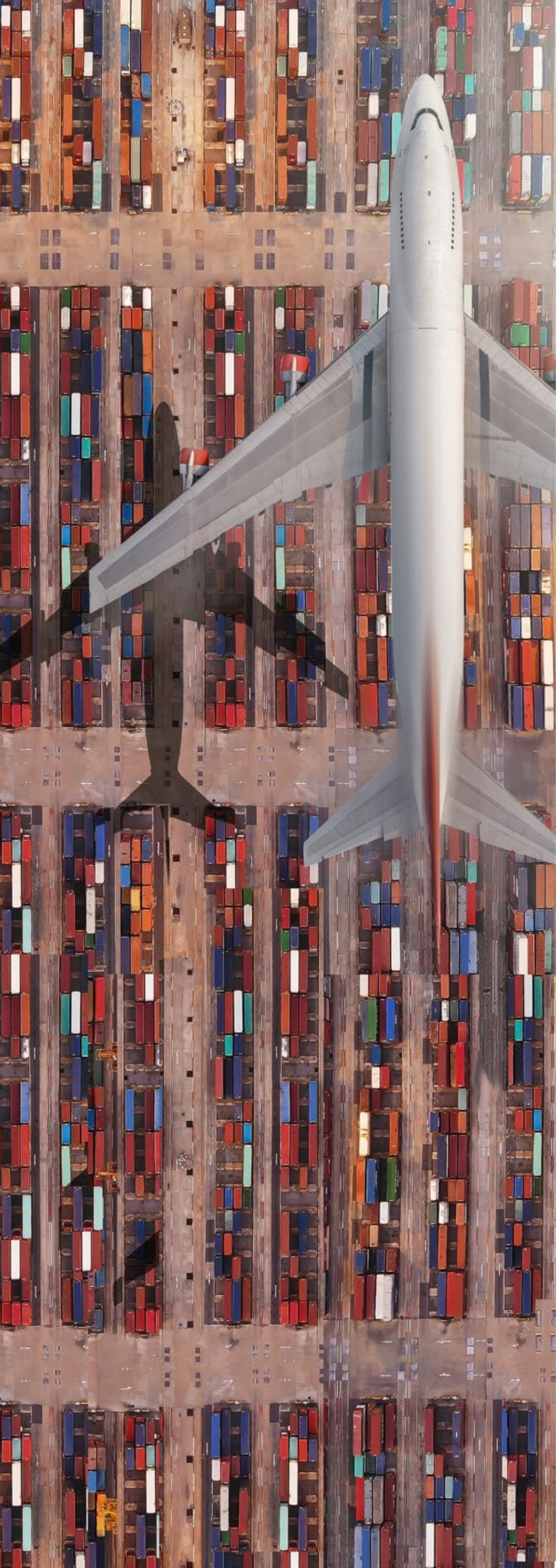


Benchmark Insights

–

IIoT cybersecurity for transportation companies

Mitigating risk and
building resilience

IBM Institute for
Business Value

How IBM can help

Connecting systems that monitor and control physical environments to the internet without securing them adequately is risky and potentially expensive. A successful cyber attack on Industrial Internet of Things (IIoT)-enabled transportation operations can have catastrophic consequences. However, many of these risks can be addressed or mitigated. IBM helps transportation industry executives manage the growing amount of attack surfaces. We bring our cognitive approach to security disciplines that help protect critical infrastructure assets and provide new services that support platforms and ecosystems. The depth of our global industry and security experts can address quality while helping protect assets and processes. IBM applies cognitive approaches to help reduce security risks. For more information, please visit ibm.com/industries/travel-transportation.

By Eric Maass, Gerald Parham, Julian Meyrick, Keith Dierkx, Lisa-Giane Fisher, and Steve Peterson

Key takeaways

Without effective security, IIoT benefits may come at a high cost

Many transportation services providers rely on IIoT solutions to manage operations, yet almost a third of their cybersecurity incidents are IIoT-related. Without adequate protection, transportation operations are vulnerable to cyber attacks that can trigger catastrophic consequences across multiple industries.

Unpatched vulnerabilities in legacy systems are a significant risk

Many industrial control systems (ICS) that enable transportation operations run on legacy systems, some with critical, unpatched software vulnerabilities. These systems often rely on IIoT devices for routing, positioning, tracking, and navigation—and to interface with public applications.

Ten controls and practices help drive IIoT cyber resilience

Our research reveals specific security controls and AI-driven practices that help companies align their prevention, detection, and response capabilities, better positioning them to quickly respond to, mitigate, and recover from IIoT-related cyber attacks.

—

Edge technologies can transform transportation operations, but introduce risk

Transportation is uniquely positioned as a conduit between business and consumers. Transportation providers rely heavily on third parties, and many industries are entirely dependent on transportation providers for continuous operations and delivery of goods and services. The global scope and integration within transportation supply chains represent a large, diversified attack surface, which makes the industry an attractive target for malicious actors.

IIoT solutions promise revolutionary changes to industry operations, particularly in managing globally distributed fleets of assets that are increasingly connected and ubiquitous. This expansion introduces operational challenges and new attack vectors. The idea of driverless semi-trucks independently navigating highways is both exciting and terrifying. As connected, autonomous, and smart devices move to production, transportation companies need to re-examine their security operations.

With increasing dependence on IIoT platforms and data services that enable insights and automation, the potential for unauthorized access to proprietary data and critical systems is growing, placing physical and digital assets at risk. As connected services and ecosystems become essential components of critical infrastructure networks, the scope of this risk extends to the entire value chain (see “Insight: Travel and transportation share critical infrastructures”).

Whether executed by financially driven cyber criminals or politically motivated nation-states, a successful attack on any segment of the transportation industry is dangerous for myriad reasons. The potential impact on public safety and the economic consequences of disruption can be particularly severe.

79%

of transportation executives say DDoS attacks are their greatest IIoT-related threat

59%

of top security performers identified in our survey have adapted their incident response plans to address compromised IIoT components, compared with 34% of other companies

2x

These top performers can detect, respond to, and recover from IIoT-related incidents and breaches at least 2X faster than other companies

Based on key IIoT cybersecurity metrics, some organizations are more cyber resilient than others. They are better at not only protecting their organizations from IIoT-related attacks, but also detecting, responding to, and recovering from breaches when they occur.

