Benchmark Insights

Mind the utilities cybersecurity gap

Move from pieced together to peace of mind

IBM Institute for Business Value

By Cristene Gonzalez-Wertz, Lisa-Giane Fisher, Steven Dougherty and Mark Holt

Talking points

IIoT in utilities

Utilities are early and extensive adopters of IIoT technologies. Our survey reveals where and how they are using them.

A cybersecurity dilemma

Utility companies are aware of cybersecurity risks. So, why does comprehensive IIoT cybersecurity remain a challenge?

Five concrete strategies

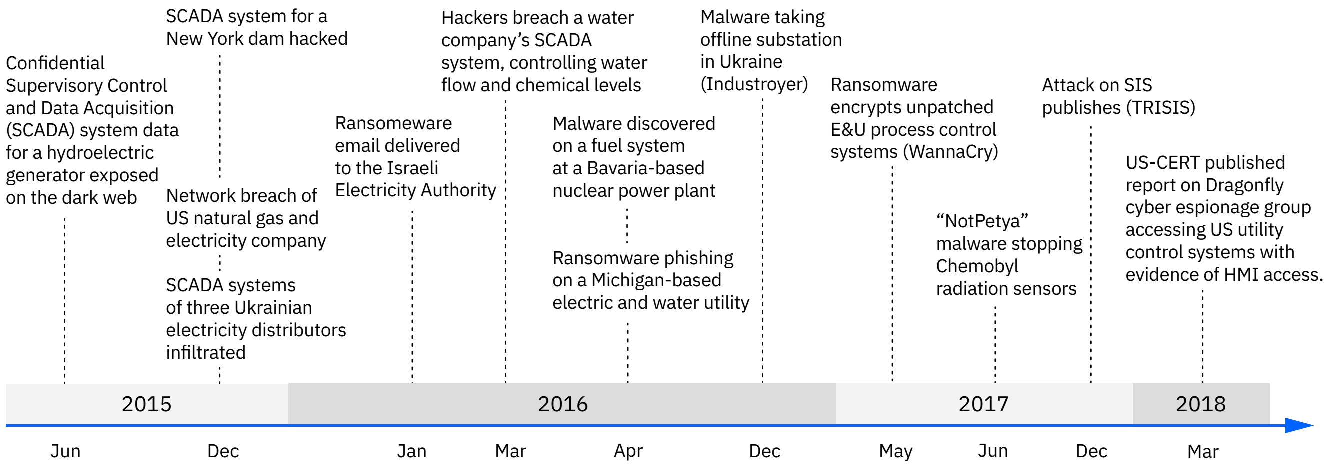
Learn how to institute and enhance IIoT cyber hygiene by building a strong cybersecurity foundation—and then leveraging AI and automation for more advanced capabilities.

–

As Industrial Internet of Things (IIoT) technologies enable increasingly intelligent automated equipment and processes, utilities run an increased risk of cyberattacks. Whether initiated by terrorists, cyber hackers or nation state actors, successful attacks can result in devastating consequences. Breaches of nuclear-based power plants and energy grids can affect the provision of energy, while cyberattacks on water facilities can lead to contamination or denial of drinking water. The risks to citizen safety, critical infrastructure and the environment are alarming. Fundamental IIoT cyber hygiene, augmented with automation and artificial intelligence (AI), is critical to continuity of operations and service delivery for utilities.

Today, utilities leverage IIoT technologies in collecting data to monitor assets, gain operational insights, and improve efficiency and safety. Yet, as IIoT expands, attempts to exploit and gain access to industrial control systems (ICS) networks will continue. The attack surface in an IIoT-enabled environment can range from high-value assets or services to critical workloads in the cloud. It also can include process control systems in cyber-physical systems and critical business, operational and consumer data. For example, the U.S. Department of Homeland Security (DHS) recently reported that the Dragonfly espionage group accessed Human Machine Interfaces (HMI) that control processes at several North American power generation utilities. While inside the system, the group copied configuration information and gained the potential to sabotage or take control of the facilities.[1]

Attacks on ICS networks: A snapshot


Confidential Supervisory Control and Data Acquisition (SCADA) system data for a hydroelectric generator exposed on the dark web
SCADA system for a New York dam hacked
Network breach of US natural gas and electricity company
SCADA systems of three Ukrainian electricity distributors infiltrated
Ransomeware email delivered to the Israeli Electricity Authority
Hackers breach a water company's SCADA system, controlling water flow and chemical levels
Malware discovered on a fuel system at a Bavaria-based nuclear power plant
Ransomware phishing on a Michigan-based electric and water utility
Malware taking offline substation in Ukraine (Industroyer)
Ransomware encrypts unpatched E&U process control systems (WannaCry)
"NotPetya" malware stopping Chemobyl radiation sensors
Attack on SIS publishes (TRISIS)
US-CERT published report on Dragonfly cyber espionage group accessing US utility control systems with evidence of HMI access.
2015
2016
2017
2018
Jun
Dec
Jan
Mar
Apr
Dec
May
Jun
Dec
Mar

Source: IBM Security research.

