SANS

A SANS Survey

The 2018 SANS Industrial IoT Security Survey:

Shaping IIoT Security Concerns

Written by **Barbara Filkins**
Advisor: **Doug Wylie**

July 2018

Sponsored by:
ForeScout Technologies, Inc.

SANS Analyst Program

Foreword by IIC

The world is evolving toward a future that is built upon smart systems composed of disparate types of "things" including cyber/physical systems, embedded systems, industrial control systems, connected medical devices, connected cars and smart "everything," and this trend cannot be stopped. However, to realize this future, industries must properly integrate the connected, software-enabled, real-world interactive types of devices and systems that we call the Industrial Internet of Things (IIoT) into a cohesive system. Unfortunately, along with the promise of greater technical capabilities and business opportunities comes increased complexity, and in turn, a higher vulnerability to cyber security threats that may upset the entire applecart. However, IIoT security cannot be considered in isolation, but rather as part of the system characteristics that must support the safety, reliability, resilience and privacy expectations that can be described as the trustworthiness of the system. The trustworthiness must also contend with the culture clash between the convergence of information technology and operational technology that is presenting both challenges and opportunities for organizations and the industries that support and supply them.

To help address these challenges, the Industrial Internet Consortium (IIC)[1] was created in 2014 to pave the way for realizing the business value in IIoT and address the risks that emerge, affecting those that use, operate or live in proximity to those IIoT systems. This report provides much-needed insights and validation into the real problems faced today and what is working to address them. It provides useful input to many, including the IIC and its partners across the globe, where the concerns related to security are not only being addressed, but also being addressed as part of the holistic need for trustworthy IIoT systems.

— Industrial Internet Consortium

Foreword by ARC

The digital transformation of industry, infrastructure and cities has clearly begun. Whether it's called Industrial Internet of Things (IIoT), Industry 4.0 or digitalization, companies are developing new business improvement strategies based on analytics, artificial intelligence (AI) and machine learning. These efforts are widespread and far-reaching. They will affect every critical activity including operations, maintenance and engineering. Information technology (IT), operational technology (OT) and engineering technology (ET) will all be affected by the explosion in sensors, new networking solutions and architectural changes.

Smart organizations understand the urgency of building a cybersecurity plan that supports these programs. New strategies need to be in place before business leaders demand widespread deployment. Expecting them to wait for security is naïve; the cost

[1] Industrial Internet Security Framework (IISF) Technical Report, Chapters 2 - 4, September 2016, www.iiconsortium.org/IISF.htm

and performance benefits are simply too large to ignore, and competition is forcing rapid adoption. These IIoT efforts will invariably lead to violations of implicit cyber security assumptions, including well-defined perimeters and architectures, which need to be addressed. Understanding how peers are dealing with these challenges will help you accelerate development of a resilient, IT-OT-IIoT cyber security program.

The findings of this SANS research align quite well with ongoing feedback ARC receives from end users in process industries, discrete manufacturing and infrastructure. Predictive maintenance and operational improvements are the primary focus of most of their IIoT efforts. Both involve broad-based connection of existing and new plant sensors with cloud-based solutions and service providers. Cloud connectivity is a concern, but most companies believe they can deal with this through network segmentation and isolation of control networks. The security of new endpoints is clearly more troublesome. Few organizations believe they can rely on the sensors' original equipment manufacturers (OEMs) in this emerging market to provide secure devices. Lack of control over development processes and complex supply chains aggravates end user concerns. Managing endpoint security updates and patches is another daunting challenge. Plant staffs are already overwhelmed with security hygiene tasks for existing assets. There is no bandwidth for coordinating security patches from a multitude of different OEMs. Likewise, few plants have the kind of secure remote access needed to enable direct management by the OEMs. Not surprisingly, these endpoint security concerns are driving increased support for standards groups such as the Industrial Internet Consortium (IIC) and device-certification programs offered by groups such as the International Society of Automation (ISA) and Underwriters Laboratories (UL).

— Sid Snitkin, PhD
Vice-President, Cybersecurity Services
ARC Advisory Group

Executive Summary

The term *IoT* broadly refers to the connection of devices—other than the typical computational platforms (workstations, tablets and smartphones)—to the Internet. IoT encompasses the universe of connected physical devices, vehicles, home appliances and consumer electronics—essentially any object with embedded electronics, software, sensors, actuators and communications capabilities—that enable it to connect and exchange data. Within this universe, Industrial IoT (IIoT) focuses specifically on industrial applications that are often associated with critical infrastructure, including electricity, manufacturing, oil and gas, agriculture, mining, water, transportation and healthcare.

IIoT, like the ISA/IEC-62443[2] zone and conduit concept model before it, has broken the rules of traditional, mainly physically and functionally separated network system architectures, as recommended by the Purdue Enterprise Reference Architecture (PERA) since the 1990s.[3] Endpoint devices can, and often do, now connect directly to Internet, either individually or as part of an IIoT system.

[2] https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf

[3] www.pera.net

This growth will continue. Most organizations in this survey envision a 10 to 25% growth in their connected devices for the foreseeable future, a growth rate that will cause the systems to which IIoT devices connect to double in size roughly every three to seven years. In its 2017 Roundup of Internet of Things Forecasts, Forbes reports that the installed base of IoT devices is forecast to triple in the next seven years (from 23.14B in 2018 to 75.44B in 2025), with manufacturing accounting for 84% of this growth in the past year.[4] IPv6 can enable the needed expansion of the Internet's address space to accommodate this growth, but business drivers also demand corresponding advancements into increased visibility, efficiency, security and control over these connected assets.

