Internet of threats

Securing the Internet of Things for industrial and utility companies

IBM Institute for Business Value

Become unassailable

The Internet of Things (IoT) has become ubiquitous. Insights derived from data collected from connected devices are being used across industries to enhance productivity, solve problems and create new business opportunities and operational efficiencies. But there are also risks. Security was an afterthought for many early generation IoT applications, creating vulnerabilities in the network and the potential for industrial process interruption, manipulation or espionage. But the Internet of Things cannot become simply the internet of threats. Industry and utilities companies, in particular, need to develop new strategies to mitigate and manage cyber-risks.

Building the plane while flying it

It is mind-boggling how fast IoT technology is flourishing across all industries, including industrial and utilities companies. The IoT market is projected to grow from an installed base of 15 billion devices in 2015 to 30 billion devices in 2020 and 75 billion in 2025.[1] The volume of data generated will reach 600 zettabytes per year by 2020.[2]

IoT for industrial environments, driven mostly by next-generation manufacturing, is also referred to as the Industrial Internet of Things (IIoT) and represents a huge market, one that could add 14 trillion USD to the global economy by 2030.[3] IIoT can harness the data from machines and equipment to transform the processes and systems of the modern plant environment. And from smart meters, to sensors, to alarms, IoT devices are flooding utility operations. It makes sense that these industries use IoT for things such as real-time data analytics, equipment monitoring, predictive maintenance and machine automation beyond corporate borders.

But underlying concerns about the security and vulnerability of devices and sensors are justified. According to the 19th edition of the IBM Global C-suite Study conducted by the IBM Institute for Business Value (IBV), 36 percent of executives surveyed say securing an IoT platform and its devices is a top challenge for their organizations.[4] An IBV benchmarking study of 700 industrial and utilities IT and OT leaders found that devices and sensors, followed by IoT platforms, are the most vulnerable parts of IoT deployments.[5]

IoT solutions span information technology (IT), operational technology (OT) and consumer technology (CT) functions. Deploying IoT technologies at a faster pace than they are secured can open organizations to dangers greater than negative public sentiment. For industrial manufacturing, chemical, oil and gas and utilities, security breaches can lead to large-spread contamination, environmental disasters and even personal harm. OT has become a growing target, accounting for 30 percent of all cyberattacks.[6] In the Middle East, 50 percent of cyberattacks are directed against the oil and gas industry, creating major impacts to safety, productivity and efficiency.[7]

From infancy to implementation

The IBV benchmarking study shines a light on the current state of IoT security in industrial and utilities.

Most industrial and utilities organizations are in the early stages of adopting practices and protective technologies to mitigate IoT security risks. Only a small percentage have fully implemented operational, technical and cognitive practices or IoT-specific security technologies.[8]

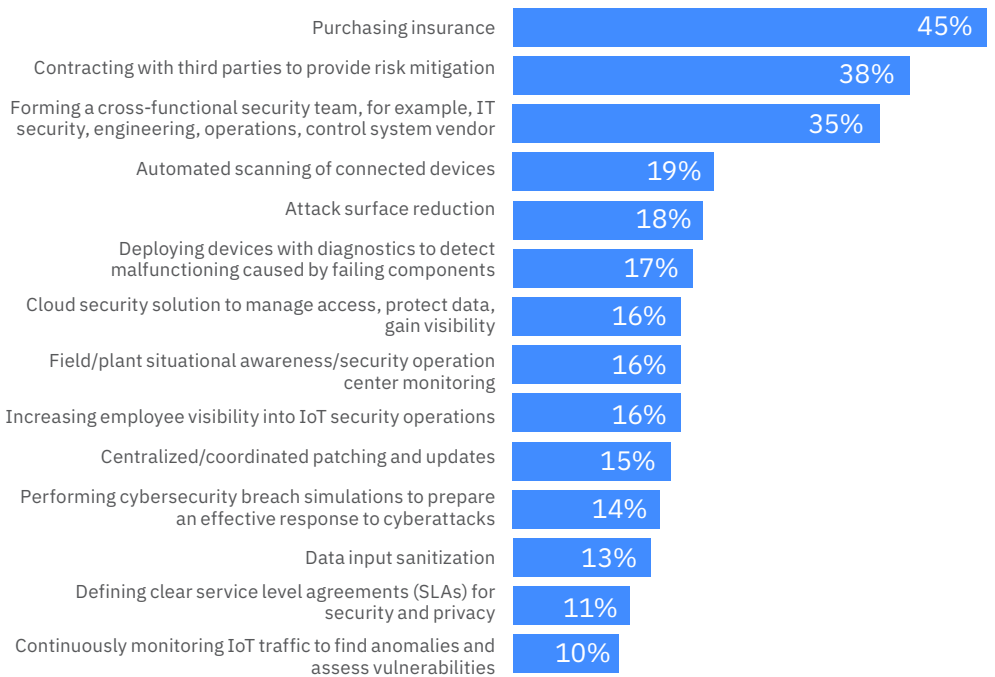
As a result, the IoT security capabilities of most organizations are in their infancy (see Figure 1). Investments have been made and IoT deployments are underway, but cybersecurity risks are still being evaluated and risk assessments performed on an ad hoc basis. Known issues and challenges are likely to prevent an organization from having comprehensive IoT security practices. These issues include:

