Benchmark Insights

IIoT cybersecurity for travel companies

Protecting travel operations

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 cyberattack in IoT-enabled travel operations can have catastrophic consequences. However, many of these risks can be addressed or mitigated. IBM helps travel 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 Lisa-Giane Fisher,
Greg Land, Eric Maass,
Julian Meyrick, Gerald Parham,
and Steve Peterson

Key takeaways

IIoT benefits can come at a high cost
Many travel providers rely on Industrial Internet of Things (IIoT) solutions to manage complex operations, yet one third of cybersecurity incidents at travel companies are IIoT related. Without adequate protection, travel operations are vulnerable to cyber attacks that can trigger catastrophic consequences.

Unpatched vulnerabilities in legacy systems are a signicant risk
Many travel companies are dependent on older industrial control systems, some with critical software vulnerabilities. Because they are difficult to update, these systems are inherently unsecure, yet firms connect IIoT devices to them for operational applications, including some used by travelers.

Ten controls and practices help improve 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.

—

While global travel and travel workforces have been reduced as a result of the COVID-19 crisis, threat activity against the aviation sector has not. A case in point is a March 2020 data breach disclosed by the San Francisco International Airport. Reportedly, the attack was perpetrated by Russia's state-sponsored hacking group Dragonfly.[1] This group typically targets organizations in critical infrastructure sectors with the objectives of reconnaissance, lateral movement, and cyber espionage.[2]

Sustaining and securing critical infrastructures – such as those shared by travel and transportation companies – have always been challenges. The addition of COVID-19-related concerns has strained companies' security, resiliency, and continuity plans to their limits. While the industry will recover from COVID-19, it may never be immune to cyber attacks. Overcoming this global challenge requires adaptability and innovative security and risk management practices.

The travel industry is an attractive target for malicious actors. The reliance on information technology (IT) to facilitate operations, the ubiquitous need for integration of third-party vendors, and the global scope and integration of the travel supply chain represent a large, diversified attack surface.

As the industry has become more dependent on IIoT platforms and data services that enable automation, new vulnerabilities have appeared. Use of these platforms and services increases the potential for unauthorized access to proprietary data and critical systems that can disrupt physical assets. Whether executed by financially motivated cybercriminals or politically motivated nation-states, a successful attack on a segment of the travel industry can result in severe cascading effects that can influence aggregate travel demand and, thus, the entire global economy.

As attack vectors multiply, and critical vulnerabilities are exploited in short order, risks grow exponentially — often rapidly and without precedent. One factor that made the 9/11/2001 attacks in the United States so devastating was the assailants' ability to evade multiple safety and security protocols, compounded by the orchestration of multiple attack vectors simultaneously. The property damage alone amounted to nearly USD 100 billion, and estimates of the total economic damage range up to USD 2 trillion.[3]

68%

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

59%

of security leaders have adapted their incident response plans to address the course of action for compromised IIoT components compared to only 34% of other companies

2x

Security leaders are able to detect, respond to, and recover from IIoT-related incidents and breaches at least 2X faster than other companies.

As ecosystems multiply, companies become even more vulnerable. And continued innovation across the industry makes it likely the travel ecosystem will continue to expand and evolve. To prepare for the future, travel organizations should focus on improving their cyber resilience today.

Our research and analysis reveal ten security controls and AI-driven practices that can positively impact IIoT cybersecurity performance. They are a combination of Center for Internet Security (CIS) Critical Security Controls and AI-driven practices from IBM IoT security research.[6] In this report, we provide recommendations on how travel companies can implement them as part of a two-phase approach to help improve their IIoT cybersecurity postures and resilience:

Phase 1: Establish a strong defensive foundation by defining and implementing an IIoT cybersecurity strategy and program and then focusing on highly effective protection and prevention controls and practices.

Phase 2: Enable travel security automation at scale by applying highly effective detection, response, and recovery controls, as well as practices to build and test automated response capabilities.

The travel industry is an attractive target for malicious actors.