The security of the IIoT endpoints is the leading concern for respondents to the 2018 SANS IIoT Security Survey, with network security controls and countermeasures currently being the main enablers of IIoT security. Most of the growth for connected devices is expected to be for those used for monitoring, status, alarms and alerting, as well as predictive maintenance, but over 50% of respondents are still using their devices for directly controlling operations and processes. As IIoT moves industrial operations increasingly toward distributed, online processes, increased visibility at the endpoint needs to supplement today's reliance on the collection and analysis of network traffic and security events for incident response and remediation.

Securing an organization's IIoT infrastructure requires understanding the threats and risks to be faced. According to the survey data, over the next two years, the leading threats pertain to IIoT life-cycle management issues and human error, while the top reported risk is related to security considerations in product and system installation, configuration, service, support and maintenance. One way to interpret this is that attackers will capitalize on vulnerabilities inherent in the products, or weaknesses introduced by those responsible for building, operating and maintaining the systems where these devices are in use, not unlike what we see in other network systems. In most industrial settings, when organizations need to make a choice between ongoing operations and security, it is rare for security to take priority.

Confidence in how well organizations are able to secure their IIoT environments, however, depends on who has been assigned to manage IIoT risk. The closer someone is to the IIoT systems, the greater the recognition of a challenging reality. The individuals probably the most knowledgeable about IIoT implementation, the OT team, appear the least confident in their organization's ability to secure these devices, while company leadership and management, including department managers, appear the most assured.

Convergence in IIoT is not just about technology; it's about who manages the risk and defines the budget. For many, such organizational disparities make security budgeting, staffing and training decisions all the more difficult to execute. The split that often separates IT and OT perspectives on setting proper priorities among availability, integrity, confidentiality and safety objectives is sometimes dwarfed by an unintentional chasm between company leadership and operations. As IT/OT operational convergence starts to overcome differences, even today, it's not unusual for other differences in language, risk tolerance and perceptions of the threat landscape to show themselves when comparing the proverbial top floor and shop floor of many of today's companies.

The following whitepaper provides additional results and recommendations from the survey.

Reshaping Industrial Controls

of IIoT devices connect directly to Internet, bypassing traditional IT security layers.

rely on IP suites to control, configure and collect data from devices.

of devices are already used for monitoring (process health, condition monitoring).

collect specific security and operations data about IIoT devices and systems.

Key Findings

- Confusion over what is meant by "endpoint" further highlights the need for a reference architecture unique to IIoT.
- Endpoints are the concern; networks are the current control.
- The perception of risk, held by those closest to the issues, needs to be shared by those who approve and manage the IIoT budget.

[4] www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#24806afc1480

The Problem

IIoT is accelerating, since both the near-term and long-term benefits for its adoption are clear. IIoT solutions can help reduce costs and increase productivity, reflected by tangible ROI. For example, predictive maintenance is now a reality facilitated through the use of intelligence and often highly specialized sensors that collect better data faster on machines and apply math, data analytics and machine learning to determine exactly when a machine will need maintenance.

IIoT also faces significant challenges. Cyber attacks against connected assets can result in the loss of intellectual property; the loss of production through disruption or damage to physical equipment, systems and product; huge financial losses; and serious injuries or death. Orchestrating meaningful network communication across a variety of endpoints can be challenging, especially when proprietary protocols and vendor-specific implementations still overlay open standards, making interoperability complicated, if not unachievable.

SANS conducted this survey during early 2018 to study what may be facilitating or impeding the security of IIoT solutions. Given the emergence and growth of IIoT systems, what limitations are affecting broad-scale connectivity across industries? And how should these limitations be characterized in terms of the demands placed on both IT and OT security practitioners to safeguard these increasingly complex systems, while ensuring greater reliability, operational integrity, efficiency and productivity?

Characterizing IIoT

Since the late 1990s, ICS network designs have aligned more closely with the Purdue Enterprise Reference Architecture, which describes a standard hierarchy of applications and controls, data flows and enforcement boundaries needed to perform complicated industrial operations. While useful in designing the functional segmentation of control systems, the Purdue Model is not a security architecture; no one envisioned an ICS that follows its hierarchy, nor does it require an organization to implement security controls in the architecture. Nevertheless, the Purdue Model can still help determine an effective security design that protects sensitive control, process and safety devices from other, more publicly exposed layers through physical and logical segmentation and the effective placement of assets, such as intervening firewalls, IDS and IPS.

The growth of IIoT requires a rethinking of this traditional approach with the expansion of borderless industrial systems, new control system architectures and communication pathways. IIoT, like ISA/IEC-62443 before it, blurs the Purdue Model hierarchy into a more "federated" and effectively flatter architecture, dissolving the delineation of levels and zones along

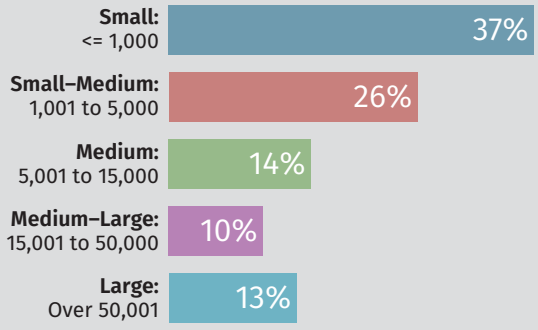
Respondent Demographics

- More than 200 respondents participated in the survey; the number of responses to each question vary.
- Top industries represented include energy/utilities, cyber security, government/public sector, technology and education/training.

Industry	Percentage
Energy/Utilities	17.33%
Cyber security	8.91%
Government/Public Sector	8.91%
Technology	8.91%
Education/Training	6.93%
Oil and gas production or delivery	6.93%
Banking/Finance	5.94%
Manufacturing	5.94%

- Organizations range in workforce size from small (<=1,000) to large (over 50,001).

What is the size of the workforce at your organization, including employees, contractors and consultants?