Through our research and analysis, we identified a set of ten highly effective controls and practices that are instrumental to achieving this level of performance. These controls and practices are based on Center for Internet Security (CIS) Critical Security Controls and AI-driven practices from IBM IoT security research, and we will describe them in detail throughout this report. [1]

We will also provide recommendations on how transportation companies can take three steps to implement the highly effective controls and practices to help improve IIoT cybersecurity postures and resilience:

1. Establish a strong defensive foundation for IIoT.

2. Adapt incident response and management for IIoT.

3. Enable IIoT security automation at scale.

With increasing reliance on third parties, security becomes an important layer of operational assurance and resilience.

IIoT technologies in transportation: a mixed blessing

For transportation industry providers, order to cash, inventory management, fulfillment, and logistics services form the core of the business. Many providers are successfully applying smart, adaptive technologies to decades-old industry problems in areas such as route optimization.

For more insight into the latest industry dynamics, the IBM Institute for Business Value (IBV) conducted a survey in cooperation with Oxford Economics. Our study explored how transportation providers apply IIoT technologies, how well they understand the associated cybersecurity risks, and the maturity—and effectiveness—of their capabilities to mitigate them. (See "Methodology" section on page 17.)

We interviewed information technology (IT) and operational technology (OT) executives responsible for the security of their organizations' IIoT deployments and environments. Respondents are from 300 organizations in 11 locations across the globe and include 225 from the transportation industry.

Our analysis revealed a respondent group of "top security performers" who perform better on security key performance indicators (KPIs). They are also more confident that their vulnerability management capabilities protect them from the latest threats (see "Insight: Top security performers by the numbers").

Insight: Travel and transportation share critical infrastructures

Travel and transportation providers have much in common—most notably a common backbone of critical infrastructure and facilities. They also share a set of security-specific use cases:

1. Identity. Recognize passengers, customers, employees, and partners.

2. Safety. Secure access not only to equipment and facilities, but also digital software and data stores.

3. Supply chain integrity. Impart the provenance of goods and services, and the trust this engenders.

4. Visibility and analytics. Monitor fleet assets, maintain network resilience, and understand how risks impact business operations upstream and downstream.

For transportation industry providers, the emphasis is on supply chain integrity and enhancing visibility, accountability, and efficiency—from production to fulfillment. In travel, the primary focus is on safety and consumer experience. While the use cases illustrate the common security fabric connecting travel and transportation providers, risks remain distinct: travel is consumer-centric (B2C), and transportation is business-centric (B2B).

Transportation industry providers focus on managing complicated supply chains and multiple third-party suppliers of products and services, typically in a complex regulatory environment that varies by industry and country. Communications and the exchange of data between parties are vital to routine business operations.

Risks are communal, and any threats to delivery and fulfillment capabilities can have an outsized impact on business outcomes. While little consumer data is at risk, valuable trade secrets and intellectual property are vulnerable.

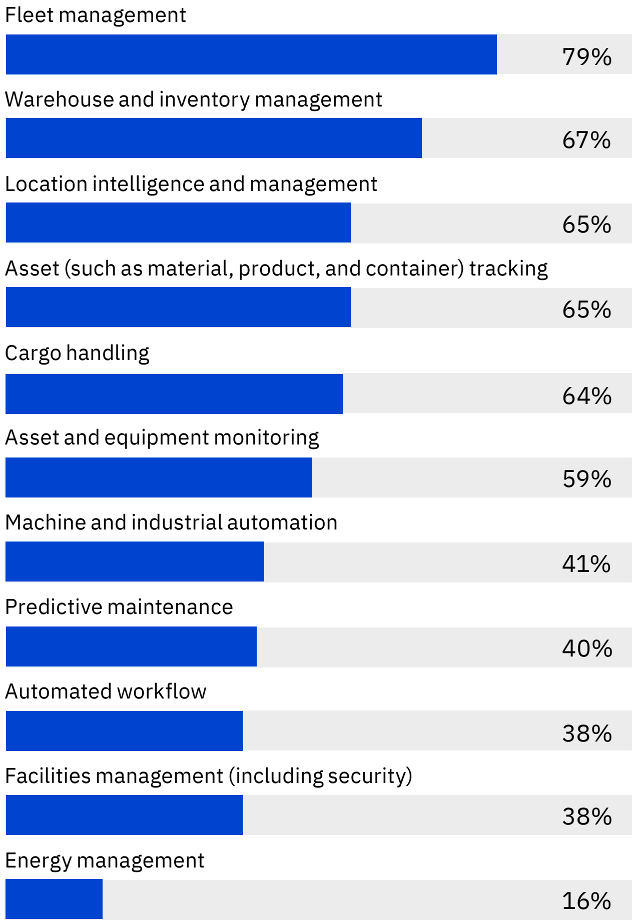
Clearly, security strategies should demonstrate how the organization approaches risk in terms of identification, encapsulation, and remediation. Because of the increasing reliance on third parties and partners, security serves as an important layer of operational assurance and resilience. As operations modernize for digital channels, security governance becomes critical to success.

Our findings confirm the rapid adoption of IIoT technologies. Fleet, warehouse, inventory, and location management are the primary use cases supported (see Figure 1).

—

Figure 1

How IIoT technologies are applied in transportation operations



Source: IBM Institute for Business Value benchmark study, 2019. Q. How is IIoT technology being applied in your organization's operations? Select all that apply.

Insight: Top security performers by the numbers

Top security performers include companies across the travel and transportation industries. Of the 300 companies surveyed, 59 fell into this group, including 36 from transportation. They are defined as being, on average, the top 20 percent of performers in three measures:

1. Percentage of cybersecurity budget represented by IIoT cybersecurity.

2. Percentage of known IIoT vulnerabilities addressed by security controls.

3. Cycle time to respond to and recover from IIoT cybersecurity incidents.

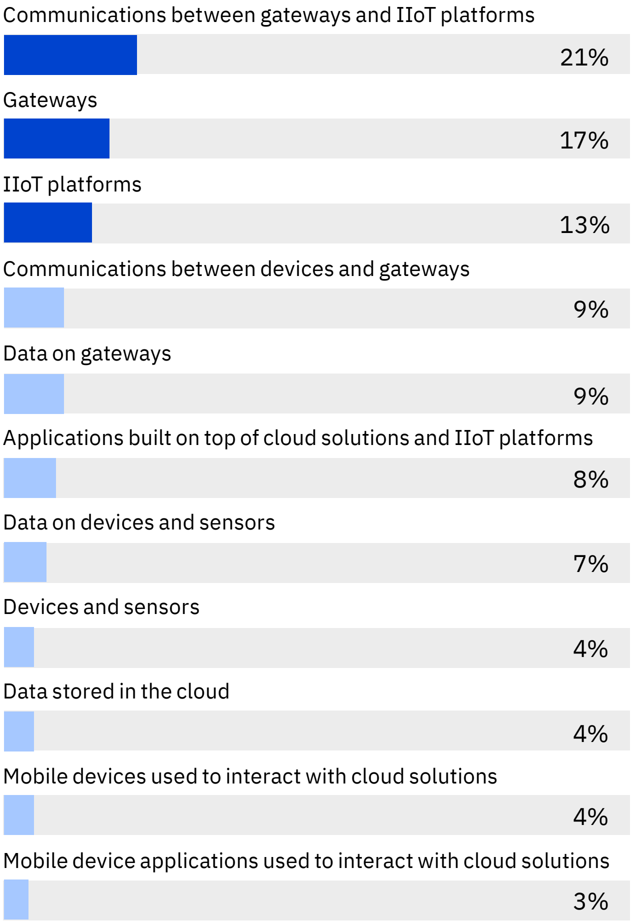
For the purposes of this study, the term “top security performers” refers to all 59 companies, including the 36 transportation companies. References to “all other companies” include the other 241 travel and transportation companies.

Transportation executives are concerned about the potentially devastating consequences of IIoT-related security breaches.

However, executives are apprehensive about the security of information flowing among their operational, corporate, and IIoT networks. They cited gateways and gateway-related connectivity as the most vulnerable IIoT components (see Figure 2).

Figure 2

Most vulnerable parts of transportation IIoT deployments



Source: IBM Institute for Business Value benchmark study, 2019. Q. What is the most vulnerable part of the IIoT solution that your company has deployed? Select one.

Transportation companies are aware that connecting systems that monitor and control physical environments to public networks, such as the internet, can introduce risks (see Figure 3). Yet only 16 percent have evaluated these risks fully and established formal IIoT cybersecurity programs to build, manage, and update the tools, processes, and skills required to mitigate them.

We asked survey respondents to evaluate various IIoT-related cybersecurity risks with a rating based on both likelihood and potential impact. The following sections explore those that most concern transportation executives:

Damage to an organization’s reputation and loss of public confidence

More than two-thirds of executives rate this risk as high or very high. In addition to potentially disrupting operations and exposing sensitive data, a successful IIoT-related cyber attack in the transportation industry can result in injury or loss of life. These outcomes can have a substantial negative impact on a company’s image and reputation. Not only can the brand’s credibility and trustworthiness be undermined, but business and customer relationships can be irreparably damaged.

Exposure of sensitive data

Twenty-one percent of executives are acutely aware that losses directly attributable to data leaks can be severe and rate data exposure as a very high risk. It is estimated that since January 2018, more than 566 million records in the transportation industry—including unencrypted passport numbers, customer payment details, and other data—have been leaked or compromised. The estimated cost to these companies is USD 60 billion.[2]

Endangerment of individuals’ safety

Forty percent of transportation executives surveyed evaluate the probability of this occurring and the impact it will have on their companies as high or very high. Altering the timing of a traffic light by even a few seconds could result in physical injuries or fatalities. Similar consequences could stem from a malicious actor tampering with mechanical or electrical devices, such as those that control railway signals. For example, a 14-year-old in Lodz, Poland, modified a TV remote control so it could be used to change railway track points. As a result, four vehicles were derailed, injuring 12 people.[3]

Operational disruptions or shutdowns

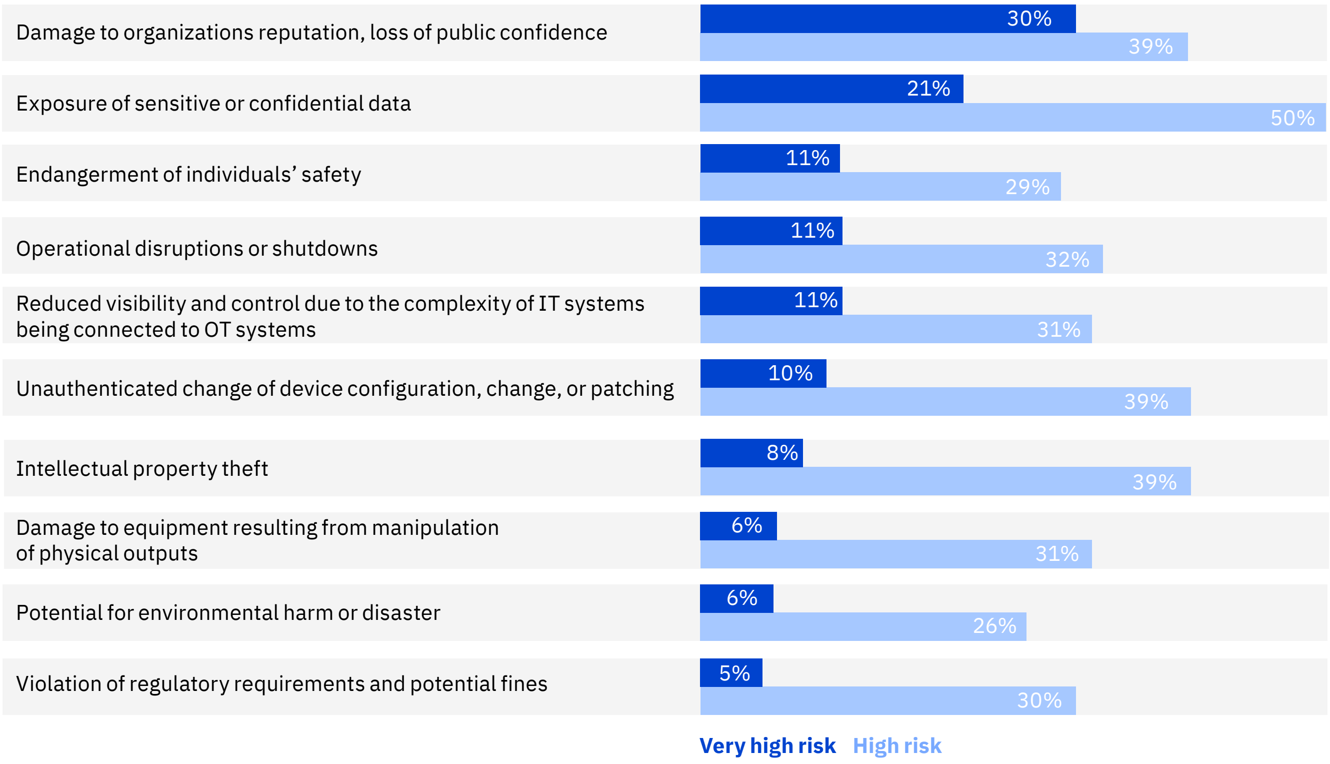
The June 2017 ransomware attack on a global shipping company is an example of the cascading effect of operational disruptions in the transportation industry. This attack caused almost 80 ports and terminals around the globe to either come to a standstill or experience significant delays. The disruption was not limited to maritime ports and container vessels: trucks destined for inland facilities were held up at ports waiting for systems to come back online so they could process and receive or deliver their shipments. This interruption delayed product distribution for extended periods. The shipping company had to rebuild a significant portion of its IT infrastructure at an estimated cost of USD 300 million.[4]

Reduced visibility and control due to the complexity of IT systems being connected to OT systems

IIoT solutions span IT, OT, and consumer technology. These systems are typically managed in silos by different teams with different areas of expertise. This makes defense against cyber attacks extremely difficult, and detection of IIoT-related incidents and intrusions a real challenge.