IIoT technologies in travel: a mixed blessing

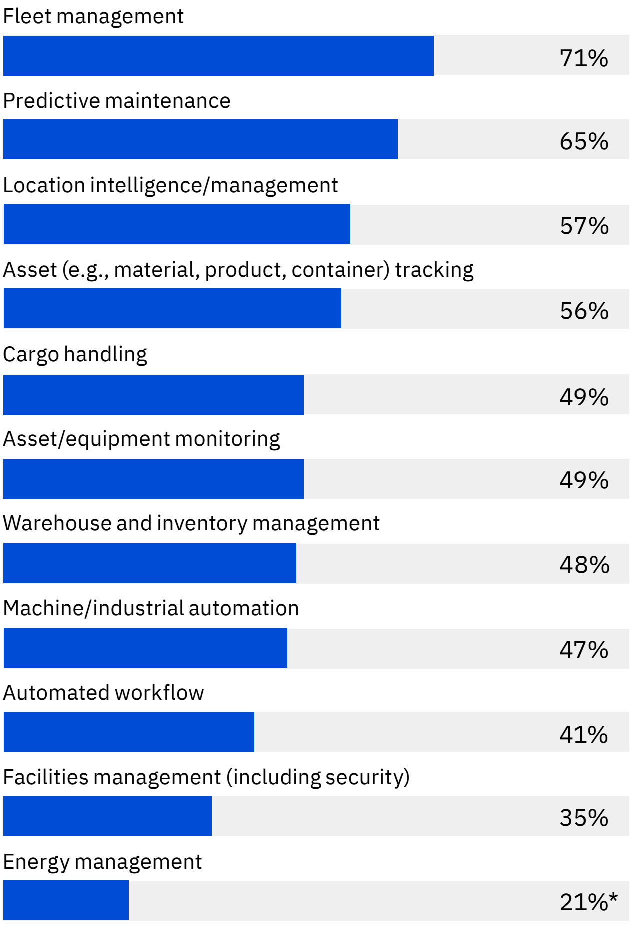
Travel companies are applying IIoT technologies extensively throughout their operations. Examples abound, crossing virtually every aspect of airline and ground transportation operations, as well as the sales, marketing, and customer service aspects of many travel agencies, tour operators, and associated travel intermediaries. Less clear is how well these travel organizations understand the associated cybersecurity risks and the maturity – and effectiveness – of the capabilities in place to mitigate them.

To better understand what makes some organizations more secure and cyber resilient than others, the IBM Institute for Business Value (IBV), in cooperation with Oxford Economics, surveyed IT and operational technology (OT) leaders from 300 travel and transportation organizations in 11 locations across the globe, 75 of which are from the travel industry. Leaders interviewed are responsible for the security of their organizations' IIoT deployments and environments (see the "Study approach and methodology" section).

Our findings confirm the rapid adoption of IIoT technologies in a wide variety of functional areas. Many companies are applying these technologies in their supply chain and logistics processes – for fleet management, predictive maintenance, and location management (see Figure 1).

Figure 1

How IIoT technologies are applied in travel operations



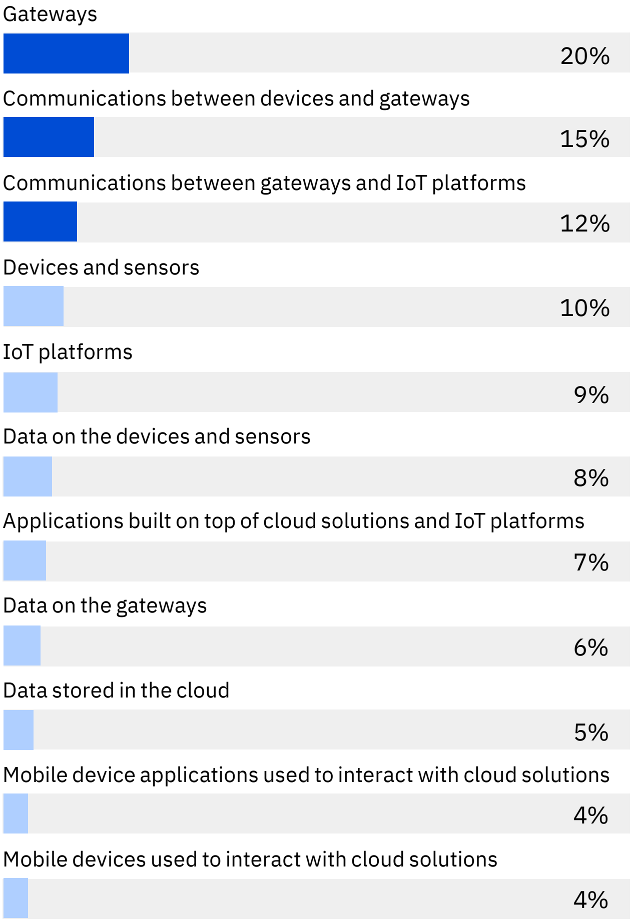
Source: IBM Institute for Business Value benchmark study, 2019.
**For all figures, asterisk denotes low n-counts (n<20), which are statistically unreliable but can be considered directional when compared to remaining respondents.*
Q: How is IoT technology being applied in your organization's operations? Select all that apply.

Many travel companies continue to deploy IIoT technologies faster than they can secure them.

However, executives are apprehensive about the security of information flowing between their operational, corporate IT, and IIoT networks. Gateways and gateway-related connectivity represent almost half of the most vulnerable IIoT components reported by travel companies (see Figure 2).

Figure 2

Most vulnerable parts of travel IIoT deployments



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

Connecting systems that monitor and control physical environments to public networks like the internet can introduce risks, especially when those systems are not secured in accordance with a broader security governance policy. Potential risks include impacts to individuals related to data leakage and erosion of consumer trust.