- Respondent roles are mainly security administrator/analyst (**20%**) and security manager or director (**11%**). More respondents held IT roles than OT roles, which may influence the perspective provided in this paper.

with the prescriptive data flows on which industry has come to rely. Respondents (32%) report that their devices connect directly to Internet, either individually or as part of an IIoT system. Another 32% state that their assets connect through a gateway into the enterprise that transforms information received from external devices (located in the DMZ). See Table 1.

Table 1. The Purdue Model and IIoT Connection Facts

Purdue Model Hierarchy			% of IIoT Devices Connecting to Network Infrastructure	Protocols Used	Communication
Internet			32.4%	1. IP Suite (27.3%) 2. Web (21.2%) 3. IP Domain-specific (19.2%)	1. Wired (25.8%) 2. Wi-Fi (22.7%) 3. Cellular (17.5%)
Internet DMZ (Gateway)			32.4%	1. IP Suite (28.3%) 2T. Web & IP Domain-specific (18.2%)	1. Wired (27.8%) 2. Wi-Fi (18.6%) 3. Cellular (18.6%)
Business Zone		Level 5: Enterprise Business Network	37.3%	1. IP Suite (33.3%) 2T. Web & IP Domain-specific (22.2%)	1. Wired (30.9%) 2. Wi-Fi (27.8%) 3. Cellular (21.6%)
Business Zone		Level 4: Business Unit or Plant Network	44.1%	1. IP Suite (36.4%) 2. IP Domain-specific (31.3%) 3. Web (21.2%)	1. Wired (41.2%) 2. Wi-Fi (28.9%) 3. Cellular (19.6%)
Control Demilitarized Zone			32.4%	1. IP Suite (24.2%) 2. IP Domain-specific (22.2%) 3. Web (20.2%)	1. Wired (30.9%) 2. Wi-Fi (19.6%) 3. Cellular (17.5%)
Operations Zone		Level 3: Operations Support	43.1%	1. IP Suite (35.4%) 2. IP Domain-specific (31.3%) 3. Web (22.2%)	1. Wired (42.3%) 2. Wi-Fi (26.8%) 3. Serial (20.6%)
Operations Zone	Process Control SCADA Zone	Level 2: Supervisory Control			
Operations Zone	Process Control SCADA Zone	Level 1: Control Devices	30.4%	1. IP Suite (25.3%) 2. IP Domain-specific (25.3%) 3. Non-IP based (21.2%)	1. Wired (27.8%) 2. Wi-Fi (16.5%) 3. Serial (15.5%)
Operations Zone	Process Control SCADA Zone	Level 0: Process (Instrumentation)			
Safety Zone			N/A		

While the Purdue Model can help readers understand where IIoT connects into an ICS, it does not provide any information about the level of risk these devices introduce into the infrastructure. IP-based protocols and wireless communication channels allow IIoT systems to more easily connect across IT and OT networks and applications, to integrate processes and data more efficiently, but also to increase vulnerabilities and attack surfaces.

TAKEAWAY

Today, the traditional ICS must embrace the idea that the control system perimeter can extend beyond the traditional security boundaries to often include some means of connectivity to the Internet. IIoT reference architectures must reflect these expanded operational borders, while also accounting for a secure and trustworthy integrated data network and ensuring that endpoints are both trusted and protected.

What Is an IIoT Endpoint?

Surprisingly, the majority (40%) of respondents have fewer than 100 connected devices. Having fewer than 100 connected devices should not necessarily be construed as having a small set of endpoints. The definition of an IIoT endpoint and its relationship to an IIoT device remain hotly debated topics. A device manufacturer may consider the single, embedded sensor or actuator as the IIoT endpoint, while a system integrator may define that endpoint as a collection of such devices serving a particular function within a larger subsystem. The asset owner may consider an endpoint as a more complex system that is masked behind a gateway or edge device, such as a wind turbine or cooling tower. See Figure 1.

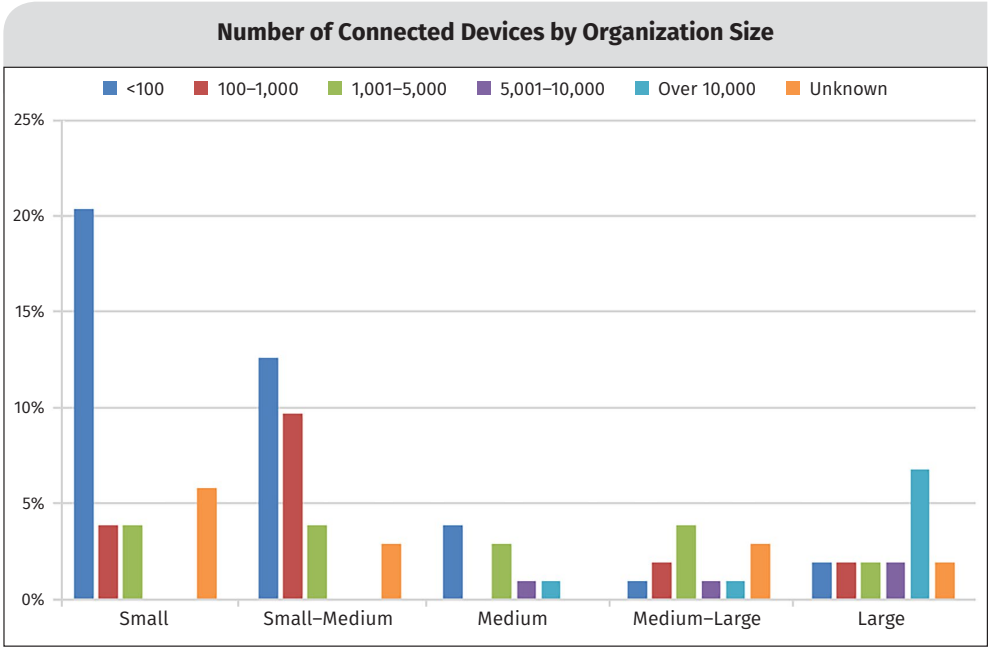


Figure 1. Number of Connected Devices by Organization Size

Given this range in the definition of an IIoT endpoint and the somewhat confusing relationship to a device, the actual number of IIoT devices may be understated here, pointing out the need for asset management—knowing what you have and how it is configured—and its importance in maintaining a secure infrastructure. It is hard to protect what you do not know about!