- *Continued shortage of requisite cybersecurity skills.* The lack of skilled resources is the greatest challenge to securing IoT deployments. A deep talent pool must be made available. Along with being savvy to IT cybersecurity risks, resources should be prepared to:
  - cover a larger and more dispersed inventory of equipment
  - deal with tradeoffs and considerations across security, privacy and reliability aspects of the equipment
  - create and employ automation and continuous engineering, delivery and integration to apply consistent protections across this larger computing environment.

– *Limited awareness of IoT security.* An incomplete understanding of the risks posed by IoT deployments, coupled with a lack of a formal IoT security program contributes to the gap between IoT adoption and the capabilities in place to secure it. IT-centric security frameworks and organizational structure are often not adequate to address reliability and predictability needs of always-on IoT equipment.

– *Slowly emerging IoT security standards.* Established Center for Internet Security (CIS) controls, operational and technical practices, protective technologies and IoT authentication must be implemented. CIS controls include authorized device and software inventories, deploying devices with built-in diagnostics and secure, hardened hardware and firmware.

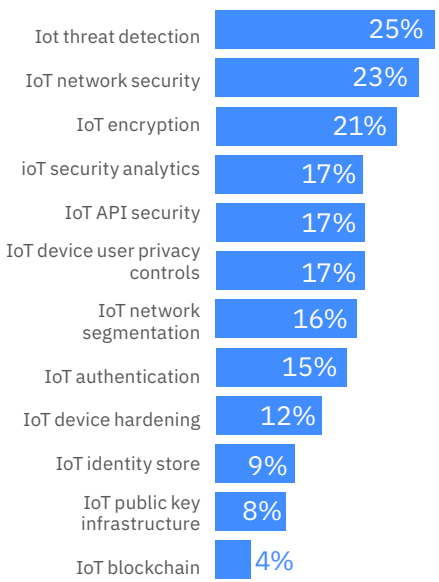
Figure 1
Organizations in the advanced stages of implementing practices to mitigate IoT security risks



Source: IBM Institute for Business Value benchmarking study

Catch up to the threat

Figure 2
Organizations in the advanced stages of implementing protective technologies to mitigate IoT security risks



Source: 2018 IBM Institute for Business Value benchmarking study

IoT security doesn't exist in a vacuum. Procedures must be followed, practices and technologies adopted and measures taken to meet key performance indicators (KPIs). To mitigate IoT security risk and improve performance, organizations can implement practices that:

- *Establish a formal IoT security program.* Follow an operational excellence model of people, process and technology to build IoT security capabilities. Increase employee visibility into IoT security operations, IT and OT. Makers of next-generation connected devices and services may consider purchasing insurance against software malfunctions and any damage hackers might cause.
- *Understand each endpoint, what it does and who it talks to.* Every IoT endpoint must be identified and profiled, added to an asset inventory and monitored. Define clear SLAs where there is reliance on partners and system integrators. Form a cross-functional security team made up of IT security, engineering, operations and a control system vendor.
- *Know when and how to be proactive.* To prepare an effective response to cyberattacks, carry out breach simulations, regular field and plant situational awareness and engage in security operation center monitoring.

