to help reduce security risks. Please visit **ibm.com**/industries/electronics.

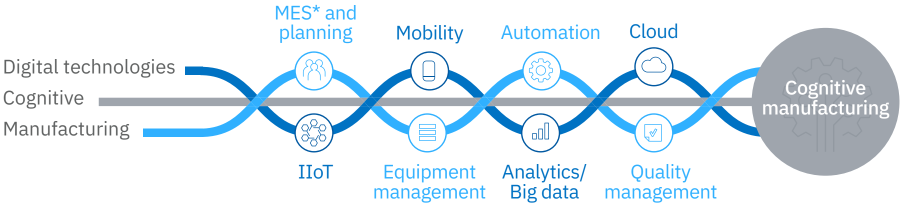
Electronics industry aims for stronger cybersecurity

Security for connected consumer devices gets all the attention. However, electronics companies should also focus deeply on security for industrial systems used to manufacture components and increasingly high-tech products. The production of "intelligent industrial things" must also have effective cybersecurity, or it can place a company's entire ecosystem at risk. Our research found more than 80 percent of electronics companies are implementing Industrial Internet of Things (IIoT) technologies in plants and assembly lines without fully evaluating the risks or preparing effective responses. Electronics companies need cybersecurity capabilities that are contextual, cognitive and adaptive to continuously identify, mitigate and prevent risk.

Unsecure all around

You wouldn't leave your plant door unlocked, would you? Yet electronics manufacturers might be exposing intelligent equipment and automated processes to potentially more dangerous risk. Manufacturing plants are becoming instrumented and connected. They are transforming into cyber-physical systems, with the IIoT as a core component of cognitive manufacturing (see Figure 1). IIoT devices and sensors embedded in physical assets provide data about the functioning of these systems. When this data is analyzed, it gives organizations a better understanding of their manufacturing operations and brings new business and operational opportunities to light.[1]

Figure 1
IIoT technologies are a foundational enabler of smarter manufacturing



*Source: IBM Services. *Manufacturing Execution Systems*

82%

of electronics companies surveyed are deploying IIoT technologies without fully evaluating the risks

91%

of electronics companies surveyed do not perform regular IIoT cybersecurity assessments

82%

of electronics companies surveyed do not have a formally established IIoT cybersecurity program

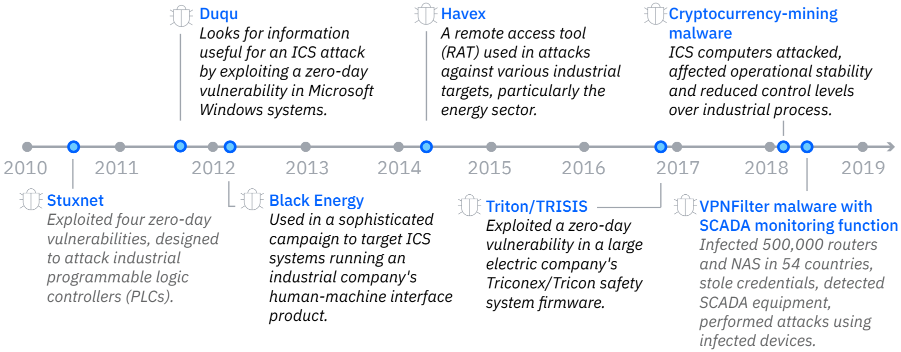
Manufacturing operations are among the most expensive parts of the electronics value chain. While IIoT provides insight, it can also increase the risk of exposure to potential cyberattacks and damage on multiple fronts. Each point presents a new opportunity for unauthorized entry. Whether caused by cyber hackers, competing companies, countries engaged in corporate espionage or even disgruntled employees, losses can mount quickly once under attack. The risks may include equipment failure, loss of critical data and corporate reputation, or even injury and loss of life.

IIoT technologies can vastly improve operational efficiencies, yet they also expose potential new attack surfaces and security targets if not properly protected. Each new machine joins “a system of systems” as it connects to additional IIoT devices. Technological expansions such as 5G will likely increase the use of IIoT technologies by providing the infrastructure needed to carry huge amounts of data.[2] But this also widens the attack surface. Virtually anything can become vulnerable, from high value assets or services, critical workloads in the cloud, process control subsystems in cyber-physical systems to critical business and operational data.