Endpoints are everywhere in an IIoT landscape, whether making a direct or indirect connection. An endpoint should be characterized specific to the IIoT system of which it is a part, especially if the endpoint requires configuration or programming based on its intended use in the system. This is essential to develop appropriate protective mechanisms against known and, in some cases, unknown attack vectors. The IIoT community is embracing the development of best practices around endpoint security, as described by the IIC white paper, "Endpoint Security Best Practices," published March 12, 2018.[5]

The Industrial Internet Consortium (IIC) Vocabulary defines an **endpoint** as a "component that has computational capabilities and network connectivity."[6]

IIoT endpoints support two basic connection types: "**Direct**: where the [endpoint] can either talk as a client … to whatever remote online application it interfaces with or where it can be seen online as a server; and **indirect**, where communication to the IIoT is mediated by some method other than IP."[7]

[5] www.iiconsortium.org/press-room/03-12-18.htm

[6] www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.0.pdf, p.11.

[7] www.networkworld.com/article/2165483/data-center/indirectly-connected-to-the-internet-of-things.html

IIoT Device Utilization

More than 56% of respondents are using their connected devices in IIoT systems to collect data for monitoring (71%); status, alarms and alerting (69%); and predictive maintenance (56%), as opposed to directly controlling operations and processes (53%). See Figure 2.

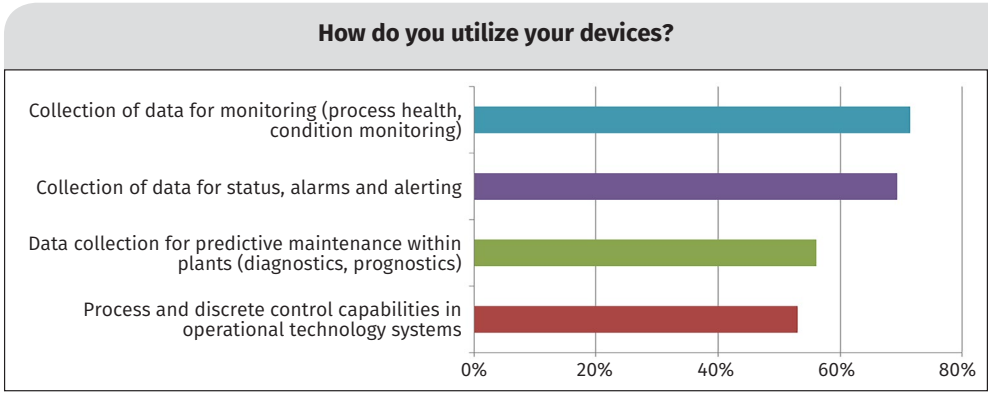


Figure 2. IIoT Device Utilization

The high utilization of devices for monitoring, and status, alarms and alerts points to the likely trend of retrofitting legacy systems with additional new sensors as a cost-effective way to gather key data for predictive/preventive maintenance purposes and to optimize performance (for example, replace previously manual processes) and improve productivity (complement the absence of personnel). To put this in perspective, review Table 1. The presence of non-IP (Layer-2, Serial, USB) in the OT network side at Level 1 (Process Control) and 0 (Instrumentation) may also indicate the added use of older, specialized devices that are supplying local, historically nonrouted information to complement data supplied by newer IP-based devices—all of which create a more encompassing view of IIoT systems.

The connection method and cabling may provide a clue as to whether this is the case. Physically wiring these connections can be expensive due to installation costs and network upgrades. Portions of systems may be difficult to reach, in an environmentally unfriendly location, or be part of moving or rotating equipment—making wired connections impractical or impossible. Here, wireless can be a cost-effective, if not the only, viable connection method, especially if the devices are not considered mission critical. Comparing device utilization with the connection method does show that the use of Wi-Fi and cellular connections is higher for monitoring and status than for predictive maintenance and process control, suggesting that this may be a trend being followed by the respondents and a direct result of the practical and technical limitations of wired connections. See Figure 3.