The IBV benchmarking study gauged use of relevant and important technologies for delivering IoT security among respondents (see Figure 2). These include:

- Encryption to protect against attacks that could compromise sensitive information and lead to the destruction of property and equipment, or create personal safety issues
- Network security and device authentication to secure deployments between IoT devices, edge equipment and with back end systems and applications.
- Security analytics to identify potential IoT attacks and intrusions that may have bypassed traditional security controls.
- Identify and access management that can help enterprises and service providers manage and secure relationships between identities and IoT devices.

Safe and secure

Risk has long been used to identify, assess, control, monitor and respond to hazards across operations, including safety. As industrial organizations quickly adopt IoT technologies, they must also bring IoT security practices into alignment with their broader risk frameworks. To begin a more robust security conversation, and deliver an optimized technology solution, leaders can take the following steps:

- Manage IoT cybersecurity risk at an enterprise level. Perform regular risk assessments to identify vulnerabilities in IoT systems and connected production environments, and document and execute plans to mitigate potential risks. Build or augment cybersecurity intelligence capabilities to understand the attack vectors to which the organization is most vulnerable.
- Understand the differences among IoT systems, standard corporate IT systems and operational equipment, and share IT and OT security expertise to better protect them. Take differences into account when deciding the correct prioritization of security controls for optimal risk mitigation.
- Break down the silos between IT and OT organizations. Create a common risk approach across disciplines to manage traditionally IT-centric information processing technologies and OT-centric technologies that monitor and control cyberphysical system environments .

About BenchmarkInsights@IBV reports

BenchmarkInsights@IBV integrate the opinions of thought leaders on newsworthy business and related technology topics with research findings from the IBM Institute for Business Value (IBV) Benchmarking team. They are based upon conversations with leading subject matter experts from around the globe and relevant data from studies conducted by the IBV Benchmarking team. For more information, contact Lisa-Giane Fisher, IBV Benchmarking at global.benchmarking@us.ibm.com.

Experts on this topic

Tim Hahn

Chief Architect
Internet of Things Security at IBM
hahnt@us.ibm.com
linkedin.com/in/hahnt/

Marcel Kisch

WW Security Lead E&U and Manufacturing
IBM Security
marcel.kisch@de.ibm.com
linkedin.com/in/highpotential/

James Murphy

Global Leader IoT, Security and Blockchain
IBM Watson and Cloud Platform
jamesmur@uk.ibm.com
linkedin.com/in/jamesmurphygb/

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
March 2018

62013962USEN-01

Notes and sources

1 Columbus, Louis. "Roundup of Internet of Things forecasts and market estimates." Forbes. 2016. https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#789467a8292d

2 McKendrick, Joe. "With Internet of Things and big data, 92 percent of everything we do will be in the cloud." Forbes. 2016. https://www.forbes.com/sites/joemckendrick/2016/11/13/with-internet-of-things-and-big-data-92-of-everything-we-do-will-be-in-the-cloud/#18a41ee74ed5

3 Gerbrandt, Ryan. "IIoT for Utilities: Lessons learned, opportunities ahead." Internet of Things Institute. January 2018. http://www.ioti.com/smart-energy-and-utilities/iiot-utilities-lessons-learned-opportunities-ahead

4 Nordman, Carl, Cristene J Gonzalez-Wertz and Karen Butner. "Intelligent Connections: Reinventing enterprises with Intelligent IoT." IBM Institute for Business Value. January 2018. https://www-935.ibm.com/services/studies/csuite/iot/

5 "Benchmarking survey." IBM Institute for Business Value. 2018. (unpublished data)

6 Menachery, Martin. "New study: Middle East oil and gas sector needs readiness boost as industrial cyber risk increases." Arabian Oil and Gas. November 2017. http://www.arabianoilandgas.com/article-18052-new-study-middle-east-oil-gas-sector-needs-readiness-boost-as-industrial-cyber-risk-increases/

7 Ibid.

8 "Benchmarking survey." IBM Institute for Business Value. 2018. (unpublished data)