IIoT cybersecurity in utility operations

70%

of utilities are deploying IIoT technologies with—at most—a moderate understanding of IIoT cybersecurity

64%

of power utilities rate production disruptions/shutdowns and the resulting loss of public confidence among their greatest IIoT cybersecurity risks

Utilities detect less than

50%

of their IIoT cybersecurity incidents themselves

To better understand the state of IIoT security, the IBM Institute for Business Value (IBV) partnered with Oxford Economics to survey 700 executives from industrial and energy organizations in 18 countries, including 120 from utilities. At the time of the survey, all 700 organizations were implementing IIoT in their operations.

The research confirmed that utilities are early and extensive adopters of IIoT technologies. Respondents say their organizations primarily apply them for alarms, meter reading and real-time equipment monitoring, generating huge volumes of data that move across supervision and control networks.

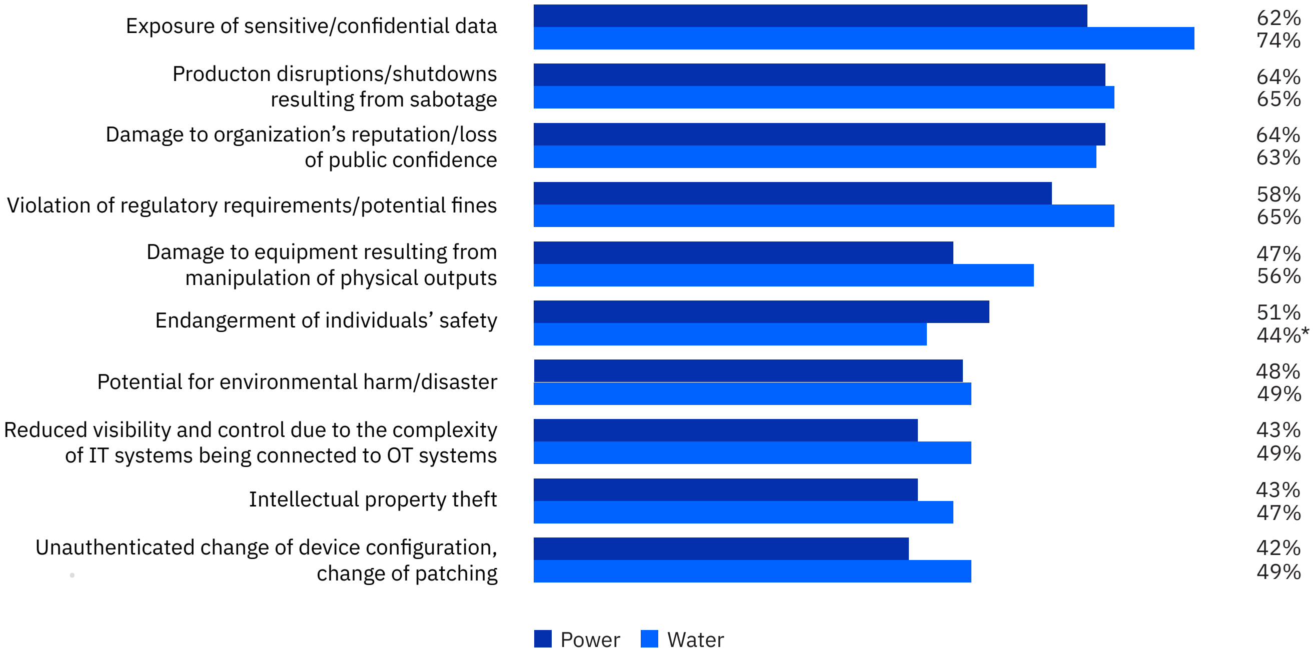
However, utility executives are apprehensive about the security of their IIoT endpoints. Devices and sensors are cited by 24 percent of respondents as the most vulnerable parts of their IIoT deployments. Utility executives are also concerned that data on these devices and sensors, as well as on gateways, is not adequately protected. Twelve percent of utilities are concerned with the vulnerability of data in the cloud.