Consider an electronics manufacturer using Safety Instrumented System (SIS) controllers to read data from industrial equipment to help make sure machinery is functioning property. Compromises to these systems have the potential to cause physical damage and disrupt operations. In fact, in December 2017, Triton/Trisis malware was used to exploit a zero-day vulnerability in the firmware of a large electronics company’s Triconex/Tricon safety system. This caused a malfunction in the emergency protection system (see Figure 2).[3] It is not just assets that can be lost – the network itself is at risk.

Figure 2

Attacks on Industrial Control Systems (ICS) – A snapshot[4]



Stuxnet
Exploited four zero-day vulnerabilities, designed to attack industrial programmable logic controllers (PLCs).

Duqu
Looks for information useful for an ICS attack by exploiting a zero-day vulnerability in Microsoft Windows systems.

Black Energy
Used in a sophisticated campaign to target ICS systems running an industrial company's human-machine interface product.

Havex
A remote access tool (RAT) used in attacks against various industrial targets, particularly the energy sector.

Triton/TRISIS
Exploited a zero-day vulnerability in a large electric company's Triconex/Tricon safety system firmware.

Cryptocurrency-mining malware
ICS computers attacked, affected operational stability and reduced control levels over industrial process.

VPNFilter malware with SCADA monitoring function
Infected 500,000 routers and NAS in 54 countries, stole credentials, detected SCADA equipment, performed attacks using infected devices.

Organizations need capabilities that will protect not only their assets and networks, but also their entire IIoT ecosystems. Equally important is the ability to respond quickly and effectively in the event of a breach. Organizations of virtually all types must work to keep pace with ever-evolving IIoT threats.

To better understand IIoT security risks and implications, the IBM Institute for Business Value (IBV) partnered with Oxford Economics to survey 700 executives. They represent 700 companies in 18 countries from the energy and industrial sectors, of which 269 were electronics. They are all implementing IIoT in their plants.

Figure 3

The top five applications of IIoT technologies in electronics plants and assembly lines

65%
Real-time equipment monitoring

58%
Predictive maintenance

52%
Asset/equipment monitoring

45%
Machine/industrial automation

43%
Automated workflow

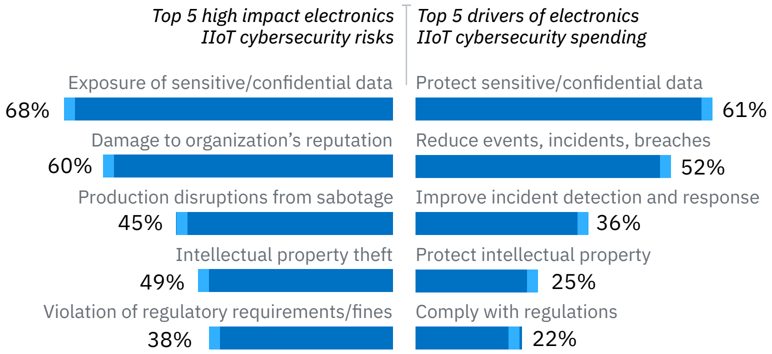
n=269.

The two most prevalent applications are for real-time equipment monitoring and predictive maintenance, at 65 percent and 58 percent (see Figure 3). Automation of machines and processes are also common applications, with 45 percent and 43 percent using IIoT technologies to automate machines and workflow respectively.

Electronics companies are aware of the cybersecurity risks and are working to manage their security spending accordingly (see Figure 4). But they are less clear on the combination of IIoT cybersecurity capabilities – skills, controls, practices and protective technologies – required to secure their current and future business from IIoT threats.

Figure 4

IIoT cybersecurity risks compared to security spending drivers



n=269.

