Automotive Industrial Internet of Things

Quick to implement, slow to secure

IBM Institute for Business Value

Benchmark Brief

Automotive

In this report

Automotive IIoT cybersecurity risks and adoption progress

Three areas where top performers differentiate in securing their IIoT environments

Nine essential cybersecurity practices

IBM capabilities

Today’s vehicles are evolving from a mode of transport to also serve as a new kind of moving data center with onboard sensors and computers that capture information about the vehicle. Using such real-time data, IBM helps auto executives provide new services that the connected consumer needs and expects from the vehicle experience. Our combined strength in manufacturing and depth of global automotive expertise can help address consumer concerns about safety and quality. Innovative technologies such as Watson for analytic capabilities can meet original equipment manufacturer (OEM) and supplier needs, including products and services that are more secure and reliable to enable higher brand loyalty and customer satisfaction. Please visit **ibm.com**/industries/automotive.

Automotive industry aims for stronger cybersecurity

Security for connected and autonomous vehicles gets all the attention. But companies need to focus on fundamentals – the industrial systems used for manufacturing automobiles and their increasingly high-tech components. Bringing "intelligent industrial things" online without effective cybersecurity puts an entire company at risk. Based on an IBM Institute for Business Value (IBV) survey, 87 percent of automotive companies are implementing Industrial Internet of Things (IIoT) technologies in plants and assembly lines without fully evaluating risk or preparing effective responses. Automotive companies need improved cybersecurity capabilities that are contextual, cognitive and adaptive, allowing them to continuously identify, mitigate and prevent risk.

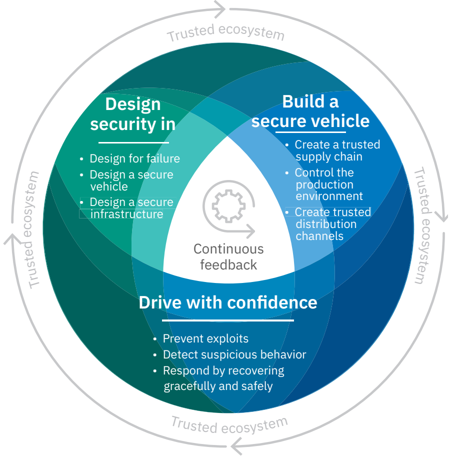
Unsecure all around

As manufacturing equipment and processes become more intelligent and automated through the implementation of IIoT technologies, companies run the risk of cyberattacks. Whether by cyber hackers, competing companies, countries engaged in corporate espionage or even disgruntled employees, cyber incursions can lead to extensive equipment damage, loss of critical data and corporate reputation, or even injury and loss of life.

In the IBV study "Accelerating security: Winning the race to vehicle integrity and data privacy," we introduced the Design, Build, Drive security approach (see Figure 1).[1] The "Build a secure vehicle" phase of this approach articulates a requirement to control the production environment.

Figure 1

The Design, Build, Drive approach to security


Trusted ecosystem
Trusted ecosystem
Trusted ecosystem
Trusted ecosystem
Design security in
• Design for failure
• Design a secure vehicle
• Design a secure infrastructure
Build a secure vehicle
• Create a trusted supply chain
• Control the production environment
• Create trusted distribution channels
Continuous feedback
Drive with confidence
• Prevent exploits
• Detect suspicious behavior
• Respond by recovering gracefully and safely

Source: IBM Institute for Business Value analysis.

87%

of automotive companies surveyed are deploying IIoT technologies without full evaluation of the risks

86%

of automotive companies surveyed do not perform regular IIoT cybersecurity assessments