Figure 3

Highest-rated IIoT cybersecurity risks



Source: IBM Institute for Business Value benchmark study, 2019. Q. What is the probability that each of the following IIoT cybersecurity risks will occur at your organization, as well as the impact it will have on your organization if it were to occur? Assign a probability that the risk will occur and the impact it will have on the organization if it were to occur, where 1 = Very low, 2 = Low, 3 = Moderate, 4 = High, 5 = Very high.

A three-step approach can help improve IIoT cybersecurity postures and resilience.

Three steps to strengthen IIoT cybersecurity and resilience

We found top security performers are likely to have fully evaluated IIoT cybersecurity risks and to have a strong understanding of the cybersecurity capabilities required to mitigate them. Top security performers are also likely to regard security controls as highly effective enablers and protectors. But what truly differentiates them is their cyber resilience: they detect, respond to, and recover from IIoT-related incidents and breaches at least twice as fast as other companies.

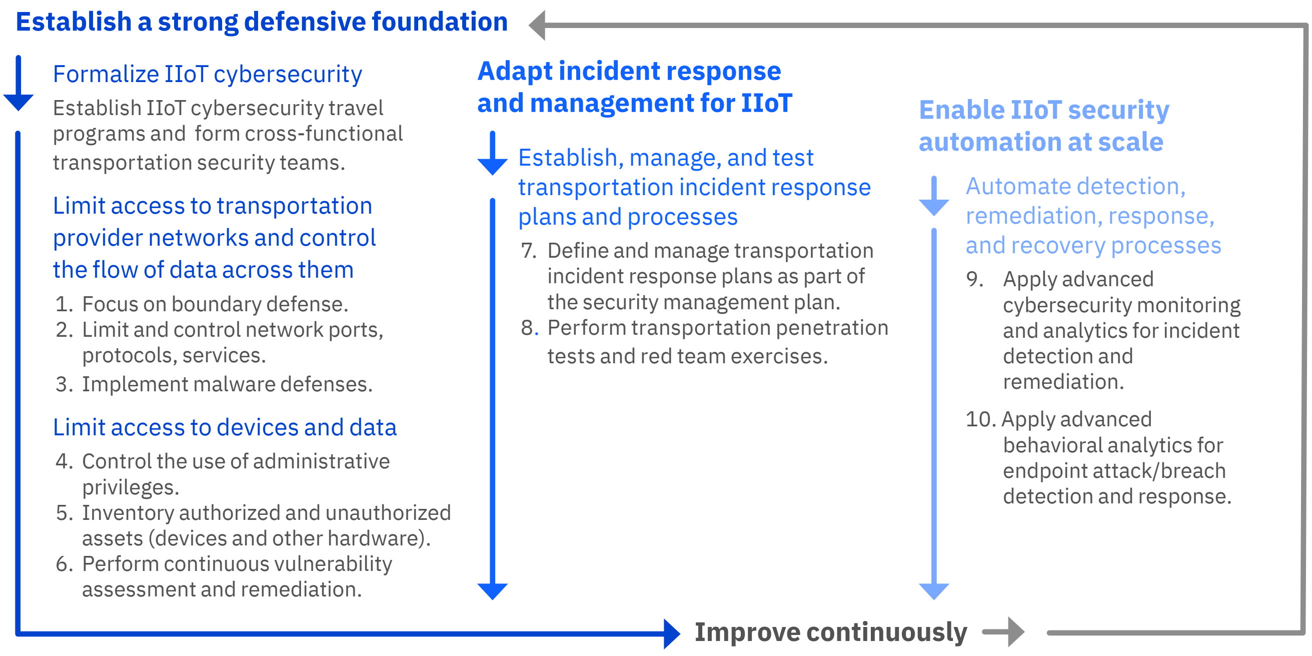
Our research indicates that this performance is strongly influenced by eight of the 20 CIS Critical Security Controls and two of the six more advanced, AI-driven practices that many transportation companies are adopting. Each of these highly effective controls and practices relates to a security function—protection and prevention, or detection, response, and recovery.

These controls and practices can be implemented in three steps (see Figure 4):

- Establish a strong defensive foundation for IIoT by defining and implementing an IIoT cybersecurity strategy and program. Then, focus on six controls and practices to help bolster protection and prevention capabilities.
- Adapt incident response and management for IIoT by using two controls to integrate IIoT cybersecurity into security operations for a more effective response to IIoT-related incidents and breaches.
- Enable IIoT security automation at scale by implementing two artificial intelligence (AI)-driven practices to automate detection and response capabilities across business units, platforms, and ecosystems.

Figure 4

A three-step process to help improve IIoT cybersecurity posture and resilience



Establish a strong defensive foundation

Formalize IIoT cybersecurity

Establish IIoT cybersecurity travel programs and form cross-functional transportation security teams.

Limit access to transportation provider networks and control the flow of data across them

1. Focus on boundary defense.
2. Limit and control network ports, protocols, services.
3. Implement malware defenses.

Limit access to devices and data

4. Control the use of administrative privileges.
5. Inventory authorized and unauthorized assets (devices and other hardware).
6. Perform continuous vulnerability assessment and remediation.

Adapt incident response and management for IIoT

Establish, manage, and test transportation incident response plans and processes

7. Define and manage transportation incident response plans as part of the security management plan.
8. Perform transportation penetration tests and red team exercises.

Enable IIoT security automation at scale

Automate detection, remediation, response, and recovery processes

9. Apply advanced cybersecurity monitoring and analytics for incident detection and remediation.
10. Apply advanced behavioral analytics for endpoint attack/breach detection and response.

Improve continuously

Incorporate new knowledge, experience, and findings and adapt as needed.