Amid the rapid adoption of new technology, companies not prioritizing appropriate cybersecurity protection measures expose themselves to significant risks:

1. *Exposure of sensitive data.* Surveyed executives rate this as their highest risk. Sixty-eight percent are keenly aware of the impact that exposure of sensitive or confidential data, such as customer and employee data, supplier/partner intellectual property and contracts, could have on their company's growth. The outcomes may be serious: loss of revenue and investment, first-to-market advantage and losing business to competitors or counterfeiters.
2. *Damage to an organization's reputation and loss of public confidence.* The negative impact to an electronics company's image and reputation resulting from a security breach could be substantial, according to 60 percent of executives. The credibility and trustworthiness of a brand can be undermined and business and customer relationships irreparably damaged.
3. *Production disruptions resulting from sabotage.* Forty-five percent of surveyed executives said that this type of risk is significant, potentially resulting in damage to physical equipment and injured plant floor employees. Cyberattackers may gain access to a company's industrial systems and manipulate network infrastructure (see Figure 2 on page 3). An incursion could modify machine software programs or supervisory control and data acquisition systems (SCADA).

4. *Intellectual property (IP) theft.* IP is central to future growth. Trade secrets, such as engineering plans and proprietary manufacturing processes, are sources of competitive advantage. Forty percent of electronics companies recognize the impact that IP theft could have on their future growth. One small incursion places product design IP at risk.
5. *Violation of regulatory requirements.* The General Data Protection Regulation (GDPR), effective May 2018, coupled with environmental laws governing products and production processes, increase regulatory exposure and risk. Thirty-eight percent of surveyed executives are highly concerned about the potential impact of noncompliance with regulatory mandates – infractions that can lead to significant fines. While GDPR protects personal data, actual operating policies also require focus: emissions, energy use, recyclability and asset/waste disposition.

From a spending perspective, 61 percent of electronics respondents report that protecting sensitive data is the primary driver of their IIoT cybersecurity spending. More than 50 percent also cite reducing events, incidents and breaches as a primary driver.

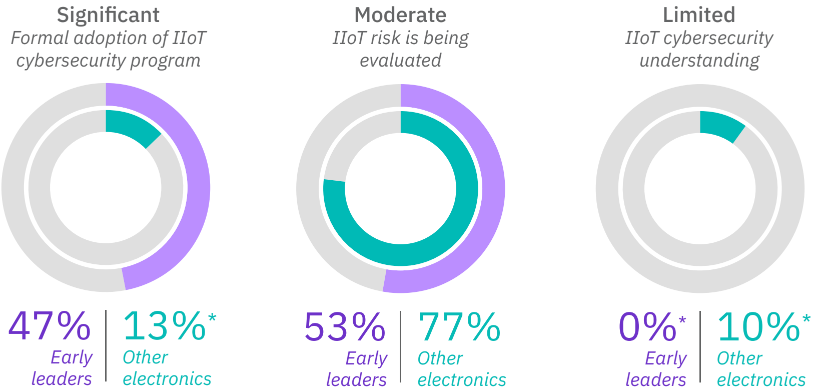
Aware and active: Early leaders are moving ahead to secure environments

We identified a group of early leaders who are already taking steps to secure their IIoT environments (see sidebar, “Early leaders by the numbers”).

While early leaders have some distance to cover before truly protecting these environments, they do have a significantly better grasp of the security needs of their IIoT deployments and connected Industrial Control Systems (ICS) than their peers. Forty-seven percent have created formal cybersecurity programs to establish, manage and update required IIoT cybersecurity tools, processes and skills versus only 13 percent of other electronics companies (see Figure 5).

Figure 5

Understanding of IIoT cybersecurity and adoption of formal cybersecurity programs



Early leaders n=76; other electronics n=233.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*
Note: See sidebar for details.