87%

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

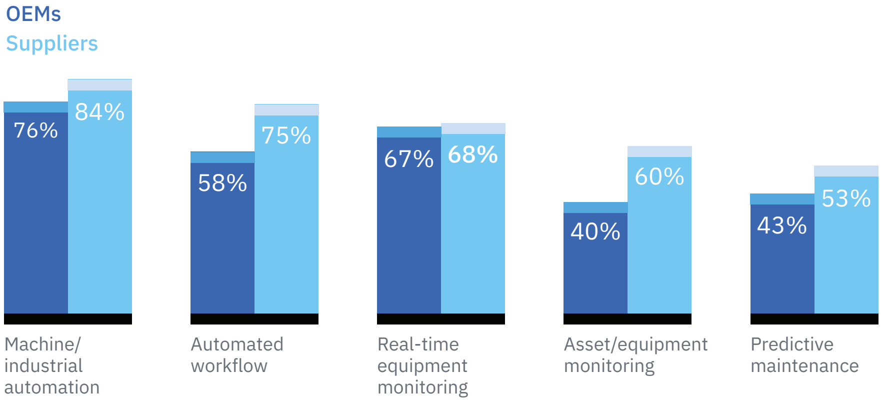
While IIoT implementations can vastly improve operational efficiencies, they also expose potential new attack surfaces and security targets if not properly protected. Virtually anything can become vulnerable to cyberattacks, from high-value assets or services, critical workloads in the cloud, process control systems in cyber-physical systems, to critical business and operational data.

To better understand IIoT security risks and implications, the IBV partnered with Oxford Economics to survey 700 executives. They represent 700 companies in 18 countries from the energy and industrial sectors (of which 135 were automotive) that are implementing IIoT in their plants.

Machine/industrial automation leads the list of IIoT applications for 76 percent of original equipment manufacturers (OEMs) and 84 percent of suppliers (see Figure 2). Next, 58 percent of OEMs and 75 percent of suppliers said they have automated workflow applications. Surprisingly, predictive maintenance applications were not as high on the list as expected

Figure 2

Top five applications of IIoT technologies in automotive plants and assembly lines

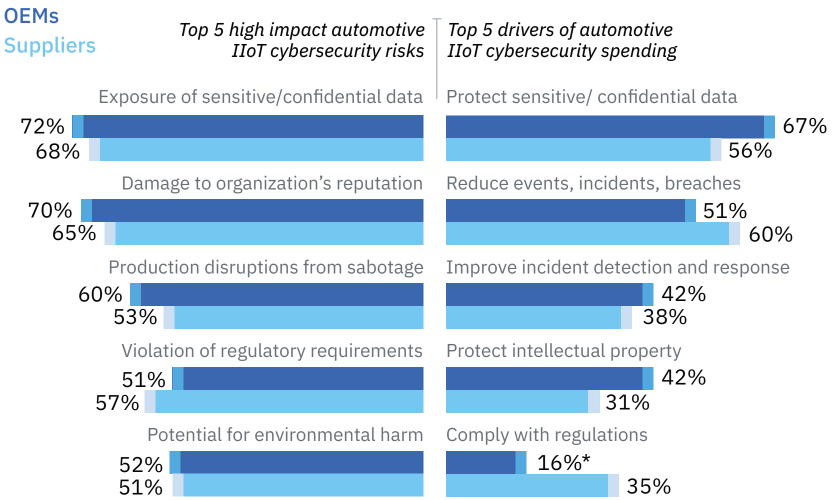


n=135.

Automotive companies appear to be aware of the cybersecurity risks and have, to an extent, aligned their IIoT spending accordingly (see Figure 3). But they are not clear on the combination of IIoT cybersecurity capabilities – skills, controls, practices and protective technologies – required to secure their current and future businesses from IIoT threats.

Figure 3

IIoT cybersecurity risks compared to spending drivers



n=135.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

By failing to implement appropriate cybersecurity protection measures, automotive companies are exposed to significant risks. Specifically:

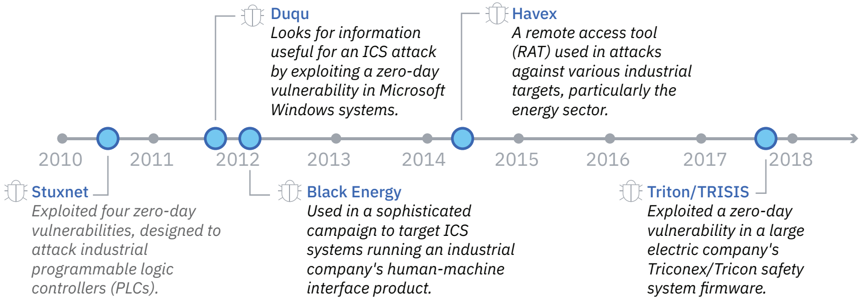
1. *Exposure of sensitive/confidential data.* Surveyed executives rate this as their highest risk. Seventy-two percent of OEMs and 68 percent of suppliers are keenly aware of the impact that the exposure of data, such as customer intellectual property and advanced engineering designs, could have on their company's growth.