Cyberattacks on utilities can have far-reaching health, economic, environmental and psychological impacts.

On average, the exposure of sensitive data is rated by utilities as the highest impact IIoT-related risk. This includes billing and revenue information (from smart grid and smart metering systems), control systems information, and employee and customer data. Power utilities are more concerned with production disruptions or shutdowns and the resulting damage to their reputations. More than half of all utilities are worried about the potential impact of regulatory violations and damage to equipment (see Figure 1).

Figure 1

Utility market: High-impact IIoT cybersecurity risks



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

What is cyber hygiene?[2]

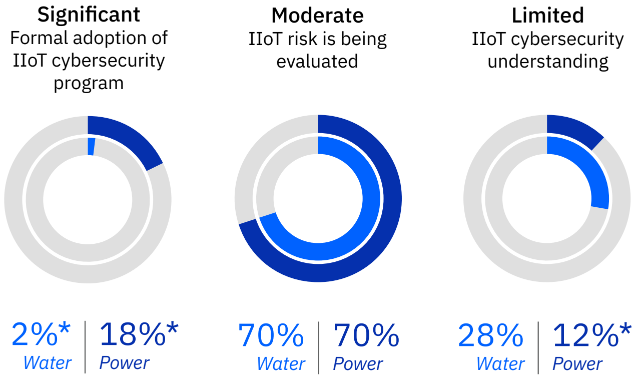
Cyber hygiene refers to baseline cyber practices that organizations use in their cybersecurity programs, as well as the steps organizations and users of computers and other devices take to maintain system health and improve online security. Often, these practices are part of a routine to help ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

Why haven't utilities closed the gap?

Utility companies are clearly aware of the cybersecurity risks, but 70 percent say they have—at most—a moderate understanding of IIoT cybersecurity. Survey results reveal that utilities lack fundamental IIoT cyber hygiene—the organization, technology and processes required to mitigate the risks. While power utilities have a way to go before their operations can be called "secure," they do have a better grasp of the security needs of their IIoT deployments and connected cyber-physical systems than water utilities. Eighteen percent of power utilities have formal IIoT cybersecurity programs to establish, manage and update required IIoT cybersecurity tools, processes and skills compared to only 2 percent of water utilities (see Figure 2).

Figure 2

Understanding of IIoT cybersecurity and adoption of formal cybersecurity programs



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

A majority of utilities have only a moderate understanding of IIoT cybersecurity.

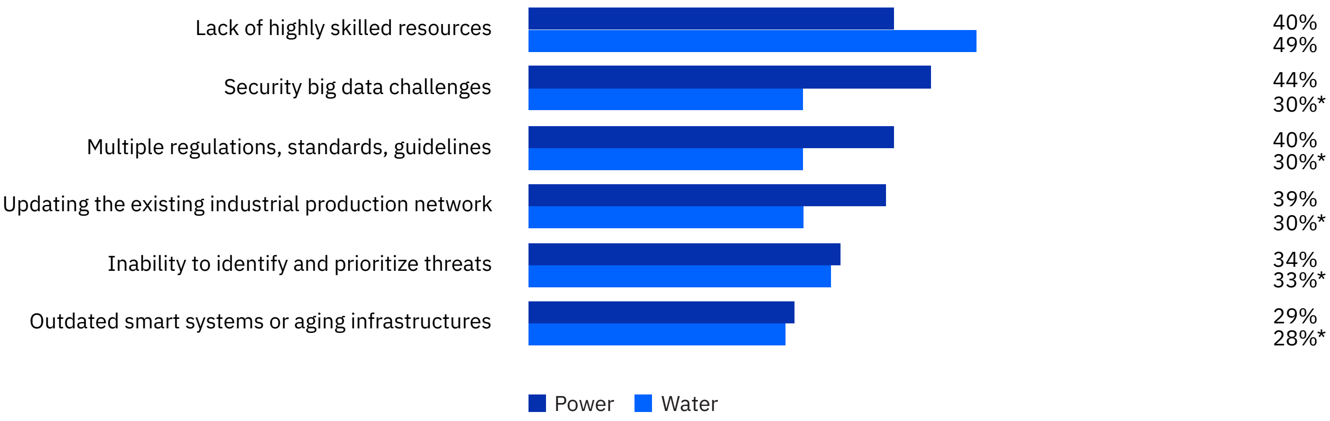
Although power companies' programs are more mature on average, the IIoT cybersecurity capabilities of both groups are nascent. They face significant challenges that account for the gap between IIoT technology and cybersecurity deployment and prevent comprehensive IIoT cybersecurity (see Figure 3).