While travel companies may be aware of the risks, many continue to deploy IIoT technologies faster than they can secure them. The resulting gaps in configuration and control can be exploited. Almost two thirds of surveyed executives say they have, at a minimum, the capabilities to provide new IIoT-enabled offerings and services, yet only half say they can do so in a secure manner. These findings underscore the risks that arise from gaps in securing operational infrastructure.

We asked survey respondents to evaluate various cybersecurity risks with a rating based both on likelihood and potential impact (see Figure 3). The following sections explore some of the risks that most concern travel executives:

Exposure of traveler data

Travel executives rate the exposure of traveler data as one of their top two IIoT cybersecurity risks. In addition to being a public relations liability, data breaches can be a significant financial liability.

For example, in 2019, a large airline was fined USD 230 million in connection with a data breach that violated the General Data Protection Regulation (GDPR) and affected 500,000 customers. Due to poor security controls, a variety of personal information was compromised, including log in, payment card, and travel booking details, as well name and address information. The fine, which represented 1.5 percent of the airline’s total annual revenue, was the highest that the UK Information Commissioner’s Office had ever levied on a company over a data breach.[7]

Damage to travel brands and erosion of public confidence

In addition to the potential for data exposure and operational disruption, a successful travel industry cyber attack can result in injury and loss of life. The negative impact to a company’s reputation could be irreversible.

Not only is the credibility and trustworthiness of the brand undermined with current customers, prospective business and customer relationships are irreparably damaged. Perhaps unsurprisingly, respondents cite the impact on brand and public confidence as one of their two greatest IIoT-related risks.

Theft of intellectual property (IP)

Many travel companies have invested heavily in building brand assets and proprietary intellectual property to differentiate themselves. Trademarks, geographical indications (certification marks, collective marks, or sui generis system), industrial designs, and other forms of IP such as patents, copyrights, and trade secrets are sources of competitive advantage. Travel executives recognize the impact IP theft can have on their future growth, citing it as their third highest IIoT security risk.

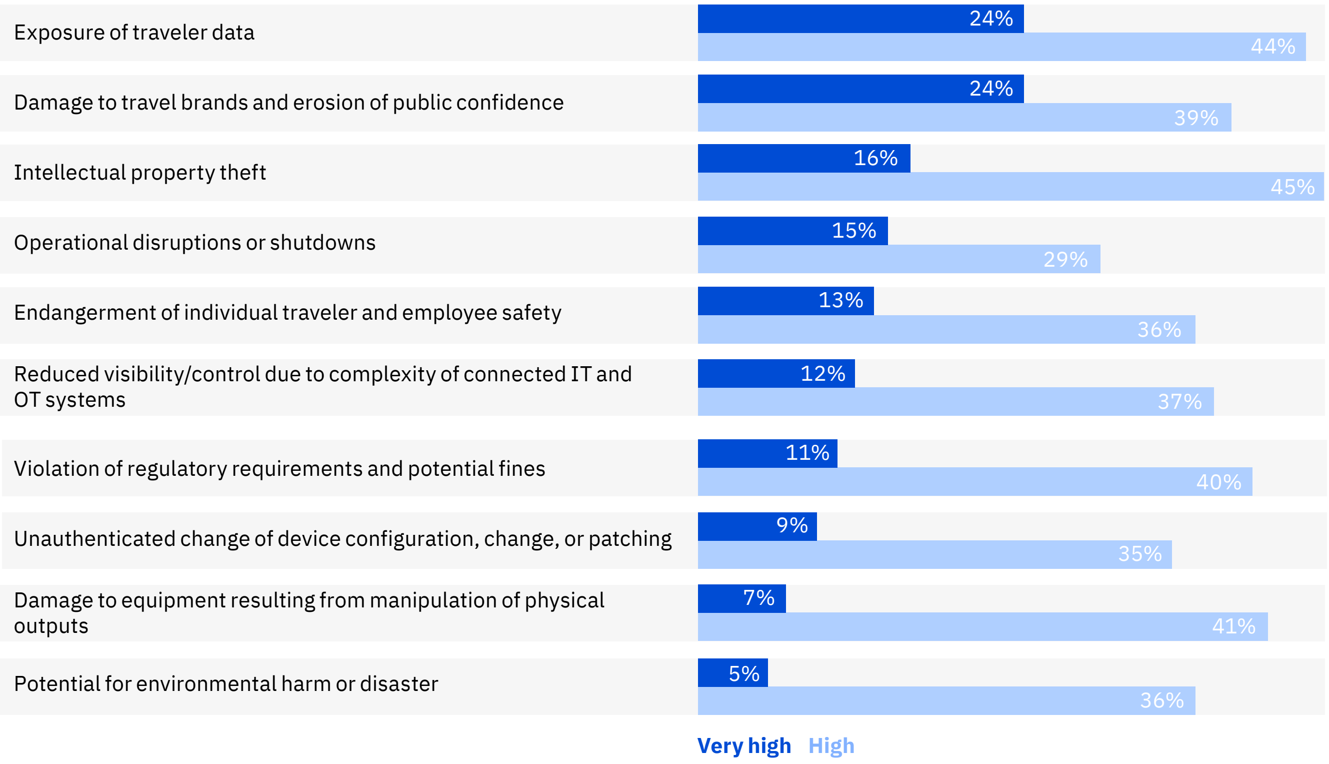
Operational disruptions or shutdowns

Fifteen percent of travel executives view operational disruptions as a very high risk. In 2016, the light rail system in San Francisco suffered a malware attack. Agency email and back-office computer systems were commandeered by hackers demanding bitcoin in exchange for captured agency data.[8]