2. *Damage to an organization's reputation and loss of public confidence.* The negative impact to an automotive company's image and reputation resulting from a security breach can be substantial, according to 70 percent of OEMs and 65 percent of suppliers. The credibility and trustworthiness of a brand can easily be undermined, with business and customer relationships irreparably damaged.

3. *Production disruptions resulting from sabotage.* Sixty percent of OEMs and 53 percent of suppliers said that this type of risk is significant, potentially resulting in the destruction of physical equipment and production of faulty parts or vehicles. Cyberattackers can gain access to a company's industrial systems and manipulate network infrastructure (see Figure 4). They can modify machine software programs or supervisory control and data acquisition systems (SCADA).

Figure 4

Attacks on Industrial Control Systems (ICS) – A snapshot[2]



Duqu
Looks for information useful for an ICS attack by exploiting a zero-day vulnerability in Microsoft Windows systems.
Havex
A remote access tool (RAT) used in attacks against various industrial targets, particularly the energy sector.
2010
2011
2012
2013
2014
2015
2016
2017
2018
Stuxnet
Exploited four zero-day vulnerabilities, designed to attack industrial programmable logic controllers (PLCs).
Black Energy
Used in a sophisticated campaign to target ICS systems running an industrial company's human-machine interface product.
Triton/TRISIS
Exploited a zero-day vulnerability in a large electric company's Triconex/Tricon safety system firmware.

4. *Violation of regulatory requirements.* The General Data Protection Regulation (GDPR), effective May 2018, and similar laws increase regulatory exposure and risk. Fifty-one percent of OEMs and 57 percent of suppliers surveyed say they are highly concerned about the potential impact of noncompliance with regulatory mandates – infractions that can lead to significant fines.

5. *Potential for environmental harm.* Fifty-two percent of OEMs and 51 percent of suppliers surveyed are highly concerned about the release of hazardous materials into the environment if controls are breached.

From a spending perspective, protecting sensitive data is at the top of the list, with 67 percent of OEMs and 56 percent of suppliers citing it as a primary driver of their IIoT cybersecurity budgets. More than 50 percent of OEMs and suppliers also state that reducing events, incidents and breaches are high-priority areas.

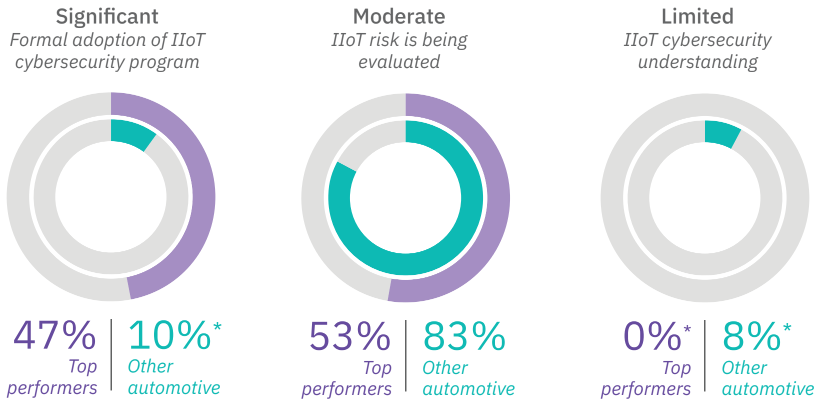
Top performers lead

We identified a group of top performers who lead the way in securing their IIoT environments (see sidebar, “Top performers by the numbers”).

While top performers have a ways to go before truly protecting these environments, they do have a significantly better grasp of what’s needed 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 10 percent of other automotive companies (see Figure 5).

Figure 5

Understanding of IIoT cybersecurity and adoption of formal cybersecurity programs



Top performers n=76; other automotive n=115.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*
Note: See sidebar for details.

