Automotive Industrial Internet of Things

*Quick to implement, slow to secure*
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.

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
Unsecure all round

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). The “Build a secure vehicle” phase of this approach articulates a requirement to control the production environment.

---

Source: IBM Institute for Business Value analysis.
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.

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 2
Top five applications of IIoT technologies in automotive plants and assembly lines

<table>
<thead>
<tr>
<th>Application</th>
<th>OEMs</th>
<th>Suppliers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine/industrial automation</td>
<td>76%</td>
<td>75%</td>
</tr>
<tr>
<td>Automated workflow</td>
<td>84%</td>
<td>84%</td>
</tr>
<tr>
<td>Real-time equipment monitoring</td>
<td>58%</td>
<td>58%</td>
</tr>
<tr>
<td>Predictive maintenance</td>
<td>67%</td>
<td>67%</td>
</tr>
<tr>
<td>Asset/equipment monitoring</td>
<td>68%</td>
<td>68%</td>
</tr>
</tbody>
</table>

Source: IBM Institute for Business Value benchmarking study, 2018, n=135.
Figure 3
IIoT cybersecurity risks compared to spending drivers

<table>
<thead>
<tr>
<th>Exposures of sensitive/confidential data</th>
<th>Protect sensitive/confidential data</th>
</tr>
</thead>
<tbody>
<tr>
<td>72% (68%) OEMs</td>
<td>67% (56%) Suppliers</td>
</tr>
<tr>
<td>70% (65%) Suppliers</td>
<td>Reduce events, incidents, breaches</td>
</tr>
<tr>
<td>51% (42%) Violation of regulatory requirements</td>
<td>Protect intellectual property</td>
</tr>
<tr>
<td>57% (42%) Production disruptions from sabotage</td>
<td>Comply with regulations</td>
</tr>
<tr>
<td>52% (51%) Potential for environmental harm</td>
<td></td>
</tr>
</tbody>
</table>

Source: IBM Institute for Business Value benchmarking study, 2018, 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).

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

Source: IBM Institute for Business Value benchmarking study, 2018, 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: References to “top performers” in this and other figures 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

Source: IBM Institute for Business Value benchmarking study, 2018, 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

- Protecting data throughout the IIoT ecosystem
- Protecting devices throughout their lifecycles, keeping security systems up to date
- Augmenting detection and response with automation and cognitive intelligence

<table>
<thead>
<tr>
<th>Area of Protection</th>
<th>Top Performers</th>
<th>Other Automotive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting data</td>
<td>33%</td>
<td>19%</td>
</tr>
<tr>
<td>Protecting devices</td>
<td>37%</td>
<td>29%</td>
</tr>
<tr>
<td>Augmenting detection and response</td>
<td>28%</td>
<td>17%*</td>
</tr>
</tbody>
</table>

Source: IBM Institute for Business Value benchmarking study, 2018, 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. Systems must be 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

- IIoT device user privacy controls: 20% (41% for top performers)
- IIoT authentication for user verification: 20% (30% for top performers)
- Defined clear SLAs for security and privacy: 17%* (28% for top performers)
- Inventoried of authorized and unauthorized software: 46% (57% for top performers)
- Devices with built-in diagnostics: 24% (39% for top performers)
- Automated scanning of connected devices: 28% (26% for top performers)
- Secure and hardened device hardware and firmware: 24% (19% for top performers)
- Advanced behavioral analytics for breach detection and response: 17%* (32% for top performers)
- AI technology to enable real-time monitoring and response: 17%* (24% for top performers)

Source: IBM Institute for Business Value benchmarking study, 2018, 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
The greatest 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). Consider these three practices to help protect data throughout the IIoT ecosystem:

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. 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.

2. **Implement IIoT authentication for user verification.** Thirty percent of top performers versus twenty 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.

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 help stop 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 more closely.
Protecting devices throughout their lifecycles, keeping security systems up to date

Just over one-third of automotive executives surveyed 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
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 losses 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

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.
Is your business at risk?

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


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


5  Ibid.