—

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 IoT cybersecurity risks will occur at your organization, as well as the impact it would have on your organization if it were to occur? Assign a probability and an impact of 1 to 5 to each risk, where 1 = Very low, 2 = Low, 3 = Moderate, 4 = High, 5 = Very high.

The city of Atlanta's department of transportation was also subject to a ransomware attack that disrupted services over a period of several months and cost USD 2.6 million in recovery efforts.[9] And for logistics operators, an entire fleet of trucks can be paralyzed by a virus attacking routing systems.

Endangerment of individual traveler and employee safety

Thirteen percent of travel executives say traveler and employee exposure to danger is a very high risk. Altering the timing of a traffic light by even a few seconds could result in physical injury or fatalities. Similar consequences could stem from the tampering of mechanical or electrical devices such as those controlling railway signals.

For example, a Polish 14-year-old in Lodz modified a TV remote control into a device he used to change railway track points. As a result, four vehicles were derailed, injuring twelve people.[10]

A two-phase approach for improving IIoT security

Using our survey data, we identified a group of companies we deem "security leaders" based on their IIoT cybersecurity budgets, known vulnerabilities addressed by security controls, and response and recovery times (see sidebar "Insight: Security leaders by the numbers"). We found security leaders more likely to have fully evaluated IIoT cybersecurity risks and to have a strong understanding of the cybersecurity capabilities required to mitigate them.

These companies perform better on security KPIs and are more confident that their organizations' vulnerability management capabilities protect them from the latest threats. They are also more likely to regard security controls as highly effective enablers and protectors.[11] But what truly differentiates security leaders is their cyber resilience: they are able to detect, respond to, and recover from IIoT-related incidents at least twice as fast as other companies.

Insight: Security leaders by the numbers

Security leaders include companies across the travel and transport industries. Of the 300 companies surveyed, 59 fell within this group, including 23 from travel. 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 "security leaders" refers to all 59 companies, including the 23 travel companies. References to "all other companies" include the other 241 travel and transport companies.

We recommend a two-phase approach to help improve IIoT cybersecurity postures and resilience.

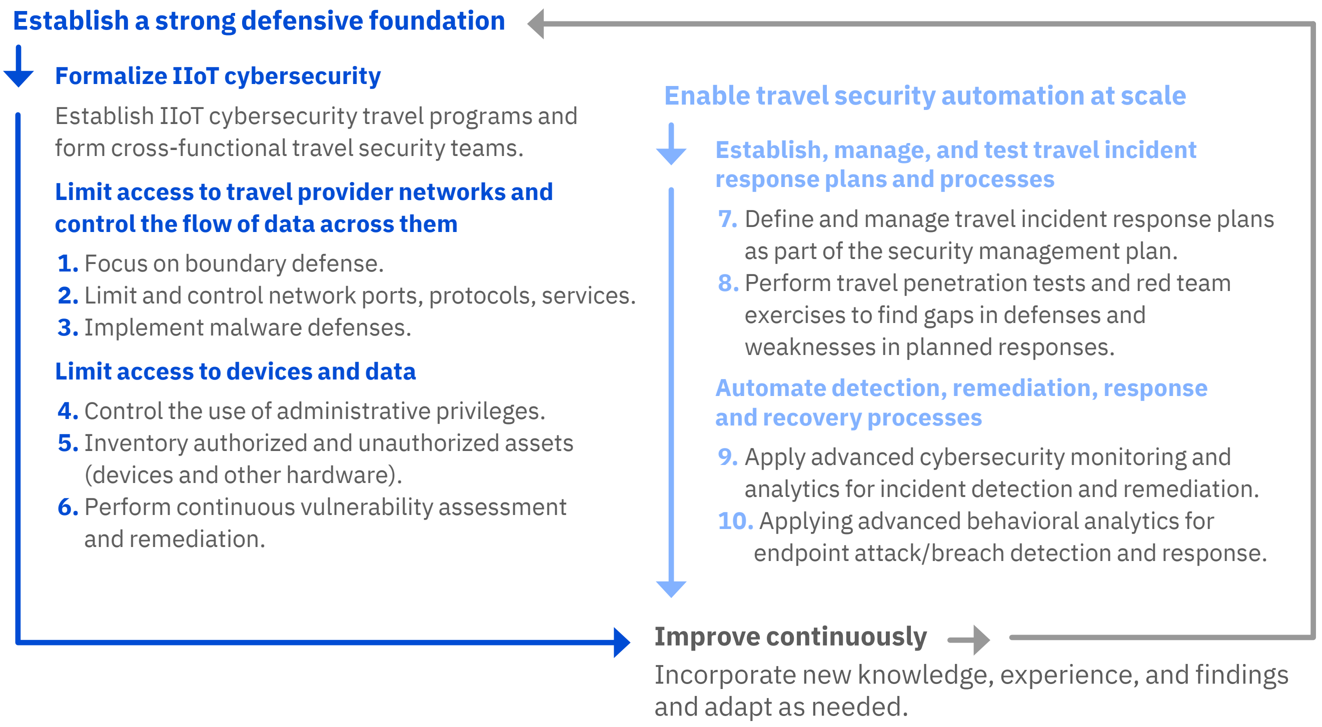
Our research indicates that this performance is strongly influenced by adherence to a combination of Center for Internet Security (CIS) Critical Security Controls and more advanced, AI-driven practices that many travel companies are adopting.[12] There are ten in total, and each relates to a security function: protection and prevention or detection, response, and recovery. We recommend implementing these highly effective controls and practices as part of a two-phase approach to help improve IIoT cybersecurity postures and resilience (see Figure 4).