Early leaders by the numbers

Early leaders are comprised of companies across the industries we surveyed, including electronics. Of the 700 companies surveyed, 76 fell within this group, including 36 from electronics. This group was defined as being in the top quartile of performance on all three of the following metrics:

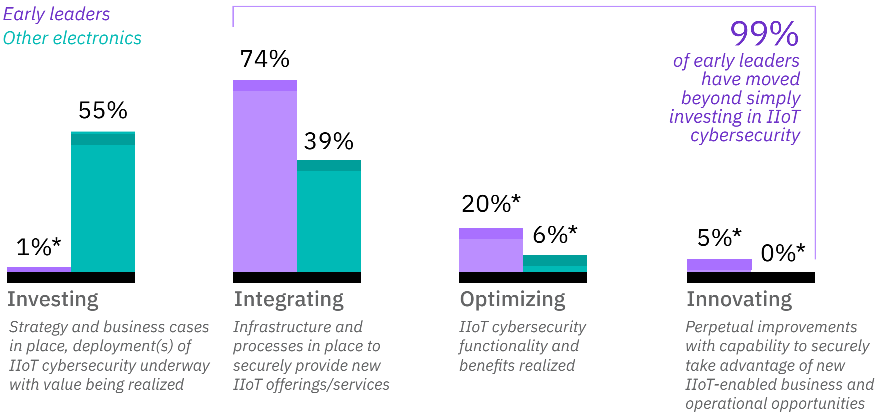
1. Percentage of known IIoT vulnerabilities addressed by security controls.
2. Cycle time to discover/detect IIoT cyber-security incidents. This excludes dwell time (the time between a successful intrusion and its discovery).
3. Cycle time to respond to and recover from IIoT cybersecurity incidents.

For the purposes of this study, references to “early leaders” include all industries surveyed, including the 36 from electronics. References to “other electronics” include the other 233 electronics companies – who were not in the 36 early leaders.

Early leaders also show greater maturity in integrating IIoT cybersecurity into their business and operational processes, with 99 percent moving beyond just investing in that area (see Figure 6). Twenty percent of early leaders have optimized IIoT cybersecurity functionality and realized benefits versus 6 percent of other electronics companies.

Figure 6

Maturity level of IIoT cybersecurity integration

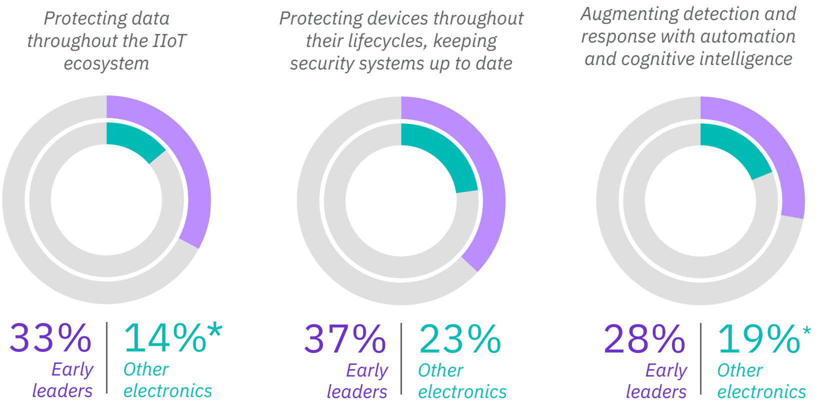


Early leaders n=76; other electronics n=233.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

Early leaders differentiate in their use of cybersecurity solutions for protecting data and devices and using automated and cognitive technologies to detect and respond to security threats in these three areas (see Figure 7):

Figure 7

Early leaders differentiate



Early leaders n=76, other electronics n=233.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

Protecting data throughout the IIoT ecosystem. A significant amount of sensitive data and IP is shared across electronics supply chains, which, if exposed or stolen, can put the future business of the company, its supply chain and partners at risk. Notably, 33 percent of early leaders versus 14 percent of other electronics companies are ahead in implementing specific cybersecurity solutions.

Protecting IIoT devices; keeping security systems up to date. Unprotected sensors and devices expose IT-OT (operational technology)-IIoT networks to cyberattacks that can have catastrophic physical and financial consequences. Thirty-seven percent of early leaders compared to 23 percent of other electronics companies are ahead in securing their IIoT devices.