Forty-nine percent of water and 40 percent of power utility executives surveyed are experiencing a cybersecurity talent shortage. In addition, velocity and scale are challenges when defending complex utility infrastructures with numerous IIoT technologies. Our research shows 44 percent of water and 30 percent of power utility executives face such big data challenges. They struggle to effectively manage, analyze and apply the data ingested by their security tools to support detection and remediation efforts.

According to a recent report on attack activity trends, the global median for the time between a successful breach and its detection was 101 days in 2017.[3] Our survey data shows that it takes power and water utilities another 14 days and 18 days respectively to respond and restore operations. In addition, our respondents tell us that about half of utility IIoT cybersecurity incidents (53 percent of power and 48 percent of water) are detected by third parties rather than the utilities themselves.

Figure 3

The greatest challenges to securing utility IIoT deployments



Source: IBM Institute for Business Value benchmark study, 2018.

Utilities selected the top three. n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

Securing cloud-based utility data

Electric control infrastructures in smart cities are generating growing volumes of data related to traffic flow, street lighting and safety sensors, as well as distributed energy resources, energy flow and usage. Cloud-hosted computing and storage resources offer utilities the means to leverage this growing volume of IIoT sensor data.

However, North American utilities in electricity generation or transmission must comply with "critical national infrastructure" regulations managed by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Committee. Therefore, they are not currently able to transmit control systems information to publicly shared cloud-hosted computing environments. NERC CIP standards are used by the Federal Energy Regulatory Commission (FERC) to help secure and regulate the bulk electric grid, requiring utilities to know who has access to their data and how it is protected.[7]

IBM is working with NERC to evolve the Federal Risk and Authorization Management Program (FedRAMP) model, a standardized approach the U.S. government uses to assess the security of cloud-based systems. CIPC is evaluating the process to determine if it can be used in an environment subject to compliance with CIP Reliability Standards. The FedRAMP model uses a trusted third party to verify that controls are in place and monitored, improving compliance and enabling the potential for accelerated adoption of cloud in IIoT.[8]

Swift response to a breach is critical. A recent report by Ponemon on the costs of data breaches reveals that the faster a data breach can be identified and contained, the lower the costs. It found that the extensive use of IoT devices increases the cost per compromised record by USD 5. Conversely, the average cost of a data breach for organizations with fully deployed security automation is approximately 35 percent less than that for organizations without automation.[4]

Our respondents also report being challenged to apply or comply with a plethora of regulations, standards and guidelines (see sidebar: *Securing cloud-based utility data*). In addition, 39 percent of power and 30 percent of water companies from our survey have industrial production networks and aging infrastructures that are difficult to update. Security was an afterthought for many early generation industrial control system applications, such as the smart grid, and legacy devices were often manufactured with lessened attention to security.

As a result, replacing them can be both expensive and impractical because newer devices are not always manufactured with modern security features, and there are limited windows in which to perform updates for devices that run all day every day.[5] This is not likely to change soon: As of September 2018, California is the only U.S. state with an IoT security law, and it doesn't go into effect until 2020.[6]

The average cost of a data breach for organizations with fully deployed security automation is approximately 35 percent less than that for organizations without automation.[4]

Closing the gap: Building a strong defense

We suggest a two-pronged approach to closing the cybersecurity gap. First, organizations should focus on building a strong IIoT cybersecurity foundation and establishing fundamental cyber hygiene. Once the defensive foundation is in place, utilities can focus on developing more advanced security capabilities using AI and automation. This will take them further toward overcoming their challenges and ensuring continuous operations and service delivery.