Source: IBM Institute for Business Value analysis.

Establish a strong defensive foundation for IIoT

The first step involves establishing a defensive foundation for IIoT. It begins with incorporating IIoT cybersecurity controls and practices—and their associated technologies—into an overarching IIoT security strategy. This action is followed by applying highly effective protection and prevention controls to help bolster defensive capabilities.

Establish IIoT cybersecurity programs.

This activity helps define, manage, and update required IIoT cybersecurity tools, processes, and skills. While 41 percent of top security performers have achieved this, only 15 percent of other companies have done so (see Figure 5). IIoT-related risks should be addressed as part of a transportation organization's broader security risk management framework (see "Insight: A framework to manage IIoT risk").

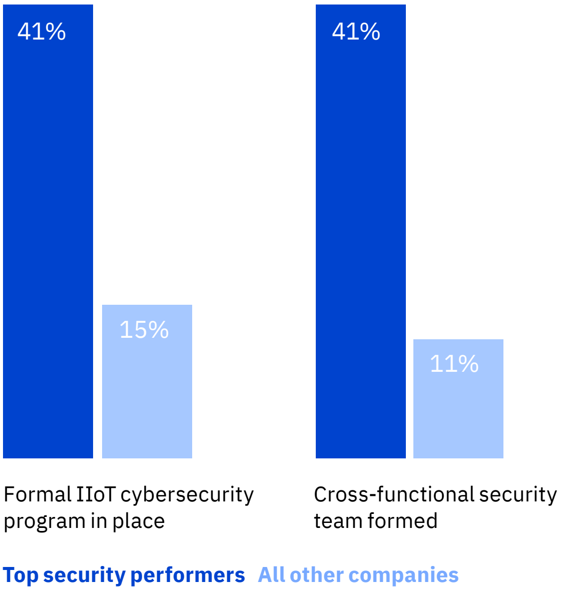
First, evaluate and prioritize risks. Then, using a common risk approach across IT and OT disciplines, make them visible and managed at an enterprise level. Perform regular risk assessments that identify vulnerabilities in IIoT environments—including connected ICS—and document and execute plans to mitigate them.

Form cross-functional transportation security teams.

Top security performers appear to understand the value of working cross functionally. Having representatives from IT security, engineering, operations, and control system and security vendors on the team helps develop a clearer understanding of the differences among IIoT systems, corporate IT systems, and operational equipment. Using IT and OT expertise supports the correct prioritization of security controls to help optimize risk mitigation.[5]

Figure 5

Formalize IIoT cybersecurity



Source: IBM Institute for Business Value benchmark study, 2019.
Q. Which description best captures your organization's understanding of IIoT cybersecurity?
Q. To what degree is your organization implementing the following operational approaches to mitigate IIoT cybersecurity risks?
Note: Figures 5-9 display responses for companies that selected 4 = Rolling out, 5 = Fully implemented.

Boundary defense has the greatest impact on IIoT cybersecurity performance.

Limit access to transportation provider networks and control the flow of data across them.

IIoT devices generate massive amounts of data that naturally flow across corporate IT and less-protected IIoT networks. Defining roles and permissions, limiting access to these networks, and controlling the flow of data across them are essential to maintaining a consistent security posture. Three highly effective controls can help:

1. Focus on boundary defense. According to our research, this control has the greatest impact on IIoT cybersecurity performance. It addresses the detection, prevention, and correction of the information flow across networks of different trust levels, with a focus on security-damaging data.

Thirty-six percent of top security performers use segregation strategies to keep IIoT components operating in their own zones or on their own separate networks (see Figure 6).[8] This practice helps mitigate the negative effect a compromised, less-trusted IIoT network could have on the more secure corporate IT network.

2. Limit and control network ports, protocols, and services. Compared to other companies in our study, more than twice as many top security performers are actively defining and enforcing the ports, protocols, and services that may be used by IIoT devices in their operational environments.

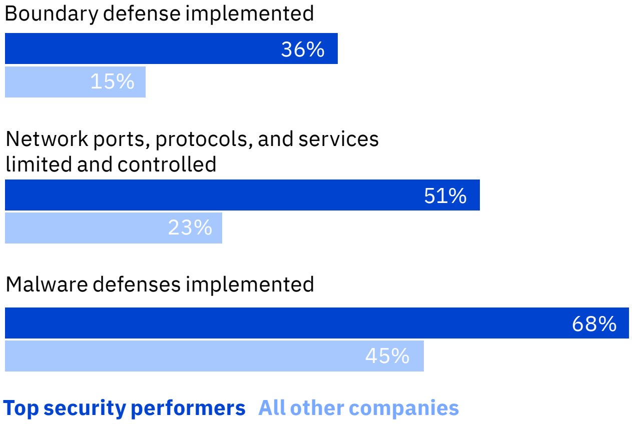
Some devices might implement communication protocols, such as Bluetooth, that do not ride on the corporate network. In such cases, fully understanding which protocols are consistent with the organization's security policies helps significantly reduce windows of vulnerability. Test IIoT devices to assess their susceptibility to messaging that does not conform to expectations.[9]

3. Implement malware defenses. Both malware and exploits are now tailored to affect IIoT devices and platforms. Build a strategy to control the installation, spread, and execution of malicious code at multiple points throughout the organization. Continuously monitor the gateways through which IIoT device information (updates and data) flows to help detect malware or to correlate observed activity with known, legitimate, and planned activity.

—

Figure 6

Limit access to networks and control the flow of data across them



Source: IBM Institute for Business Value benchmark study, 2019. Q. To what extent are you applying the following critical security controls to mitigate IIoT cybersecurity risks?

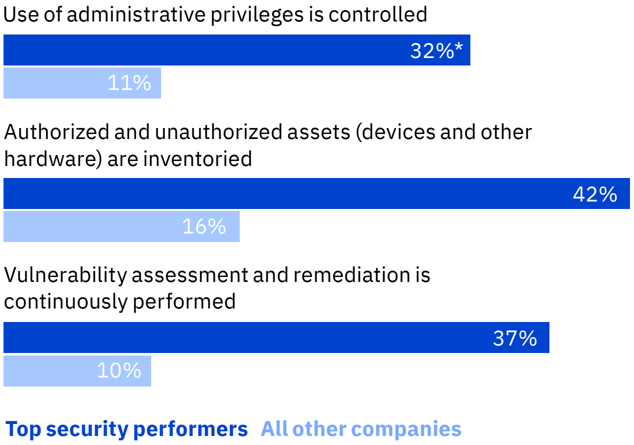
Limit access to devices and data.