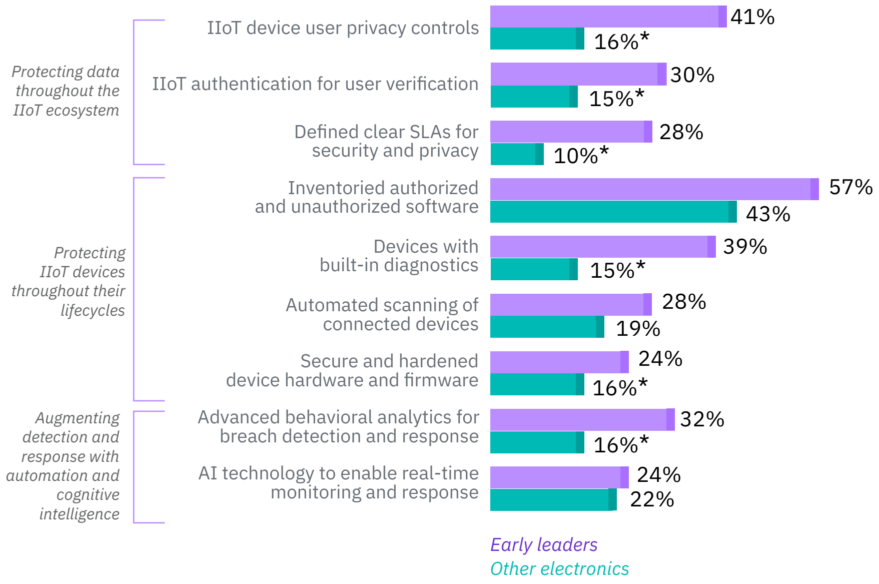
Augmenting detection and response with automation and cognitive intelligence. Protection and prevention do not address all issues. Put systems in place to detect breaches and to mitigate damage. Traditional detection systems are designed to address known attack and threat vectors and vulnerabilities. Cognitive capabilities, such as artificial intelligence (AI), machine learning and advanced behavioral analytics, help handle “unknowns” that may emerge and become exploited in the future. Twenty-eight percent of early leaders are ahead in implementing a combination of these practices versus 19 percent of other electronics companies.

Recommendations: Essential practices

Early leaders apply a risk- and compliance-based approach to security focusing on nine specific practices (see Figure 8).

Figure 8

Early leaders adopt differentiating security practices



Early leaders: n=76; other electronics: n=233.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

Protect yourself, your ecosystem and your customers: SLAs are mission critical to your success and safety. Know who has been granted entitlements to access sensitive functions or data.

Protecting data throughout the IIoT ecosystem

The greatest IIoT-related risk for electronics companies is the exposure of sensitive data. In fact, of all the types of IIoT-cybersecurity incidents (suspected, attempted and successful incursions) that occur in the electronics industry, data leakage is number one. It accounts for 26 percent of the total. These practices can help:

1. *Implement IIoT device user privacy controls.* If usage data can be linked to a device, information about a company's production and process secrets can be deduced.[5] To address this, companies should implement controls that allow users to specify how data is stored on their devices and how it is used and shared with third parties. Similar strategies are also important in other situations, such as change of ownership.[6]

1. *Implement IIoT authentication for user verification.* Twice as many early leaders (30 percent versus 15 percent) are in the advanced stages of adopting this practice. The ability to authenticate IIoT device identity is essential, especially for IIoT machine-to-machine (M2M) scenarios in which devices are often unattended.[7]

2. *Define clear service-level agreements (SLAs) for security and privacy.* Almost three times as many early leaders (28 percent versus 10 percent) monitor and enforce security requirements this way. To combat insider attacks and prevent information from being stolen or compromised, implement controlled access to data. Know who has been granted entitlements to access sensitive functions or data. Monitor and audit actions of those privileged users closely.