Below are four strategies to help utilities establish a strong foundation for fundamental IIoT cyber hygiene:

1. Manage IIoT cybersecurity risk at an enterprise level.

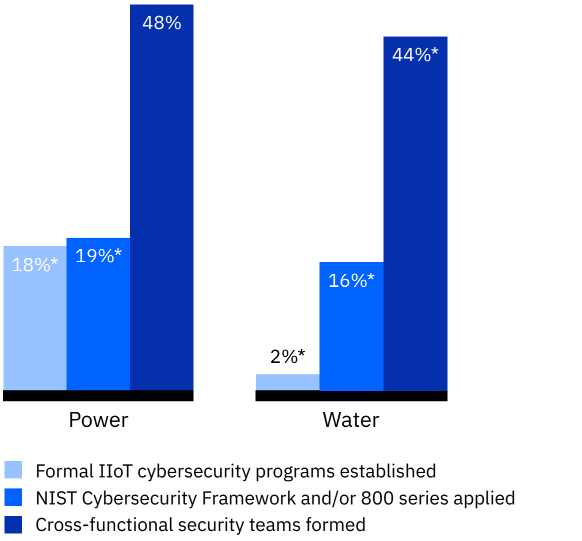
Inadequately protected utility IIoT environments pose risks to entire sectors of society. As a result, such risks should be visible to and managed across the entire utility. After defining a clear IIoT security strategy, utilities can apply three practices to infuse IIoT cybersecurity throughout the ecosystem:

- *Formally establish an IIoT security program* to define, manage and update required IIoT cybersecurity tools, processes and skills.
- *Apply a combination of security and governance frameworks*, such as National Institute of Standards and Technology (NIST) Risk Management Framework, NIST 800 standards and ISO/IEC 27000-1, as foundations to:[9]
    - 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.
- *Form cross-functional security teams* with representation from IT security, engineering, operations, and control system and security vendors. Forty-nine percent of power utilities and 44 percent of water utilities we surveyed leverage such teams. Working cross functionally can help an organization develop a clearer understanding of the differences between IoT systems, standard corporate IT systems and operational equipment. It can also help utilities leverage IT and operational technology (OT) expertise to better protect systems and equipment (see Figure 4).[10]

Employee cybersecurity education can increase awareness and enhance the effectiveness of security operations.

Figure 4

Manage IIoT cybersecurity risk at an enterprise level



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

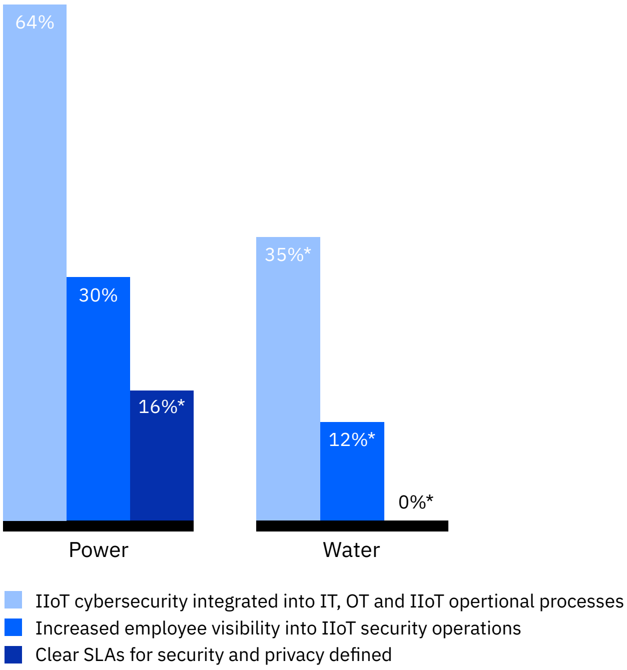
2. Operationalize and enforce IIoT cybersecurity.

As IIoT technologies become part of the critical architecture of utilities, so too should security features. Three practices can support building security features as part of the architecture, integrating them into operations and extending their effectiveness beyond a company's walls:

- *Integrate IIoT cybersecurity into IT, OT and IIoT operational processes.* Sixty-four percent of power utilities say they have, at a minimum, the infrastructure and processes in place to securely provide new IIoT-enabled offerings or services. Only 35 percent of water utilities are at this point. Deploying IIoT systems that are both high risk and complex requires not only cybersecurity experts, but also OT experts to provide guidance on the design and operation of cyber-physical systems. We suggest adopting a secure systems development lifecycle (SDLC) such as DevSecOps and integrating activities to discover and reduce vulnerabilities early.
- *Increase employee visibility into IoT security operations, IT and OT.*[11] Eighteen percent of power and 12 percent of water utilities focus on this as a preventative measure. Cybersecurity education and awareness activities are critical to achieve IIoT cyber hygiene (see Figure 5).
- *Define clear service level agreements (SLAs) for security and privacy.* This is especially important where there is reliance on third parties. Only 16 percent of power utilities monitor and enforce security requirements through SLAs, while none of our water utilities respondents leverage them. Maintaining controlled access to data can help combat insider attacks and prevent information from being stolen or compromised. It's important to document who has entitlements to access sensitive functions or data, as well as closely monitor and audit the actions of those privileged users.[12]