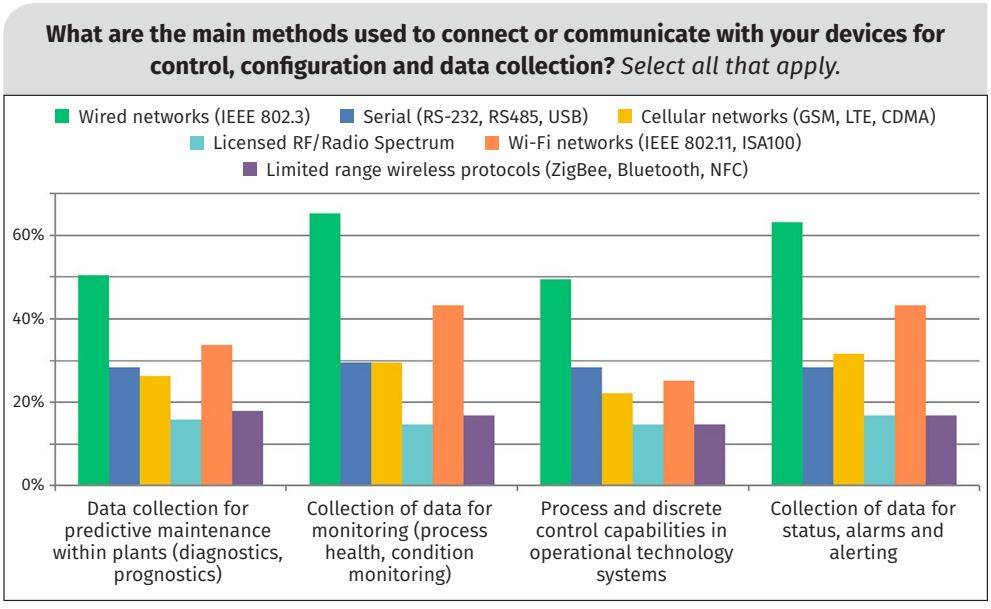


Figure 3. Communication Method Versus Device Utilization

Endpoint Management: Through the Network

Devices are managed through the network. Respondents depend on the use of Internet protocols to control, configure and collect data from devices. The majority (72%) rely on Internet Protocol Suites.[8] The use of IP-based, domain-specific protocols[9] by 53% signals continuing adoption and displacement of proprietary, non-routable and point-to-point protocols used in control systems. See Figure 4.

For the 41% of respondents collecting specific security and operations data about the IIoT devices and systems on their network, the majority (82%) are using it for visibility and investigation, including incident response, disaster recovery and forensics.

What are the main protocols used to connect or communicate with your devices for control, configuration and data collection. *Select all that apply.*

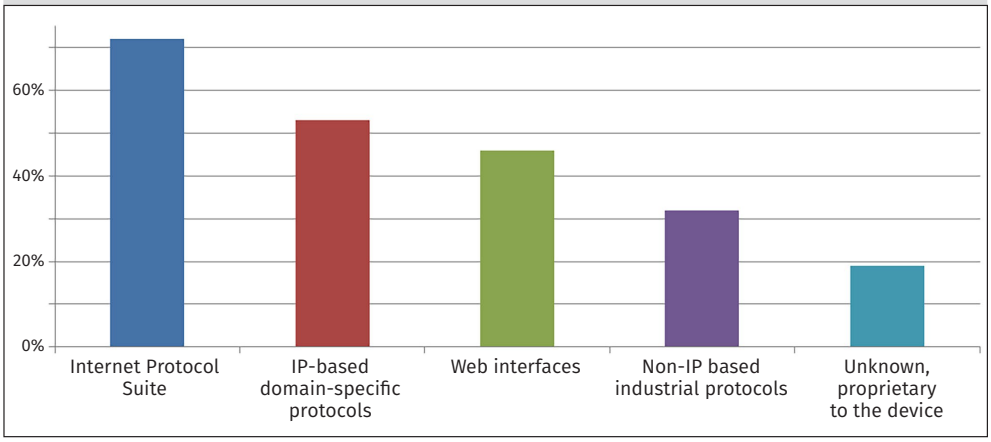


Figure 4. Main Protocols Used in IIoT

BEST PRACTICES

Lightweight, easy to implement, and included in almost all of today's IP-based products, the use of Web services to interface with devices is also popular, despite concerns and challenges from both IT and security perspectives, not to mention difficulty with enterprisewide asset management leading to risky configuration inconsistencies among devices. When using a Web-based interface to communicate with IIoT devices, be sure to identify and address potential concerns and the resulting vulnerabilities:

- Change default passwords, watch for hard-wired passwords and strongly consider adopting password rotation mechanisms that avoid password duplication and re-use.
- Manage IIoT assets and develop and maintain a real-time inventory that includes your connected devices. Use this inventory to keep products up to date, ensuring that all patches and updates are from approved and trusted sources.
- Ensure that vulnerability disclosures related to the product or services employed by the product are carefully considered and, when possible, patch products or add compensating technical and nontechnical controls to mitigate risks.
- Disable unnecessary ports and services, and monitor network traffic for future indications of activity to those ports or services. This can also help guard against non-network-based vulnerabilities such as direct connections into the device.
- Test products in a highly controlled environment absent of safety risks to personnel, machinery and the environment for vulnerabilities that range from resource exhaustion and denial of service to buffer overflows and cross-site scripting that increase exposure to data leakage.

[8] Internet Protocol Suites include TCP- or UDP-based network connectivity technology such as TCP and UDP over IP, DDS Interoperability Real-Time Publish-Subscribe Protocol (DDSI- RTPS), binary encoding technology, Constrained Application Protocol (CoAP), or MQTT (formerly MQ Telemetry Transport).

[9] Examples of IP-based domain-specific protocols include BACnet, DNP3, EtherNet/IP, Modbus/TCP, OPC Unified Architecture (OPC-UA) and Profinet, among other IP-based industry-focused protocols.

The top three data collection methods emphasize use of network logging, scanning and traffic analysis. Nearly 50% of respondents employ device-specific configuration and monitoring software, and 32% use manual, nonautomated interaction with IIoT connected devices—a sign that even with network connectivity and increasing automation, human interaction with IIoT is still prevalent for nearly one in three asset owners. See Figure 5.

How are you collecting security and operations data about IIoT devices on your network? *Select all that apply.*