Establish a strong defensive foundation for IIoT

The first phase consists of three directives. The first facilitates the establishment of an IIoT cybersecurity strategy and plan that should be aligned with the organizations' broader IT and OT risk and security frameworks. The second and third directives guide the application of highly effective protection and prevention controls and practices – and their associated technologies – to bolster defensive capabilities.

Figure 4

A two-phase approach 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 travel security teams.

Limit access to travel 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.

Enable travel security automation at scale

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

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

Automate detection, remediation, response and recovery processes

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

Improve continuously

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

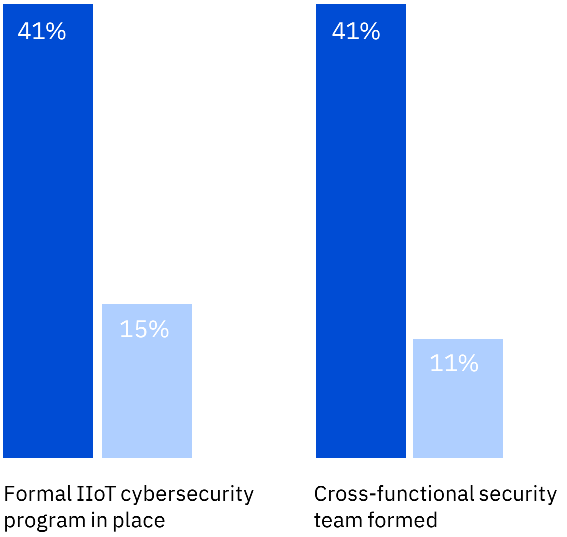
Source: IBM Institute for Business Value analysis.

Formalize IIoT cybersecurity.

An effective IIoT cybersecurity travel program enables travel companies to define, manage, and update required IIoT cybersecurity tools, processes, and skills. While 41 percent of security leaders have established these programs, only 15 percent of other companies have done so (see Figure 5). IIoT-related risks should be addressed as part of a travel organization's broader security risk management framework (see sidebar "Insight: A framework to manage IIoT risk"). First evaluate and prioritize risks. Then make them visible to and managed at an enterprise level using a common risk approach across IT and OT disciplines. Perform regular risk assessments that identify vulnerabilities in IIoT environments, including connected ICS. Document and execute plans to mitigate them.

Figure 5

Formalize IIoT cybersecurity



Security leaders **All other companies**

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

Insight: A framework to 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 ISO/IEC 27000-1, can be used as foundations to:

- 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.[13]

Malware is now tailored to affect IIoT devices and platforms.

Forty-one percent of security leaders appear to understand that working cross functionally can help travel organizations develop a clearer understanding of the differences between IIoT systems, corporate IT systems, and operational equipment (see Figure 5). By forming cross-functional travel security teams that have representation from IT security, engineering, operations, and control system and security vendors, travel companies can leverage IT and OT expertise to enable correct prioritization of security controls for optimal risk mitigation.[14]

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

IIoT devices generate massive amounts of data that naturally flow across corporate 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 highest impact on IIoT cybersecurity performance. It addresses the detection, prevention, and correction of the flow of information across networks of different trust levels – with a focus on security-damaging data. Compared to other companies, twice as many security leaders use segregation strategies to keep IIoT components operating in their own zones or on their own separate networks (see Figure 6).[15] This practice helps mitigate the negative effect a less-trusted IIoT network could have on the more secure corporate IT network.