Figure 5

Operationalize and enforce IIoT cybersecurity



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents*

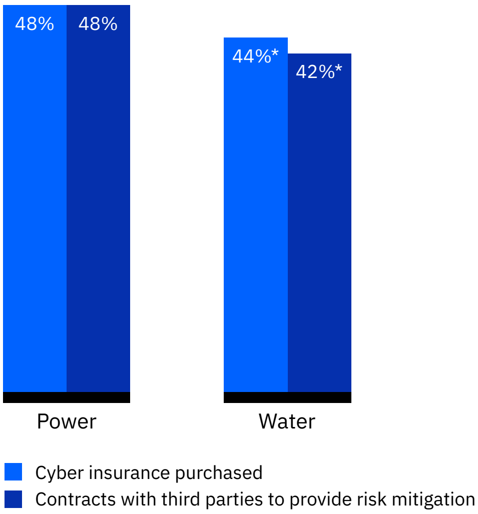
3. Understand and limit the impact of incidents and breaches.

Consider all the costs of a breach: response and notification, damage to critical infrastructure, regulatory fines, additional security and audit requirements, and other liabilities and estimated damages. Understanding which costs can be absorbed and which are potentially catastrophic can help an organization correctly prioritize its cybersecurity investments. Two practices in particular can help limit the impact of a breach:

- *Purchase cyber insurance to mitigate residual risk.* Forty-six percent of power utilities and 44 percent of water utilities purchase cyber insurance to offset costs involved with recovery after a breach or similar event.
- *Contract with third parties for risk mitigation.* Forty-two percent of power and 48 percent of water utilities take this approach (see Figure 6).

Figure 6

Understand and limit the impact of incidents and breaches



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

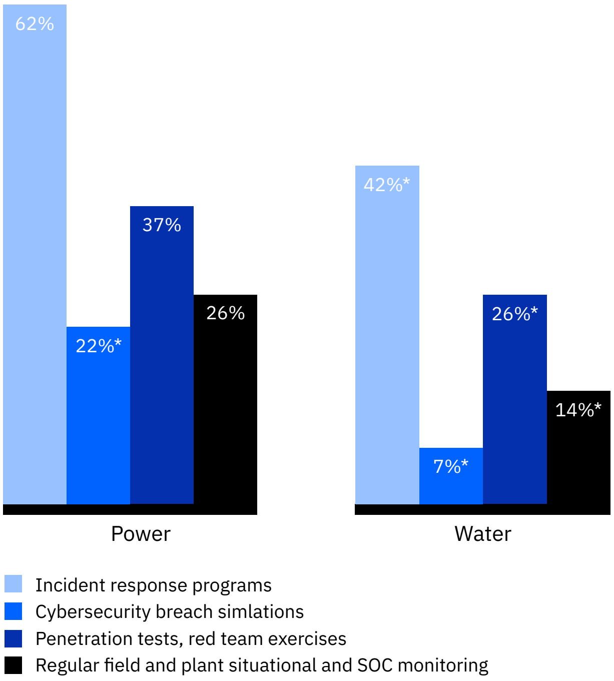
4. Prepare an orchestrated response to incidents and breaches

Utilities are faced with complex cyberattacks that shift as they unfold, complicated infrastructures and a shortage of cybersecurity skills. Technologies and processes that enable a fast, dynamic and orchestrated response are vital. We have identified four practices to help establish these capabilities:

- *Define incident response plans* as part of the security management plan. And if necessary, leverage third-party incident firms for specialized expertise. Sixty-two percent of power and 42 percent of water utilities have tailored their incident response plans to address the course of action for compromised IIoT components.
- *Perform cybersecurity breach simulations.* Twenty-two percent of power utilities are taking incident response a step further by performing breach simulations to help identify which processes, people and tools to activate in the event of a breach. Only 7 percent of water utilities surveyed are performing simulations.
- *Perform penetration tests and red team exercises.* Red teams are groups of ethical hackers that simulate cyberattacks, allowing security leaders to stress-test their incident response plans, identify gaps and adjust accordingly. Penetration tests help discover ad-hoc vulnerabilities and maintain compliance with security policies and data-privacy regulations. According to our research, 37 percent of power and 26 percent of water utilities are implementing these offensive defense strategies.
- *Perform regular field and plant situational awareness and security operation center (SOC) monitoring.* Field and plant awareness exercises should be complemented with an SOC team that continually assesses the organization's security posture, oversees security operations and works closely with organizational incident response teams. Just over a quarter of power utilities are increasing their perception of complex operational environments—such as power plants—that are critical for decision makers, compared to only 14 percent of water utilities (see Figure 7).