Managing access to networks and the flow of data is half of the defensive equation. The other half is managing access to devices and data—in use, in motion, and at rest. Three highly effective controls can help achieve this:

4. Control the use of administrative privileges. Employees often present the greatest threat to enterprise cybersecurity, whether through ill intent or inadvertent behaviors. Because they have more access to information and key infrastructures than external malicious hackers, employees are often targeted. Top security performers are ahead in limiting privileged access, documenting who is entitled to access sensitive functions and data, and monitoring all users' activity across corporate networks (see Figure 7).

Figure 7

Limit access to devices and data



Source: IBM Institute for Business Value benchmark study, 2019.
**In all figures, low n counts (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*
Q. To what extent are you applying the following critical security controls to mitigate IIoT cybersecurity risks?

Insight: A framework to help manage IIoT risk

A combination of security and governance frameworks such as the National Institute of Standards and Technology (NIST) Framework for Critical Infrastructure Cybersecurity and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27000-1)[6] can be used as foundations to help:

- Identify critical data, assets, and security boundaries.
- Identify vulnerabilities in IIoT systems, connected production environments, and people assets.
- Build and tailor a risk management framework.
- Assess risks and then document and execute plans to mitigate them.
- Secure investment and communicate progress for the most pressing security initiatives.
- Balance acceptable risk levels with business objectives and compliance requirements.[7]

To support an effective response to IIoT-related security incidents and breaches, integrate IIoT cybersecurity into security operations.

5. Inventory authorized and unauthorized assets (devices and other hardware). Unauthorized IIoT devices and networks—examples of "shadow IIoT"—operate under the radar of organizations' traditional security policies, making them difficult to detect. One way to address this vulnerability is to identify and profile all IIoT endpoints, add them to asset inventories, and monitor them. Only provide access to authorized devices and prevent access for identified unauthorized and unmanaged devices.

6. Perform continuous vulnerability assessment and remediation. Seventy-nine percent of transportation executives told us that distributed denial-of-service (DDoS) attacks (on or by applications or devices) are their greatest IIoT-related threat. Flaws and security holes in IIoT devices and ICS (including supervisory control and data acquisition, or SCADA, systems) leave transportation companies vulnerable to botnets (for example, Mirai, Aidra, Wifatch, and Gafgyt) that can spread DDoS attack malware.[10]

Transportation executives tell us that this type of attack accounts for 35 percent of total cybersecurity incidents at their companies. Regularly schedule vulnerability assessments to help identify improperly configured IIoT devices so administrators can remove or re-configure them. Active vulnerability scanning in operational environments can destabilize systems, so if automated scanning is not applicable, perform passive monitoring.

Adapt incident response and management for IIoT

Once a defensive IIoT cybersecurity foundation is in place, the second step is to integrate IIoT cybersecurity into security operations. This action supports an effective response to IIoT-related incidents and breaches. Adopting better protection and prevention practices and making sure systems are securely developed and deployed does not guarantee the organization will not be breached. Companies must be prepared to act quickly and decisively if this occurs.

Establish, manage, and test transportation incident response plans and processes.

7. Define and manage transportation incident response plans as part of the security management plan. The majority of top security performers have adapted their incident response (IR) plans to address the course of action for compromised IIoT components (see Figure 8). Routinely testing the plan can strengthen the ability to respond. Execute breach simulations to identify processes, people, and tools to activate in the event of a breach.

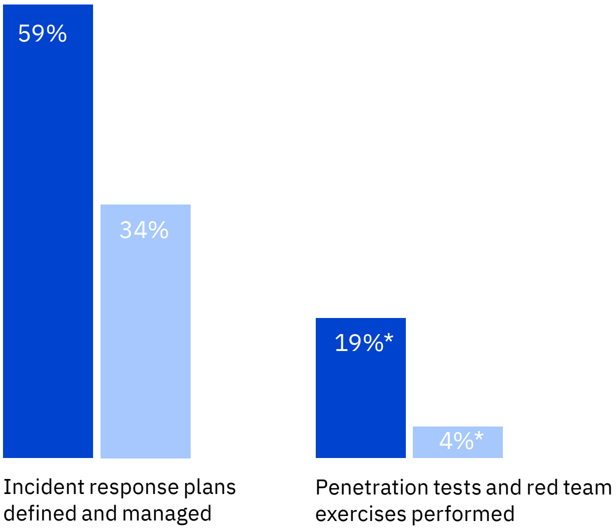
Use shared resources from within the ecosystem, such as ICS/SCADA security experts, who have specialized skills that are in short supply. Risk exposure can also be mitigated via cyber insurance policies that cover business interruption and extortion demands associated with mission-critical IIoT platforms. Few executives we surveyed reported purchasing this type of cyber insurance.

8. Perform transportation penetration tests and red team exercises. These activities can provide more detailed insights into the effectiveness of IR plans. Red teams are groups of ethical hackers that simulate cyber attacks, allowing companies to stress-test their IR plans, identify gaps, and adjust accordingly. Penetration tests help discover ad-hoc vulnerabilities and support compliance with security policies and data-privacy regulations.

We found that almost five times as many top security performers, when compared to other respondents, are implementing these offensive defense strategies (see Figure 8). In IIoT environments, errors in scanning may severely impact business operations, so it's essential to consider and address this possibility.

Figure 8

Establish, manage, and test travel incident response plans and processes



Top security performers **All other companies**

Source: IBM Institute for Business Value benchmark study, 2019. Q. To what extent are you applying the following critical security controls to mitigate IIoT cybersecurity risks?

Enable IIoT security automation at scale

In the third step of the process, deploy automated, adaptive transportation security capabilities. This step is critical because bad actors continually develop new methods for infiltrating systems. Given that essential cybersecurity skills are often in short supply, it's imperative to put automated mechanisms in place to help detect and remediate breaches.

Automate detection, remediation, response, and recovery processes. Two highly effective AI-enabled practices can support these processes:

9. Apply advanced cybersecurity monitoring and analytics for incident detection and remediation. To keep up with IIoT information in real time across operational environments, 39 percent of top security performers (versus 6 percent of other companies) have established comprehensive security telemetry capabilities. These automate the collection, integration, and analysis of data from all possible monitoring points (see Figure 9). This includes system logs, network flows, endpoint data, cloud usage, and user behavior, allowing security operations center (SOC) teams to quickly understand the surrounding context of alerts as well as differentiate between false positives and genuine alerts.

For a proactive approach, SOC teams can analyze the information extracted from internal IIoT data against externally sourced threat intelligence data. Then, machine learning can help predict attackers' next moves.