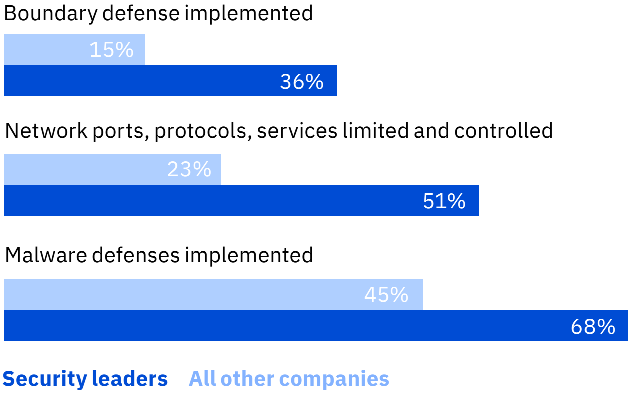
2. Limit and control network ports, protocols, and services. Compared to other companies in our study, more than twice as many security leaders are actively defining and enforcing the ports, protocols, and services that may be used by IIoT devices in their operational environments (see Figure 6). Because some devices might implement communication protocols, such as Bluetooth, that do not ride on the corporate network, fully understanding the protocols employed by each device – namely which protocols are consistent with the organization's security policies – can help significantly reduce windows of vulnerability. Test IIoT devices to assess their susceptibility to messaging that does not conform to expectations.[16]

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 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 IoT cybersecurity risks?

Employees with access to critical systems are often targets for malicious hackers.

Limit access to devices and data.

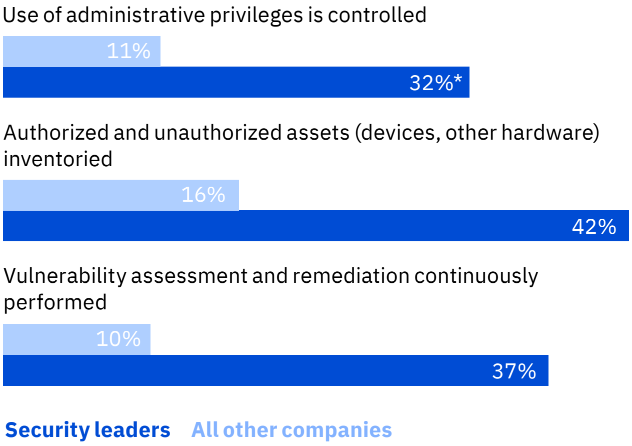
Managing access to networks and the flow of data is one half of the defensive equation. The other half is managing access to devices and data – in use, in motion, and at rest. Three highly effective security controls can help achieve this.

4. Control the use of administrative privileges. Employees with access to critical systems often present the single greatest threat to enterprise cybersecurity, whether through ill intent or inadvertent behaviors. Because they have much more access than external malicious hackers – to information and key infrastructures – these employees are often targeted. Security leaders stand apart in maintaining control frameworks around access to sensitive data to combat these types of attacks (see Figure 7).

—

Figure 7

Limit access to devices and data



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

Effective security programs limit privileged access, document who has entitlements to access sensitive functions/data, and monitor the activity of all users across corporate networks. A particular risk for the travel industry is the use of shared accounts by technicians who administer IIoT devices. The deployment of IIoT assets in insecure areas constitutes another risk. To enhance control throughout the operations lifecycle, consider more adaptive methods, such as restricting physical access; limiting administrative privileges; and providing more granular, role-based permissions.[17]

5. Inventory authorized and unauthorized assets (devices and other hardware). Twenty-eight percent of travel executives say visibility of unmanaged assets and devices is one of the greatest challenges to securing their IIoT deployments. Unauthorized IIoT devices and networks – examples of "shadow IIoT" – operate under the radar of organizations' traditional security policies, making them difficult to detect.

Identifying and profiling all IIoT endpoints, adding them to asset inventories, and monitoring them are ways to address this. Only provide access to authorized devices, and prevent access for identified unauthorized and unmanaged devices.

6. Perform continuous vulnerability assessment and remediation. Flaws and security holes in IIoT devices and industrial control systems – including supervisory control and data acquisition (SCADA) systems – leave travel companies vulnerable to botnets (for example, Mirai, Aidra, Wifatch, and Gafgyt) that spread distributed denial of service (DDoS) attack malware.[18] Travel executives tell us that DDoS attacks account for 33 percent of total cybersecurity incidents at their companies. Sixty-eight percent of our respondents cite these attacks as their greatest IIoT-related threat.

Regularly schedule vulnerability assessments to identify improperly configured IIoT devices, allowing administrators to remove or re-configure them. Active vulnerability scanning in operational environments can destabilize systems. If automated scanning is not applicable, perform passive monitoring.

Enable travel security automation at scale

Once a defensive IIoT cybersecurity foundation is in place, you can build upon it in the next phase by following two directives. They include the remaining four highly effective detection, response, and recovery controls and practices that support the deployment of automated, adaptive responsive capabilities.

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

Technologies and processes that enable a fast, dynamic, and orchestrated response to incidents and breaches are vital. The following highly effective organizational controls address the process side:

7. Define and manage travel incident response plans as part of the security management plan. Fifty-nine percent of security leaders have adapted their incident response plans (IR) to address the course of action for compromised IIoT components, compared to only 34 percent of other companies (see Figure 8). IR teams that test the plan routinely strengthen the ability to respond further.