Figure 7

Prepare an orchestrated response to incidents and breaches



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

Once the defensive foundations are in place, utilities can focus on a fifth strategy to build more advanced capabilities:

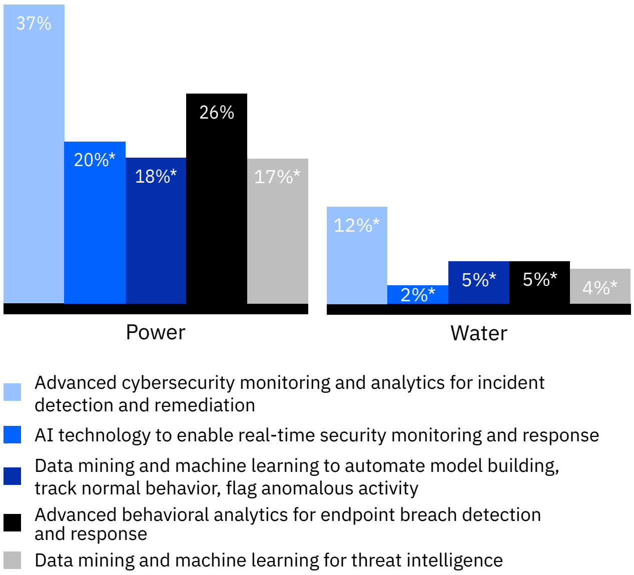
5. Apply intelligent, automated threat detection and response

To reduce the load on security resources, manual threat detection can be reduced by implementing AI-driven, automated investigation processes. Threats can be systemically prioritized for customized alerts by defining sensitive data and assets, network segments and cloud services. Security tools can make sense of the large volume of data they ingest by leveraging AI. Following are five ways to implement these capabilities:

- *Apply advanced cybersecurity monitoring and analytics for incident detection and remediation.* Thirty-seven percent of power utilities and 12 percent of water utilities focus on analyzing IIoT information rather than gathering data to generate after-the-fact auditing and reporting.
- *Implement AI technology for real-time security monitoring and response.* To keep up with IIoT information in real time and obtain a complete picture of what is happening in their environments, 20 percent of power utilities have automated 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. Only 2 percent of water utilities have implemented similar capabilities.
- *Apply data mining and machine learning to automate model building, track normal behavior and flag anomalous activity.* IIoT information from all monitoring points provides an understanding of what's "normal" down to the network level. Machine learning can automate building adaptive models of what is normal, track normal behavior and flag anomalous activity that can signal new threats. Eighteen percent and 5 percent of power and water utilities report these capabilities respectively.
- *Apply advanced behavioral analytics for endpoint breach detection and response.* Complement existing technology with endpoint detection and response mechanisms that monitor techniques used by malware creators in recent attacks and fill the gap using pattern-recognition technology powered by machine learning. Twenty-six percent of power utilities tell us they use behavior analytics that leverage machine learning, versus 5 percent of water utilities.
- *Apply data mining and machine learning for threat intelligence.* The right threat intelligence at the right time empowers an SOC team to block attacks in real time, predict attackers' next moves and proactively hunt for threats. Only 17 percent of power utilities and 4 percent of water utilities have systems to extract information from their IIoT data streams and external sources, apply machine learning to detect abnormal behavior and predict items of considerable threat (see Figure 8).

Figure 8

Apply intelligent, automated threat detection and response



Source: IBM Institute for Business Value benchmark study, 2018.

n = 120; power = 77; water = 43
** Low n count (n<20) are statistically unreliable but can be considered directional when compared to remaining respondents.*

A complete IIoT risk assessment is critical to developing a strong security strategy.

For utilities, keeping the “lights on” or “water flowing” is critical, so availability becomes a major security priority. However, implementing multiple IIoT security controls, practices and technologies without a full evaluation of IIoT risk results in a lack of clarity. It can lead to mistakenly prioritized IIoT cybersecurity investments. Without a robust evaluation, utilities may end up with gaps where key defenses are required. Cybersecurity practices and technologies must be adopted as part of an overarching IIoT security strategy and program and aligned with an organization’s broader IT and OT risk and security frameworks. It’s not about one specific tool or skill. Security is about people, technology and processes, all of which need to be well orchestrated to work properly. It’s an effort of the entire ecosystem: utilities, government, equipment providers and security vendors.