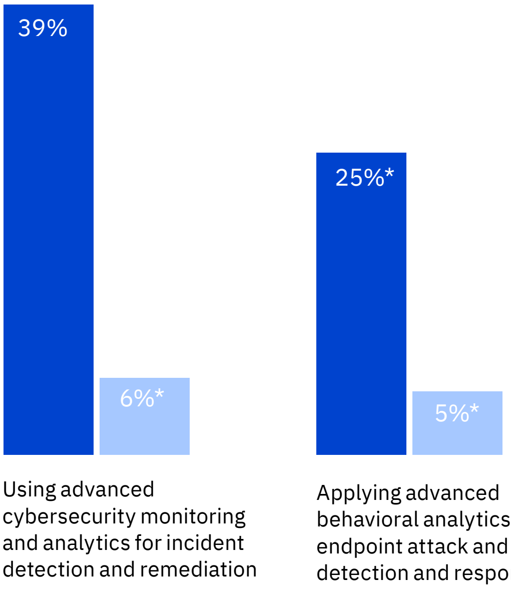
With the emergence of software services and ecosystem partner networks, integrating security governance and operations is more important than ever.

10. Apply advanced behavioral analytics for endpoint breach detection and response. AI-enabled threat detection can be applied at an enterprise level to help uncover anomalous user activities and prioritize risks. Twenty-five percent of top security performers already possess user behavior analytics that use machine learning (see Figure 9). They are also ahead in applying machine learning to automate adaptive models of what is considered "normal." This capability allows them to track these normal behavior signatures and flag unusual activity that may signal new threats.

—

Figure 9

Automate detection, remediation, response, and recovery processes



Top security performers **All other companies**

Source: IBM Institute for Business Value benchmark study, 2019. Q. To what degree has your organization implemented the following AI- and analytics-based approaches to mitigate IIoT cybersecurity risks?

Achieving IIoT resilience

Transportation companies rely on many OT systems that were designed before connected cybersecurity was a reality. In a race to achieve economies of scale, many transportation providers are adopting new technologies faster than they can secure them. With the emergence of software services and ecosystem partner networks, integrating security governance and operations is more important than ever.

The IIoT represents the convergence of IT and OT solution sets, where IT systems and networks are increasingly applied in OT environments. This trend increases complexity and introduces a unique set of risks. With an IIoT security strategy that makes security an integral part of operations, investments in IT and OT infrastructure can drive efficiency and help improve organizations' security posture and resilience.

Is your organization ready to recover from attacks on its critical infrastructure?

In what ways have you aligned IIoT security practices with your organization's enterprise risk management framework?

How are you integrating security tools and management processes into your organization's security framework and operational processes? In what ways can you maintain visibility, transparency, and accountability throughout the operational lifecycle?

How can you increase segregation to help optimize the isolation of less-secure IIoT networks?

What are your plans to bolster your incident response plan to make it easier to perform under pressure?

How are you preventing threat impacts, reducing disruption, and building capabilities to quickly recover from attacks?

Action guide

Mitigating risk and building resilience

1. First, establish a strong defensive foundation for IIoT.

Incorporate IIoT cybersecurity controls and practices, and their associated technologies, into an overarching IIoT security strategy. Then, focus on bolstering protection and prevention capabilities:

Formalize IIoT cybersecurity.

- Establish IIoT cybersecurity transportation programs.
- Form cross-functional transportation security teams.

Limit access to transportation provider networks and control the flow of data across them.

- Focus on boundary defense.
- Limit and control network ports, protocols, and services.
- Implement malware defenses.

Limit access to devices and data.

- Control the use of administrative privileges.
- Inventory authorized and unauthorized assets (devices and other hardware).
- Perform continuous vulnerability assessment and remediation.

2. Once the defensive foundation is in place, adapt incident response for IIoT.

Integrate IIoT cybersecurity into transportation security operations to help your organization respond more rapidly and effectively to IIoT-related incidents and breaches:

Establish, manage, and test transportation IIoT incident response plans and processes.

- Define and manage transportation IIoT incident response plans as part of the security management plan.
- Perform penetration tests and red team exercises to find gaps in defenses and weaknesses in planned responses.

3. Finally, scale transportation IIoT security capabilities through automation.

Bad actors continually develop new methods for infiltrating systems, and cybersecurity skills are often in short supply. Deploy automated, adaptive, responsive capabilities at scale:

Automate detection, remediation, response, and recovery processes.

- Apply advanced cybersecurity monitoring and analytics for incident detection and remediation.
- Apply advanced behavioral analytics for endpoint attack, and breach detection and response.

About the authors

Eric Maass

linkedin.com/in/ezmaass/
emaass@us.ibm.com

Eric Maass is the director of strategy and emerging technology for IBM Security Services, responsible for leading business and investment strategy across the organization's portfolio, including advanced and emerging security technologies. Mr. Maass is a security industry veteran with roughly 20 years of corporate and start-up experience across commercial, Department of Defense (DoD), and intelligence agencies. He served as founder and Chief Technical Officer (CTO) of a cloud security start-up company that was acquired by IBM in 2014. Eric is based in the greater NYC area.

Gerald Parham

linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald Parham is the Global Security and CIO Lead for the IBM Institute for Business Value. Gerald conducts research across the cyber portfolio—exploring the relationship between strategy, security operations, risk, identity, privacy, and trust. He has more than 20 years of experience in executive leadership, research, innovation, and intellectual property development. Gerald is based in Southern California.

Julian Meyrick

linkedin.com/in/julianmeyrick
julian_meyrick@uk.ibm.com

Julian Meyrick leads the Global Security Strategy Risk and Compliance and Cloud Security practices for IBM Security. Julian helps clients develop their security strategies in the context of the cyber business risks they face. He has a particular focus on advising boards on the potential business impact of cybersecurity. Julian is based in London.

Keith Dierkx

linkedin.com/in/keith-dierkx-bb510a/
kwdierkx@us.ibm.com

Keith Dierkx is the IBM Global Industry Leader for Freight, Logistics, and Rail. He has over 30 years of experience in the transportation industry, working as a senior executive, strategy consultant. He advises a number of start-ups and is the author of numerous articles focused on digital transformation. Keith is based in San Francisco.

Lisa-Giane Fisher

linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa-Giane Fisher is the Benchmarking Leader for the IBM Institute for Business Value in the Middle East and Africa. She is responsible for mergers and acquisitions and security benchmarking, and she also collaborates with IBM industry experts to develop and maintain industry process frameworks. Lisa is based in South Africa.