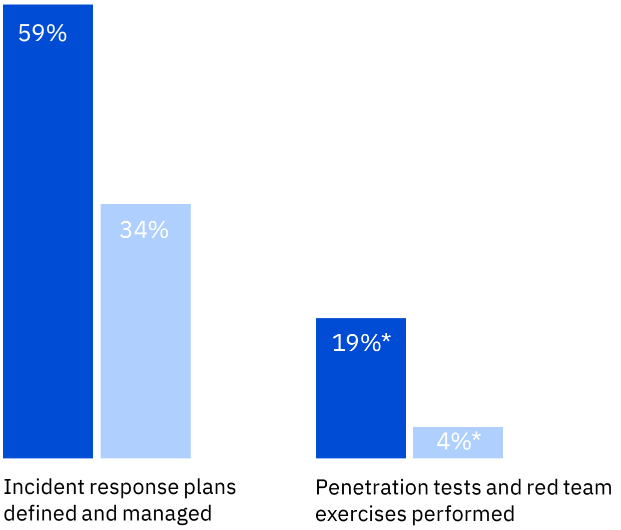
Execute breach simulations to help identify which processes, people, and tools to activate in the event of a breach. Use shared resources from within the ecosystem, such as ICS/ SCADA security experts who have specialized skills that are in short supply. Companies can also mitigate risk exposure via cyber insurance policies covering business interruption and extortion demands associated with mission critical IIoT platforms. However, our survey revealed few travel companies have purchased cyber insurance.

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

We found 19 percent of security leaders are implementing these offensive defense strategies versus only 4 percent of other companies (see Figure 8). In IIoT environments, errors in scanning may severely impact business operations, so this must be considered and addressed.

Figure 8

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



Security leaders **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 IoT cybersecurity risks?

Automate detection, remediation, response, and recovery processes

Adopting better protection and prevention practices is not a guarantee of absolute protection. Bad actors continually develop new methods for infiltrating systems. Given critical cybersecurity skills are often in short supply, automated mechanisms must be in place to detect and remediate breaches. Following are two highly effective AI-enabled practices that can support this:

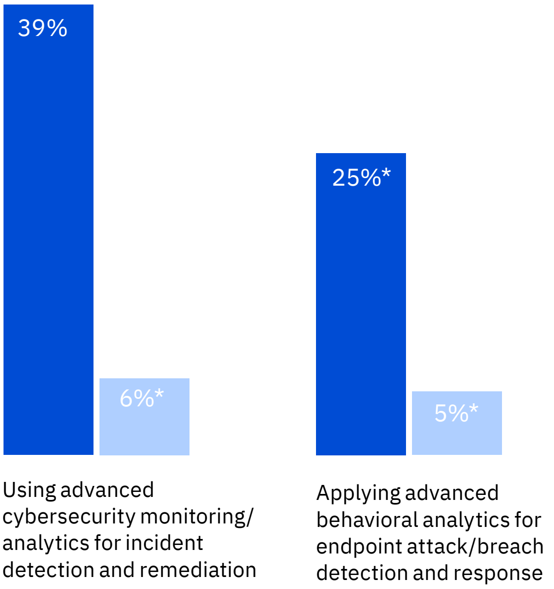
9. Apply advanced cybersecurity monitoring and analytics for incident detection and remediation. To keep up with IIoT information in real time across operational environments, 39 percent of security leaders (versus 7 percent of other companies) have established comprehensive security telemetry capabilities that automate the collection, integration, and analysis of data from all possible monitoring points. This includes system logs, network flows, endpoint data, cloud usage, and user behavior, allowing travel-industry security operations (SOC) teams to quickly understand the surrounding context of an alert and differentiate between false positives and genuine alerts. For a proactive approach, SOC teams can analyze the information extracted from internal IIoT data together with externally sourced threat intelligence data and apply machine learning to predict attackers' next moves.

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

The IIoT represents the convergence of IT and OT solution sets, many of which were designed before cybersecurity was a consideration. This raises complexity and introduces a unique set of risks. With an IIoT security strategy that makes security an integral part of operations, travel companies can benefit from the use of these new technologies without placing their companies – or the well-being of employees and travelers – at risk.

Figure 9

Automate detection, remediation, response, and recovery processes



Security leaders **All other companies**

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

Can your travel organization protect critical infrastructure?

- How 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? Is this being one in a way that maintains visibility, transparency, and accountability throughout the operational lifecycle?
- How can you increase segregation to optimize the isolation of less secure IIoT networks?
- How are you bolstering 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

A two-phased approach to boost your cyber resilience

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 travel programs.
- Form cross-functional travel security teams.

Limit access to travel 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.

Once the defensive foundation is in place, enable travel security automation at scale.

Integrate IIoT cybersecurity into travel security operations, allowing your organization to respond rapidly and effectively to IIoT-related incidents and breaches:

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

- Define and manage travel 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.