Top performers by the numbers

Top performers are comprised of companies across the industries we surveyed, including automotive. Of the 700 companies surveyed, 76 fell within this group, including 20 from automotive. This group was defined as being in the top quartile of performance on all three of the following metrics:

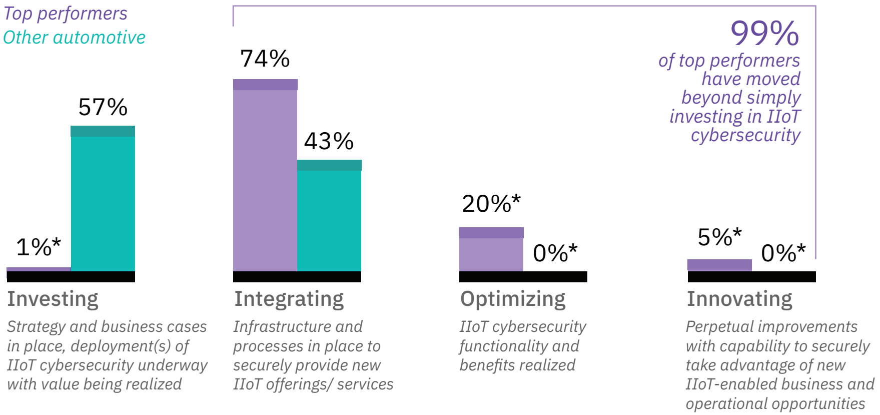
1. Percentage of known IIoT vulnerabilities addressed by security controls.
2. Cycle time to identify and detect IIoT cybersecurity incidents. This excludes dwell time (the time between a successful intrusion and its discovery).
3. Cycle time to respond to and recover from IIoT cybersecurity incidents.

For the purposes of this study, references to “top performers” include all industries surveyed, including the 20 from automotive. References to “other automotive” include the other 115 automotive companies – but not the 20 in top performers.

Top performers also integrate IIoT cybersecurity into their business and operational processes at a much faster rate (see Figure 6). Twenty percent of top performers have optimized IIoT cybersecurity functionality and realized benefits versus zero percent of other automotive companies. And an additional five percent are actually engaging in new innovations based on their IIoT cybersecurity integration.

Figure 6

Maturity level of IIoT cybersecurity integration

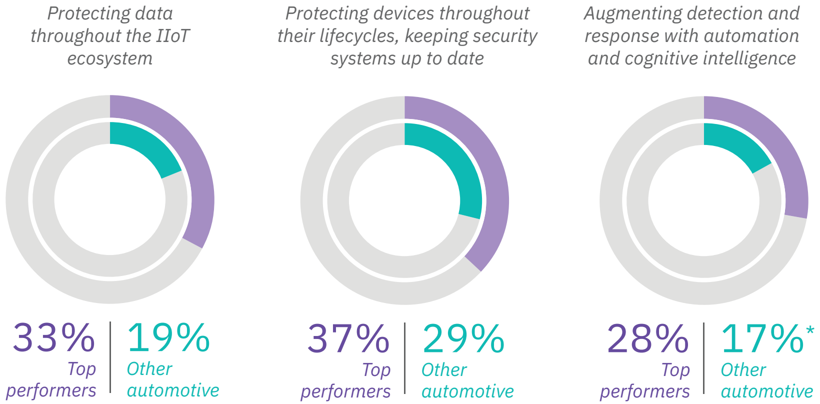


Top performers n=76; other automotive n=115.
**Low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

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

Figure 7

Top performers differentiate



Top performers n=76; other automotive n=115.
**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 intellectual property (IP) is shared across automotive supply chains. If exposed or stolen, this data can put a company's future business at risk. Notably, 33 percent of top performers versus 19 percent of other automotive companies are ahead in implementing specific cybersecurity solutions.

Protecting IIoT devices throughout their lifecycles; keeping security systems up to date. Unprotected sensors and devices expose operational technology (OT)/IIoT networks to cyberattacks that can have catastrophic physical and financial consequences. Thirty-seven percent of top performers are adequately securing their IIoT devices, compared to 29 percent of other automotive companies.