Steve Peterson

linkedin.com/in/stevenjohnpeterson
steve.Peterson@us.ibm.com

Steve Peterson is the global Travel and Transportation lead for the IBM Institute for Business Value. He is the author of numerous industry studies and has served as a strategy consultant to the industry since 1998. Steve's work has been embraced by IBM clients around the globe, and widely praised in the industry and popular press. Steve is based in Denver.

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.

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 monthly 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.

Methodology

In cooperation with Oxford Economics, the IBV surveyed 300 IT and OT leaders responsible for the security of their organizations' IIoT environments and deployments, including 75 from travel and 225 from transportation companies. All of the companies surveyed have deployed IIoT applications to support supply chain and logistics processes.

Respondents include C-suite executives (CEOs, CTOs, CISOs, CSOs, COOs, and CROs), IT directors and vice presidents, and line-of-business and internal audit managers from all major geographies except the Middle East and Africa.

Industries represented are deep sea, coastal, and great lakes water transportation; general freight trucking; rail transportation; non-scheduled air transportation; and scheduled air transportation. Each transportation mode (land, air, and water) represents a third of the total sample.

To determine what makes some companies more secure and cyber resilient, we benchmarked their IIoT cybersecurity performance and maturity using an online survey in two parts.

In the first part, we asked about organizations' capabilities to identify and protect themselves from IIoT-related cybersecurity risks and their ability to detect, respond to, and recover from incidents. In the second part of our survey, we collected cost, cycle-time, quality, and efficiency metrics to measure the effectiveness of risk and incident management capabilities.

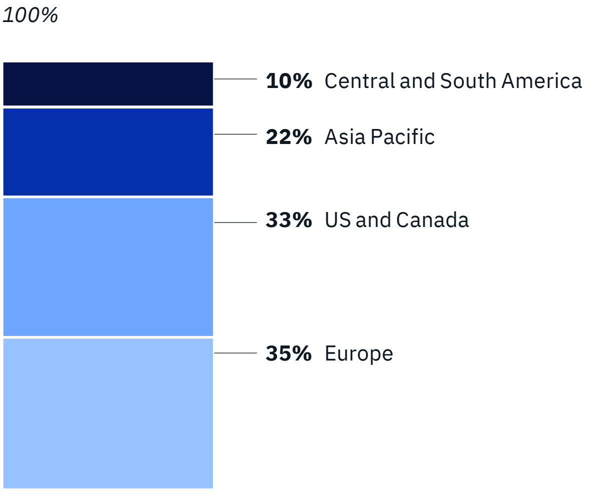
We analyzed the responses in two parts. First, we calculated an average score for each company across three key performance indicators (KPIs):

- Percentage of cybersecurity budget represented by IIoT cybersecurity.
- Percentage of known IIoT vulnerabilities addressed by security controls.
- Cycle time to respond to and recover from IIoT cybersecurity incidents.

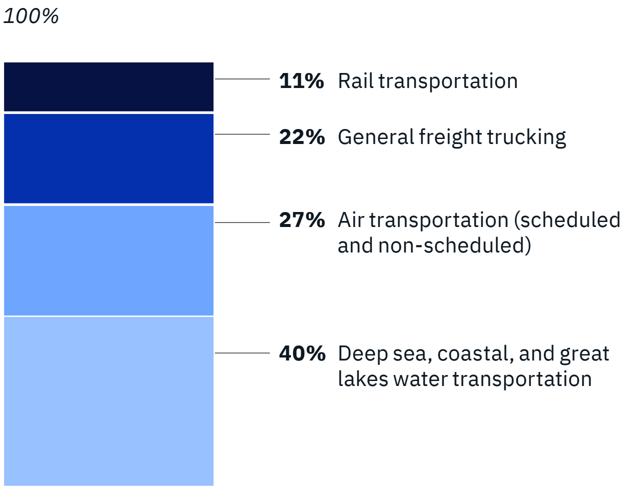
This methodology allowed us to identify the top security performers as those performing in the 80th percentile.

Second, to understand which of the 20 CIS Critical Security controls and six AI-driven practices have the greatest influence on KPIs, we performed regression analysis to create a list of all 26 elements ranked in terms of influence. The top ten are those with an above-average influence. All data, financial or otherwise, is self-reported.

Respondents by region



Respondents by type



Related reports from the IBM Institute for Business Value

Securing the Internet of Things (IoT) for industrial and utility companies
ibm.biz/iotthreats

Electronics Industrial IoT cybersecurity: As strong as its weakest link
ibm.biz/electronicsiiot

Mitigating security risks in the automotive industrial Internet of Things: quick to implement, slow to secure
ibm.biz/autoiiot

Mind the utilities cybersecurity gap: Move from pieced together to peace of mind
ibm.co/utilitiesiiot

Notes and sources

1 CIS Controls." Center for Internet Security. https://www.cisecurity.org/controls/

2 Caleb Barlow. "Why Cybercriminals Are Targeting Travel and Transportation." IBM Security Intelligence. July 10, 2019. https://securityintelligence.com/posts/why-cybercriminals-are-targeting-travel-and-transportation/

3 Shelley Smith. "Teen Hacker in Poland Plays Trains and Derails City Tram System." In Homeland Security. February 12, 2008. https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/

4 John Callon. "Cyber pirates targeting logistics and transportation companies." Cyren Security. May 14, 2018. www.cyren.com/blog/articles/cyber-pirates-targeting-logistics-and-transportation-companies

5 Tim Hahn, 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/

6 "National Institute of Standards and Technology (NIST) Risk Management Framework." NIST Computer Security Resource Center website. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview; "NIST Special Publication 800-series General Information." NIST Information Technology Laboratory. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information." International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

7 Steven Dougherty, Cristene Gonzalez-Wertz, Lisa-Giane Fisher, and Mark Holt. "Mind the utilities cybersecurity gap - Move from pieced together to peace of mind." IBM Institute for Business Value. January 2019. https://www.ibm.com/thought-leadership/institute-business-value/report/utilitiesiiot

8 "CIS Controls Internet of Things Companion Guide." Center for Internet Security. July 27, 2019. https://www.cisecurity.org/white-papers/cis-controls-internet-of-things-companion-guide/

9 Ibid.

10 "2019 IBM X-Force Threat Intelligence Index." IBM Security, 2019. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/finalibmthreatintelligenceindex022619127023627usen.pdf

11 Francis Knott. "The Threat of Cybercrime for State and Local Transportation Systems." Attila Security. November 5, 2018. https://attilasec.com/blog/transportation-systems-cybercrime/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2020

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.