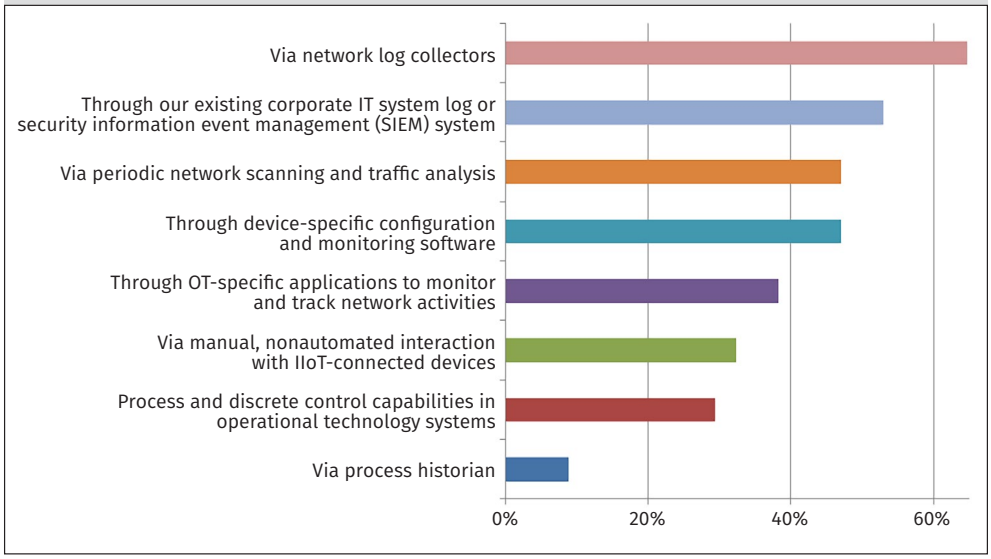


Figure 5. Collection Methods for Security and Operations Data for IIoT Devices on the Network

These results demonstrate the need to increase visibility into a wide array of IIoT endpoints through automation and what one presumes will become growing pressure to reduce manual processes of gathering security and operations data from IIoT devices locally. This goal, however, will remain problematic because not all IIoT devices conform to consistent communication and data-output standards, readily providing the same level of data as IT-grade assets. Greater consistency will be necessary in the future regarding the IIoT protocols that are employed, and in how and in what format data is presented by endpoints.

Thirty-eight percent turn to OT-specific applications to monitor and track network activities. Diagnostic and prognostic data in OT systems are excellent indicators of what expected or normal operations look like. Abrupt changes or abnormal trends over time, such as reduced output, reduction in quality, intermittent disruptions, premature wear or other seemingly erratic behavior, could indicate an accidental or malicious tampering, configuration change, or merely the presence of a threat inside a system. However, automated security tools do not typically use such process-oriented operational diagnostic and prognostic data to evaluate the security posture of a system and whether that posture has changed. The network becomes the common ground for indication of compromise based on changes to communication activity and content. Tools are needed here that overcome the limitations imposed by vendor-specific protocols or the use of agents that may disrupt operations.

The growth of IIoT is a critical sign that measures are needed to make everything interoperate between IT and OT, which are increasingly converging. Respondents rely on variety of approaches, guidelines, frameworks, standards or governing methodologies to drive their security in the use of IIoT devices, as illustrated in Figure 6 on the next page.

Overall, 79% combine one or more of these approaches, guidelines, frameworks, standards or governing methodologies, with the majority (37%) using at least three. Most (57%) cite use of NIST Cybersecurity Framework (CSF) which is, it's important to note, a guideline of guidelines since it includes mappings to other prominent standards. Following NIST CSF may also mean following NIST 800-82 and NIST 800-53 guidelines, ISO 27001, ISA/IEC 62443, and, as several mentioned in the open-ended response to this question, the CIS Critical Security Controls.

BEST PRACTICES

Establish your own long-term strategy to achieve IIoT cyber hygiene within your organization. Pay special attention to IIoT endpoint management, especially in terms of asset inventory, asset configuration and continuous monitoring of those assets.

Which, if any, approaches, guidelines, frameworks, standards or governing methodologies are driving your security in the application of IIoT devices?
Select all that apply.

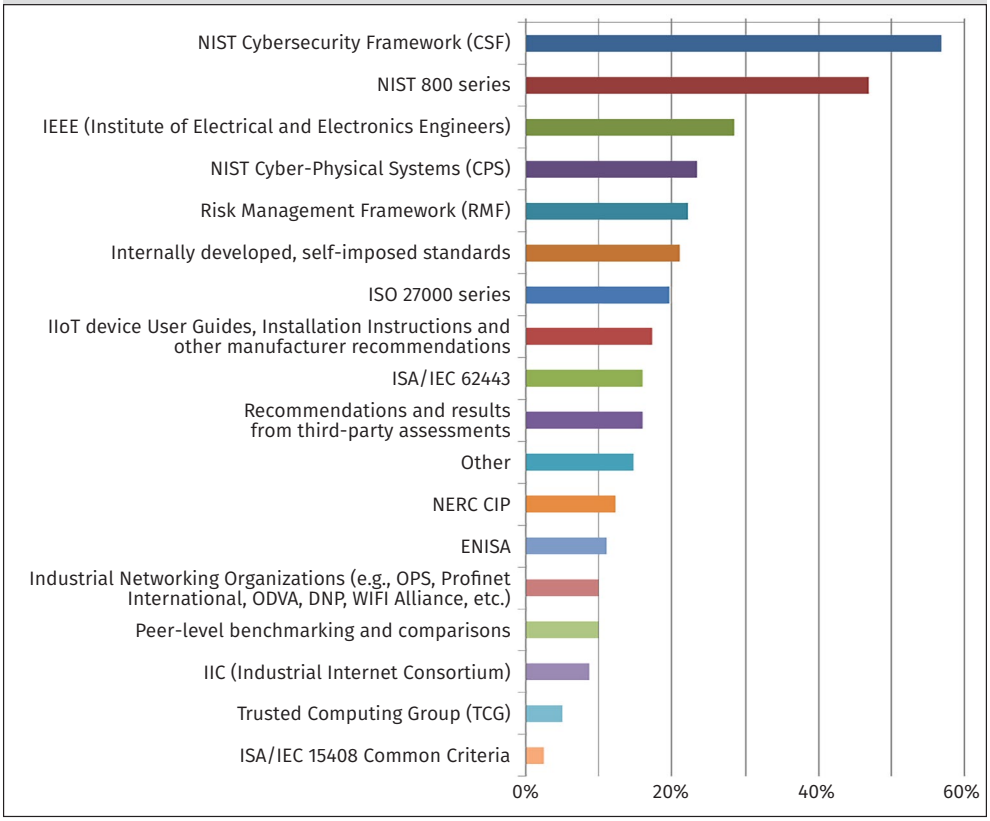


Figure 6. Standards and Guidelines Applicable to IIoT Security

Endpoints, Not the Network, Are the Primary Worry

Overall, by choosing embedded software/firmware and devices most frequently, respondents ranked endpoints, as opposed to networks, as being the most vulnerable aspect of an IIoT solution, thus presenting the most risk. See Table 2.