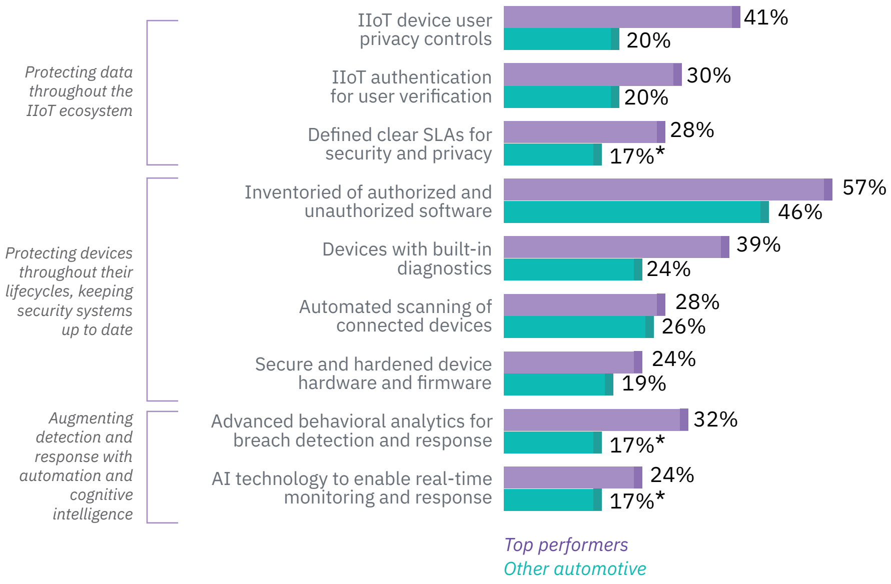
Augmenting detection and response with automation and cognitive intelligence. Protection and prevention do not address all issues. Put systems in place to detect breaches and to mitigate damage. Traditional detection systems are designed to address known attack and threat vectors and vulnerabilities. Cognitive capabilities, such as artificial intelligence (AI), machine learning and advanced behavioral analytics, help to handle "unknowns" that may emerge and become exploited in the future. Twenty-eight percent of top performers are ahead in implementing a combination of these practices versus 17 percent of other automotive companies.

Essential practices

Top performers apply a risk- and compliance-based approach to security, focusing on nine practices (see Figure 8).

Figure 8

Nine differentiating security practices deployed by top performers



Top performers n=76; other automotive n=115.

**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 critical IIoT-related risk for automotive companies is the exposure of sensitive data. The number one type of incident is data leakage. It accounts for over a quarter of IIoT cybersecurity incidents in the industry (32 percent for OEMs and 28 percent for suppliers). These practices can help:

1. *Implement IIoT device user privacy controls.* If usage data can be linked to a device, users can deduce information about a company's production and process secrets.[3] Forty-one percent of top performers versus 20 percent of other automotive companies have implemented 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.[4]

2. *Implement IIoT authentication for user verification.* Thirty percent of top performers versus 20 percent of others 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.[5]

3. *Define clear service level agreements (SLAs) for security and privacy.* Twenty-eight percent of top performers versus 17 percent of other automotive companies 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 devices throughout their lifecycles, keeping security systems up to date
Just over one-third of automotive executives report that devices and sensors are the most vulnerable parts of their IIoT deployments. Almost half report that applying software patches to connected objects is the greatest challenge to securing them. Four practices to protect devices are:

1. *Inventory authorized and unauthorized software.* Fifty-seven percent of top performers versus 46 percent of other automotive companies have been active in this area. Controlling versions of software that drive IIoT components, reviewing threats associated with versioning and establishing secure baselines are critical. These initiatives should be accompanied by deep understanding of endpoints – what they do and who they talk to. Each endpoint should be profiled, added to an asset inventory and monitored.[6]

2. *Deploy IIoT devices with built-in diagnostics.* Thirty-nine percent of top performers have implemented devices that detect malfunctioning caused by failing components or tampering attempts versus 24 percent of other automotive companies. IIoT endpoints often operate in hostile environments without human intervention for long periods of time. While security and privacy of these endpoints is paramount, the opportunity to add cryptographic security features to hardware and software is often limited.[7]

A critical IIoT-related risk for automotive companies is the exposure of sensitive data.