Protecting IIoT devices throughout their lifecycles, keeping security systems up to date

The most vulnerable parts of electronics IIoT deployments are platforms, cited by 23 percent of respondents, and devices and sensors, cited by 22 percent. Four practices to address key challenges in this area include:

1. *Inventory authorized and unauthorized software.* It is important to control versions of software that drive IIoT components, review threats associated with versioning and establish secure baselines. These initiatives should be accompanied by a deep understanding of endpoints – what they do and who they talk to. Each endpoint should be profiled, added to an asset inventory and monitored.[8]
2. *Deploy IIoT devices that have built-in diagnostics.* Early leaders are implementing devices that detect malfunctioning caused by failing components or tampering attempts. IIoT endpoints must often operate in hostile environments without human intervention for long periods of time.[9] While security and privacy of these endpoints is paramount, the opportunity to add cryptographic security features to hardware and software is often limited.[10]
3. *Automate the scanning of connected devices.* The practice of continuous vulnerability assessment and remediation is crucial. Performing active vulnerability scanning can adversely affect ICS network communications and, in turn, product and system availability. If automated scanning is not applicable, passive monitoring tools may be used instead.[11]

4. *Deploy secure and hardened device hardware and firmware.* Replacing devices is often expensive. Also, newer devices may not be available with improved security. Companies should consistently perform coordinated patching and updates, despite the inherent challenges of updating devices that often run all day, every day. This becomes particularly important for legacy devices, as many were manufactured with inadequate security.[12]

Augment detection and response with automation and cognitive intelligence
Protection and prevention do not address all issues and a securely developed and deployed system is not a guarantee of absolute protection. Attackers continually seek new ways to infiltrate systems, so automated mechanisms must be in place to detect and remediate breaches.

The greatest challenge to securing electronics IIoT deployments is a lack of highly skilled cybersecurity resources, according to 44 percent of surveyed executives. Electronics companies can reduce manual threat detection by implementing AI-driven, automated investigation processes. Threats can be systemically prioritized for customized alerts by defining sensitive data and assets, network segments and cloud services. Two practices to embrace AI-enabled threat detection and remediation are:

1. *Apply advanced behavioral analytics for breach detection and response.* Twice as many early leaders use behavior analytics that leverage machine learning. AI-enabled threat detection can be applied at an enterprise level to uncover anomalous user activities and prioritize risks. Early leaders are also ahead in applying machine learning to automate adaptive models of what is considered normal, tracking this normal behavior and flagging anomalous activity that can signal new threats.
2. *Implement AI technology to enable real-time security monitoring and response.* The ability to apply data-driven techniques to create real-time feeds of threat intelligence from both external and internal sources allows for even faster detection and remediation.

IIoT necessitates the convergence of IT and OT — the systems that monitor and control physical environments. This introduces complexity and a unique set of risks. It is crucial that IIoT technologies be properly secured. Otherwise, their immediate operational and financial benefits may come at the cost of an entire ecosystem's future.

Mitigating losses through automation[13]

The research organization Ponemon recently reported that the faster a data breach can be identified and contained, the lower the costs. They found that the extensive use of IoT devices increases the cost per compromised record by USD 5, but the average cost of a data breach for organizations with fully deployed security automation is 35 percent less than that for organizations without automation.

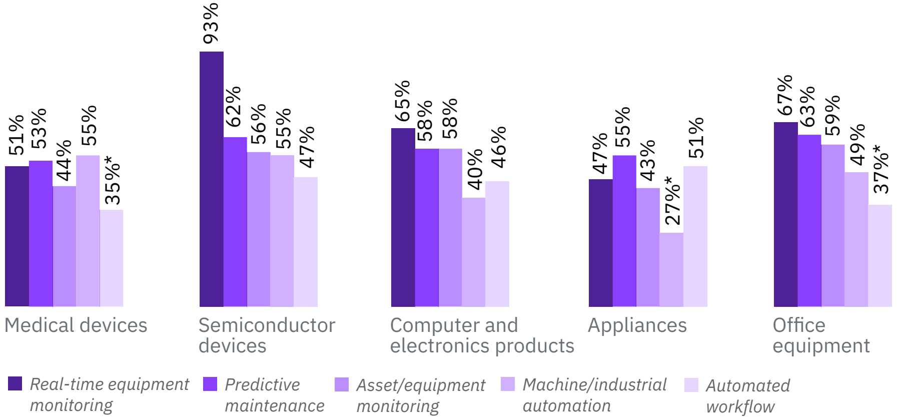
Security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning, analytics and orchestration.