Table 2. Most Vulnerable Aspects of the IIoT infrastructure

Aspect	Response
Data accessibility, reliability, availability and integrity	14.1%
Embedded software/firmware: reliability, availability and integrity	14.1%
Embedded devices: safety, reliability, availability and integrity	12.0%
General endpoints: reliability, availability and integrity	12.0%
Networking and infrastructure appliances	9.8%
Specific systems related to IIoT (process logic, data historians, HMI/operator interface)	8.7%
Personnel (insider threat, human error)	7.6%
System-level software (operating systems): reliability, availability and integrity	6.5%
Security infrastructure appliances and controls	5.4%
Secondary safety systems, including Safety Instrumented Systems (SIS)	3.3%
Other	3.3%
Data and system backups for Business Continuity & Disaster Recovery	2.2%
Databases	1.1%

However, when asked what practices, policies, procedures, methods and technical implementations are currently used to protect against the risks imposed by IIoT devices and systems connected to their networks, respondents selected network-based controls as the top three, as shown in Table 3.

"Concern over endpoints, including their design to be resilient against attack, may stem from the view of IIoT more as a device or collection of devices than as an entire system, compounded by the variety, scale and complexity of these devices, including the lack of standardization that makes interoperability possible."

—Doug Wylie, Director, SANS Industrials and Infrastructure Practice Area, personal communication

Table 3. Controls Currently Used to Protect Against IIoT Risks

Controls currently used to protect against IIoT risks	Response
Network segmentation using firewalls, data diodes, IT/OT gateways	67.8%
Physical and logical network separation, segregation and overlay of security zones and conduits model	46.7%
Network monitoring, identifying, analyzing and emphasizing unusual connections and communication behaviors	45.6%
Restriction of physical access to critical IIoT control systems and mission-critical applications	41.1%
Physical and logical inventory of connected systems	41.1%
Maintain current patch/updates at the device level	40.0%
Policies for the secure use, operation and management of IIoT devices and systems in your enterprise	37.8%
Specific employee awareness and training around IIoT	37.8%
Endpoint protection methods	36.7%
Encryption technologies for data transfer and data at rest	36.7%
Authentication/authorization of connected IIoT devices to the network/systems (e.g., integration into AD/LDAP, use of PKI)	34.4%
Standard Operating Procedures (SOP) that support your IIoT policies	28.9%
System/endpoint monitoring, identifying new device connecting without permission	25.6%
Security evaluation/testing and vetting of new IIoT devices prior to placing into operational systems	25.6%
Embedded system security solutions	18.9%
Cloud-based methods for monitoring, management and control of devices	17.8%
Secure APIs	13.3%
Geolocation services enabled at the device level for tracking	5.6%
Other	3.3%

While device-level concerns are significant, remediating endpoint risks depends on the network infrastructure as a compensating control. Only 40% of respondents (two out of five) indicated they apply and maintain current patches and updates at the device, implying that three out of five (60%) are not using device-level patching to protect IIoT devices and systems.

This high percentage suggests that the majority have not established and/or are not following a formal endpoint patching program to protect their IIoT devices and systems. Factors may include: knowledge of whether a vulnerability/patch applies to the devices in their environment, confidence in the resilience of these endpoints or, more likely, a perception that these patches are not effective, given the trade-offs that include difficulty in the actual patching process, or risk or disruption to the ongoing operation of critical IIoT systems. This latter element is crucial in industrial control—avoiding disruption of critical processes is a major factor often inhibiting security practices.

So despite the *endpoint* presenting the greatest concern, the *network* remains the focus for control efforts. One way to underscore this divergence is to ask: Who in the organization takes primary responsibility for managing IIoT risks imposed by IIoT devices connecting to the Internet and the internal network? See Figure 7.

Who in your organization takes primary responsibility for managing the risk imposed by new or existing IIoT devices connecting to the Internet and your network?
Select all that apply.