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/breach detection and response.

About the authors

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. Responsible for mergers and acquisitions and security benchmarking, she also collaborates with IBM industry experts to develop and maintain industry process frameworks. Lisa is based in South Africa.

Greg Land

linkedin.com/in/gregland
greg.land@us.ibm.com

Greg (James) Land is the IBM Global Segment leader for Hospitality and Travel Related Services. Greg has dedicated his entire 25-year career to the travel industry, where he has served as a strategy consultant, advisor, and executive. His work with global airlines, travel technology providers, and hospitality companies has informed his views on digital transformation. Greg is based in New York.

Eric Maass

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

Eric Maass is 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. He is a security industry veteran with roughly 20 years of corporate and start-up experience across commercial, DoD, and intelligence agencies. Eric served as founder and CTO of a cloud security start-up that was acquired by IBM in 2014. Eric is based in the greater NYC area.

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.

Gerald Parham

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

Gerald Parham is the Global Security & 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.

Steve Peterson

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

Steve Peterson is the global Travel & Transportation lead for the IBM Institute for Business Value. Steve is the author of numerous industry studies and has served as a strategy consultant to the industry since 1998. His 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, 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 study or the IBM Institute for Business Value, 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/ibv.

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, all of which 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 Easter 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 transport mode (land, air, 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: 1) We asked about organizations’ capabilities to identify and protect themselves from IIoT-related cybersecurity risks and their ability to detect, respond to, and recover incidents. 2) 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, and cycle time to respond to and recover from IIoT cybersecurity incidents. This allowed us to identify the security leaders as those performing in the 80th percentile. Second, to understand which of the 20 CIS Critical Security controls and 6 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 10 are those with an above average influence. All data, financial or otherwise, is self-reported.

Related reports

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. ibm.biz/iotthreats

Fisher, Lisa-Giane, Giuseppe Serio, and Ben Stanley. “Automotive Industrial Internet of Things: Quick to implement, slow to secure.” IBM Institute for Business Value. August, 2018. ibm.biz/autoiiot

Borrett, Martin, Lisa-Giane Fisher, Cristene Gonzalez-Wertz, and Peter Xu. “Electronics Industrial IoT cybersecurity: As strong as its weakest link.” IBM Institute for Business Value. October 2018. ibm.biz/electronicsiiot

Dougherty, Steven, 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. ibm.co/utilitiesiiot

Notes and sources

1 Muncaster, Phil. “San Francisco Airport Attack Linked to Russian State Hackers.” Information Security Magazine. April 2020. https://www.infosecurity-magazine.com/news/san-francisco-airport-attack/

2 “DragonFly: Energy sector attacks.” IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Dragonfly-Energy-Sector-Attacks-d4cf1567963a2cdbd24fae1fbff27111

3 Riedel, Bruce. “Al Qaeda’s 9/11 Obsession.” Brookings. July 15, 2011. https://www.brookings.edu/opinions/al-qaedas-911-obsession/

4 Bonderud, Douglas. “Loco Motives? Hacker Attacks Could Derail Train Cybersecurity, Researchers Say.” IBM Security Intelligence. January 12, 2016. https://securityintelligence.com/loco-motives-hacker-attacks-could-derail-train-cybersecurity-researchers-say/

5 Alvarez, Michelle. “Industry Overview – Critical Infrastructure (Basic Needs).” IBM Managed Security Services (MSS). March 25, 2015. https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/industry_overview_crit_infra_3-25-2015.html?cm_mc_uid=48776590151015659713589&cm_mc_sid_50200000=52979001567332373470&cm_mc_sid_52640000=66539761567332373474

6 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; 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

7 Lunden, Ingrid. “UK’s ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users.” Techcrunch. July 8, 2019. https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/

8 Rodriguez, Joe Fitzgerald. “Alleged Muni ‘hacker’ demands $73,000 ransom, some computers in stations restored.” *San Francisco Examiner*. November 28, 2016. https://www.sfexaminer.com/news/alleged-muni-hacker-demands-73000-ransom-some-computers-in-stations-restored/

9 Newman, Lily Hay. “Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.” Wired. April 23, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

10 Baker, Graeme. “Schoolboy hacks into city’s tram system.” *The Telegraph*. January 11, 2008. https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

11 This data point indicates the relative confidence of security leaders in their IIoT cybersecurity capabilities. It has a low n count (n<20) so is statistically unreliable but can be considered directional when compared to remaining respondents.

12 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; 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

13 "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/nist special-publication-800-series-general-information; "ISO/IEC 27000 family - Information security management systems." International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

14 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/

15 "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/

16 Ibid.

17 Ibid.

18 "IBM X-Force Threat Intelligence Index 2019." IBM Security. February 2019. https://www.ibm.com/security/data-breach/threat-intelligence

About Benchmark Insights

Benchmark Insights feature insights for executives on important business and related technology topics. They are based on analysis of performance data and other benchmarking measures. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
April 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.

IBM®