3. *Automate the scanning of connected devices.* The practice of continuous vulnerability assessment and remediation is crucial. Top performers and others have implemented strategies to address scanning and remediation to almost the same degree. However, performing active vulnerability scanning can adversely affect Industrial Control System (ICS) network communications and, in turn, product and system availability. If automated scanning is not feasible, passive monitoring tools need to be used instead.[8]

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 need to 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.[9] Executives from all companies surveyed recognize this issue and are focusing on it to some extent. However, top performers (24 percent) are slightly ahead in their implementations than other automotive companies (19 percent).

Augment detection and response capabilities

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.

Because cybersecurity resources are inevitably limited, automotive companies need to reduce manual threat detection by implementing investigative processes using AI and automation (see sidebar, “Mitigating loses through automation”). 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.* Thirty-two percent of top performers already possess user behavior analytics that leverage machine learning versus 17 percent of others. AI-enabled threat detection can be applied at an enterprise level to uncover anomalous user activities and prioritize risks. Top performers are also ahead of other automotive companies in applying machine learning to automate adaptive models of what is considered normal. This approach can track these normal behavior patterns and flag anomalous activity that can signal new threats.

2. *Implement AI technology to enable real-time security monitoring and response.* Top performers are slightly ahead of other automotive companies in this space, with 24 percent versus 17 percent respectively. 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.

Mitigating losses through automation[10]

Ponemon recently reported that 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.

IIoT necessitates the convergence of IT and OT. 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 organization’s future.

Have a clear IIoT security strategy. Bring security practices into alignment with the organization’s broader risk frameworks and integrate security technologies into operational processes. Be proactive. Balance prevention with detection. Make security capabilities “intelligent” 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. And have response and communications plans ready – 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 giving your employees insight into IIoT cybersecurity operations?

What types of cybersecurity breach simulations do you perform to prepare your organization?

How are you assuring visibility into the enterprise's most value assets and vulnerabilities to guide intelligent and effective prioritization of risk?

Related IBV publications

Serio, Guiseppe and Ben Stanley. "Accelerating security: Winning the race to vehicle integrity and data privacy." IBM Institute for Business Value. January 2017. https://www-935.ibm.com/services/us/gbs/thoughtleadership/acceleratesecurity/

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

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

Giuseppe Serio is the IBM Global Solution Leader for Cybersecurity in the automotive and aerospace and defense industries and has more than 20 years of experience. He engages with clients globally to discuss security programs and security challenges, including connected vehicle security. He collaborates with other IBM functions such as research and security and the IoT business units to develop and adapt security solutions to specific industry needs. Giuseppe can be reached at giuseppe.serio@de.ibm.com and on LinkedIn at linkedin.com/in/giuseppe-serio-183582

Ben Stanley is the Automotive Research Leader for the IBM Institute for Business Value. He is responsible for developing thought leadership content and strategic business insights for the IBM automotive industry practice. Ben has over 40 years of automotive experience and has worked with major automotive clients around the world in business strategy and business model innovation. Ben can be reached at ben.stanley@us.ibm.com and on LinkedIn at linkedin.com/in/benjamintstanley

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 and the American Productivity & Quality Center (APQC) to develop and maintain industry process frameworks. Lisa has over 10 years of experience consulting and managing multidisciplinary teams to deliver complex IT projects across industries. Lisa can be reached at lfisher@za.ibm.com and on LinkedIn at linkedin.com/in/lisa-giane-fisher

Notes and sources

1 Serio, Guiseppe and Ben Stanley. “Accelerating security: Winning the race to vehicle integrity and data privacy.” IBM Institute for Business Value. January 2017. https://www-935.ibm.com/services/us/gbs/thoughtleadership/acceleratesecurity/

2 “Attacks on Industrial Control Systems.” IBM Security. 2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03046USEN&attachment=SEL03046USEN.PDF; “TRISIS/TRITON.” New Jersey Cybersecurity & Communications Integration Cell. Dec. 14, 2017. https:www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton

3 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

4 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

5 Ibid.

6 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/

7 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

8 "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/

9 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

10 "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
September 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.

IBM®