Sector viewpoints

A challenge: Delivering the appropriate level of electronics sector nuance while creating a broad perspective. Yet, there are notable sector differences across the electronics industry. To capture these, the IBV created detailed sector breakouts for key questions to allow executives to explore their IIoT cybersecurity concerns more deeply. Figure 9 indicates how each sector is applying IIoT technologies in their plants and assembly lines.

Figure 9

The top five IIoT applications in plants and assembly lines by electronics sector



n=269.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

The following table summarizes the top three IIoT-related vulnerabilities, threats and incidents by electronics sector.

The top three		Medical device manufacturers	Semiconductor device manufacturers	Computer and electronics product manufacturers	Appliance manufacturers	Office equipment manufacturers
IIoT vulnerabilities	**1**	**24%** IoT platforms	**22%** IoT platforms	**32%** IoT platforms	**37%** Applications built on top of cloud solutions and IoT platforms	**27%** Devices and sensors
	2	**24%** Devices and sensors	**22%** Devices and sensors	**28%** Devices and sensors	**20%** IoT platforms	**24%** Data stored in the cloud
	3	**16%** Data stored in the cloud	**15%** Communications between devices and gateways	**19%** Data stored in the cloud	**14%** Data stored in the cloud	**16%** IoT platforms
IIoT-related threats	**1**	**56%** Information gathering, data leakage	**55%** Information gathering, data leakage	**44%** Information gathering, data leakage	**69%** Unauthorized access	**45%** Unauthorized access
	2	**42%** DOS/DDoS attacks	**45%** Unauthorized access	**40%** Unauthorized access	**51%** Access or credentials abuse	**43%** DOS/DDoS attacks
	3	**38%** Unauthorized access	**42%** DOS/DDoS attacks	**30%** DOS/DDoS attacks	**45%** Information gathering, data leakage	**35%** Information gathering, data leakage
IIoT cybersecurity incidents	**1**	**25%** IP theft/data leakage	**28%** IP theft/data leakage	**26%** IP theft/data leakage	**32%** Internal theft/fraud	**27%** IP theft/data leakage
	2	**23%** Privacy breach	**19%** Internal theft/fraud	**21%** Privacy breach	**23%** IP theft/data leakage	**23%** Internal theft/fraud
	3	**19%** Internal theft/fraud	**18%** Privacy breach	**16%** Internal theft/fraud	**21%** Privacy breach	**17%** Privacy breach

Related IBV publications

Gonzalez-Wertz, Cristene, John Constantopoulos, Qin XK Deng, Hiroshi Yamamato, and Quentin Samelson. "Why cognitive manufacturing matters in electronics: Activating the next generation of production success." IBM Institute for Business Value. February 2017. http://www-935.ibm.com/services/us/gbs/thoughtleadership/cognitivemanufacturing/

Hahn, Tim, Marcel Kisch, and James Murphy. "Internet of threats: Securing the Internet of Things for industrial and utility companies." IBM Institute for Business Value. March 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

"Intelligent Connections – Reinventing enterprises with intelligent IoT." Global C-suite Study 19th Edition. IBM Institute for Business Value. January 2018. https://www.ibm.com/services/insights/c-suite-study/iot

IIoT cybersecurity key takeaways

- Have a clear IIoT security strategy.
- Align security practices with the organization's broader risk frameworks and integrate security technologies into operational processes.
- Be proactive.
- Balance prevention with detection.
- Make security capabilities "intelligent" and automated, so they can deal with the advanced threats of today and unknown threats now and in the future.
- Be prepared to recover fast in the event of a breach.
- Develop response and communications plans – before they are needed.

Are you ready to prioritize cybersecurity?

- How does your IIoT cybersecurity program address the management of risk and compliance?
- How have you integrated IIoT cybersecurity into your business and operational processes?
- How are you assuring visibility into your enterprise's most valuable assets and vulnerabilities to guide intelligent, effective prioritization of threats?
- How are you giving your employees insight into IIoT cybersecurity operations?
- What types of cybersecurity breach simulations do you perform to prepare your organization?

For more information
To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for phone or tablet from your app store.