Can your organization protect infrastructure, the economy and society?

» How is your OT security strategy aligned with your organization’s overall security strategy?

» How have you aligned IIoT security practices with the organization’s enterprise risk management framework?

» How are you integrating security tools and management processes into the organization’s security framework and operational processes?

» How are you adopting a “security first” strategy and building foundational security features across all aspects of your IIoT design?

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

About the authors

Cristene Gonzalez-Wertz
linkedin.com/in/cjgw1
cristeneg@us.ibm.com

Cristene Gonzalez-Wertz is the Electronics and Environment, Energy and Utilities Leader for the IBM Institute for Business Value. She advises clients on technology trends and strategic positioning in AI, analytics, IoT, security and customer experience. Cristene provides guidance on emerging value opportunities, especially the data economy.

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 warranty and IoT security benchmarking and collaborates with IBM industry experts to develop and maintain industry process frameworks.

Steven Dougherty
linkedin.com/in/steven-a-steve-dougherty-cissp-cfe-4585b7
sdougherty@us.ibm.com

Steven Dougherty is an Energy, Environment and Utilities Business Development Executive for IBM Security. He has over 30 years' experience designing, delivering and operating innovative cybersecurity solutions, industry controls and technology strategies for clients across the globe. Steven is an IEEE Senior Member, a Certified Information Systems Security Professional (CISSP) and a Certified Fraud Examiner (CFE).

Mark Holt
linkedin.com/in/lmarkholt
mholt@us.ibm.com

Mark Holt is the Security Business Development Leader for IBM Global Energy, Environment, and Utilities Industry. Mark has a long background in engineering systems, asset management and IoT, having also led the IBM systems engineering strategy. Currently, Mark leads the global focus in bringing IBM security capability to utilities.

For more information

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

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

The right partner for a changing world

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

IBM Institute for Business Value

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

Related IBV publications

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

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.com/business/value/iotthreats

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

IBM capabilities

Connecting systems that monitor and control physical environments to the internet without securing them adequately is risky and potentially expensive. A successful cyberattack in IoT-enabled utility operations can have catastrophic consequences. However, many of these risks can be addressed or mitigated. IBM helps utility 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 utility experts can address quality while helping to protect assets and processes. IBM applies cognitive approaches to help reduce security risks. Please visit ibm.com/industries/energy.

Notes and sources

1 “Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” United States Computer Emergency Readiness Team alert. March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A

2 Aldorisio, Jeff. “What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More.” Digital Guardian. September 26, 2018. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

3 “M-Trends 2018.” Mandiant, a FireEye company. 2018. https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

4 “2018 Cost of a Data Breach Study: Global Overview.” Ponemon Institute LLC. July 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN

5 Gonzalez-Wertz, Cristene, Lisa Fisher, Peter Xu, and Martin Borrett. “Electronics Industrial IoT cybersecurity: As strong as its weakest link.” IBM Institute for Business Value. October 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/electronicsiiot/

6 Robertson, Adi. “California just became the first state with an Internet of Things cybersecurity law.” The Verge. September 28, 2018. https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

7 “Mandatory Reliability Standards for Critical Infrastructure Protection: A Rule by the Federal Energy Regulatory Commission.” Federal Register. January 18, 2008. https://www.federalregister.gov/documents/2008/02/07/E8-1317/mandatory-reliability-standards-for-critical-infrastructure-protection; “Critical Infrastructure Protection Committee (CIPC).” North American Electric Reliability Corporation (NERC) website, accessed December 26, 2018. https://www.nerc.com/comm/CIPC/Pages/default.aspx

8 “Critical Infrastructure Protection Committee (CIPC) Meeting Minutes.” North American Electric Reliability Corporation (NERC). June 5-6, 2018. https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC%20June%202018%20minutes%20DRAFT%20v0.pdf

9 “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

10 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

11 Ibid.

12 Gonzalez-Wertz, Cristene, Lisa Fisher, Peter Xu, and Martin Borrett. “Electronics Industrial IoT cybersecurity: As strong as its weakest link.” IBM Institute for Business Value. October 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/electronicsiiot

13 Ibid.

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
January 2019

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.