The right partner for a changing world
At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value
The IBM Institute for Business Value (IBV), part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

Authors

Cristene Gonzalez-Wertz is the Electronics and Environment, Energy and Utilities Leader for the IBM Institute for Business Value. She advises clients on technology trends and strategic positioning in AI, analytics, IoT, security, and customer experience. Cristene provides guidance on emerging value opportunities, especially the data economy. She can be reached at cristeneg@us.ibm.com or on LinkedIn at https://www.linkedin.com/in/cjgw1/

Lisa-Giane Fisher is the Benchmarking Leader for the IBM Institute for Business Value in the Middle East and Africa. She is responsible for warranty and IoT security benchmarking and collaborates with IBM industry experts to develop and maintain industry process frameworks. Lisa can be reached at lfisher@za.ibm.com and on LinkedIn at linkedin.com/in/lisa-giane-fisher

Peter Xu is currently the CTO for the IBM Global Electronics Industry. For the past 20 years, Peter has been working at the intersection of emerging information, operation and communication technologies. He excels at guiding clients in solving complex business challenges, leveraging his broad hands-on technical expertise with deep industry insights. Peter can be reached at peteryxu@us.ibm.com and on LinkedIn at linkedin.com/in/peteryxu/

Martin Borrett is the CTO of IBM Security Europe, advising senior-level clients on security-related policy, business, technical and architectural issues. Martin leads IBM’s Security Blueprint work and is co-author of two IBM Redbooks. He is a Fellow of the British Computer Society, a Chartered Engineer (CEng) and member of the Institution of Engineering and Technology. Martin can be reached at borretm@uk.ibm.com and on LinkedIn at linkedin.com/in/martinborrett/

Notes and sources

1 Gonzalez-Wertz, Cristene, John Constantopoulos, Qin XK Deng, Hiroshi Yamamato and Quentin Samelson. "Why cognitive manufacturing matters in electronics: Activating the next generation of production." IBM Institute for Business Value. February 2017. http://www-935.ibm.com/services/us/gbs/thoughtleadership/cognitivemanufacturing/

2 Moore, Mike. "What is 5G? Everything you need to know." Techradar. September 2018. https://www.techradar.com/news/what-is-5g-everything-you-need-to-know

3 "TRISIS/TRITON." New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). December 24, 2017. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton

4 "Attacks on Industrial Control Systems." IBM Security. 2015. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03046USEN. "TRISIS/TRITON." New Jersey Cybersecurity & Communications Integration Cell. Dec. 14, 2017. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton. "Threat Landscape for Industrial Automation Systems H1 2018." Kaspersky ICS CERT. 2018. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/09/06075839/H1_2018_ICS_REPORT_v1.0_ENG_05092018.pdf

5 Hahn, Tim and JR Rao. "IoT Security: An IBM Position Paper." Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. For direct link to paper go to https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN

6 Maxim, Merritt. "TechRadar™: Internet Of Things Security, Q1 2017." Forrester. January 19, 2017. https://www.forrester.com/report/TechRadar+Internet+Of+Things+Security+Q1+2017/-/E-RES117394

7 Ibid.

8 Hahn, Tim, Marcel Kisch and James Murphy. "Internet of threats: Securing the Internet of Things for industrial and utility companies." IBM Institute for Business Value. March 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

9 "Five indisputable facts about IoT security." IBM Security. February 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEF03018USEN&appname=skmwww

10 Hahn, Tim and JR Rao. "IoT Security: An IBM Position Paper." Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. For direct link to paper go to https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN

11 "CIS Controls Version 7 Implementation Guide for Industrial Control Systems." Center for Internet Security. 2018. https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

12 Grau, Alan. "What's the Difference Between Device Hardening and Security Appliances?" Electronic Design. August 3, 2017. https://www.electronicdesign.com/industrial-automation/what-s-difference-between-device-hardening-and-security-appliances

13 "2018 Cost of a Data Breach Study: Global Overview." Benchmark research sponsored by IBM Security. Independently conducted by Ponemon Institute LLC. July 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an "as is" basis and IBM makes no representations or warranties, express or implied.

85020085USEN-00