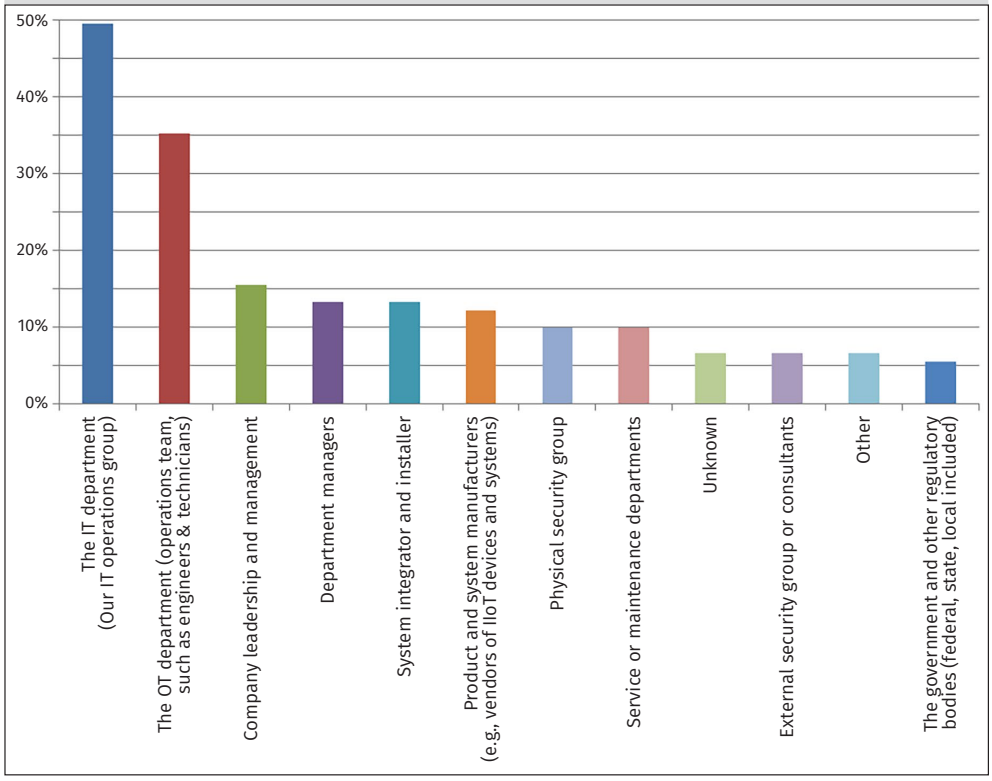


Figure 7. Responsibility for Managing IIoT Risk

Indeed, it appears to be the IT team that takes that primary role, regardless of the size of the organization. IT feels that the defensible network architecture design and management are fully within their control, while IIoT endpoint device configuration and management are largely out of their control, belonging to OT.

Within each of the responsible segments, the perception of what part of the IIoT is most vulnerable and at risk depends on where the responsibility for managing IIoT risk lies:

- The IT team, company leadership and management tend to emphasize data accessibility, reliability, availability and integrity.
- Department managers emphasize networking and infrastructure appliances.
- The OT team emphasizes the specific systems related to the IIoT endpoints and then the devices.

These differences are exposed in Table 4.

However, while endpoint risk is the driver, the network remains the enabler of security. Nearly 69% of IT, and more than 83% of OT department managers, respectively, selected network segmentation using firewalls, data diodes and IT/OT gateways as the leading control for protecting against the risks imposed by existing or new IIoT devices. Hardening the network reigns supreme as the most favored mechanism to address device-level risks with IIoT products and systems. Company leadership and senior management backs this network-centric focus, with 71% emphasizing authentication/authorization of connected IIoT devices to the network/systems (e.g., integration into AD/LDAP, use of PKI) and network monitoring, identifying, analyzing and emphasizing unusual connections and communication behaviors. It

Table 4. Top Aspect for Risk Based on Role

Category	Top Risk	Top Control
IT Department	1. Data Accessibility, Reliability and Integrity, and Embedded Software (20.0%)	1. Network Segmentation (68.9%)
OT Department	1. Specific Systems Related to IIoT (18.8%) 2. Embedded Software and General Endpoint (15.6%)	1. Network Segmentation (83.3%)
Company Leadership and Management	1. Data Accessibility, Reliability and Integrity (21.4%) 2. Embedded Devices, Networking and Infrastructure Appliances, and Specific Systems Related to IIoT (14.3%)	1. Network Monitoring and Authentication/Authorization of Connected Devices (71.4%)
Department Manager	1. Networking and Infrastructure Appliances (25.0%) 2. Embedded Devices and Security Infrastructure Appliances and Controls (16.7%)	1. Network Segmentation (83.3%)

is striking that the company leaders differ from other categories in their most-cited security controls.

The top control cited by company leadership—network monitoring and authentication/authorization services of connected devices—suggests that this group places a higher value on the *identification* and *detection* of threats (i.e., what is connected to the system and what is it doing?). This result is in high contrast to other roles who rated network segmentation as a top control, a security control that fulfills a *protective* and *preventive* function in the architecture.

BEST PRACTICES

The endpoint is the driver; the network is the enabler. A sign of security maturity is the use of good network design practices for segmentation and separation, as well as monitoring and access controls:

- Develop an effective strategy for logical network segmentation, emphasizing both physical boundaries and known IIoT perimeter locations where IT and OT systems must converge.
- Develop comprehensive networkwide monitoring for unusual, unexpected activities and behavior. Monitoring needs to span the local networks and the internal routes between devices, systems and subsystems. Pay particular attention to locations where communications between IIoT devices, systems and external sources cross trust boundaries and perimeters via the Internet.

IIoT Security Drivers

Overall, the top drivers for IIoT security included brand, line-of-sight financial loss, information and asset protection, and compliance with industry regulations more than safety, both inside and outside of the operation. In other words, these results indicate business investment and impacts trump the priority to protect employees and the community. In fact, blending IT and OT responder answers, the protection of equipment and systems was nearly 7% higher in priority than safety inside the operation, and disturbingly, nearly 25% higher than safety outside of the operation. See Table 5.

Table 5. Critical Drivers for IIoT Security and Rankings by Responsible Party

Driver		Overall Response	IT Team Rankings	OT Team Rankings
1	Protection of data (company, customer, vendor, other)	47.2%	1	6
2T	Protection of equipment and systems	40.5%	4T	3
2T	Protection against financial loss (assets, brand, company value)	40.5%	2	4T
4T	Compliance with industry regulations	36.0%	3	4T
4T	Increases in reliability, availability, efficiency, productivity	36.0%	4T	1
4T	Safety inside the operation	33.7%	6	2
7	Integration and synergistic alignment of IT and OT practices, policies and procedures	23.6%	7T	7T
8	Reduce corporate liability/improve enterprise risk management	16.9%	7T	9T
9	Safety outside of the operation	15.7%	9T	7T
10	Mitigate supply chain risks, both upstream and downstream	9.0%	9T	9T

However, who has the responsibility for IIoT risk management affects driver ranking because perceived and actual responsibilities can differ. The IT team is most concerned with the protection of data, guarding against financial loss and compliance with industry regulations, while the OT team emphasizes increases in reliability, availability, efficiency and production, safety inside the organization, and protection of equipment and systems. Even for OT, while safety in critical infrastructure is often cited as a paramount driver, pressures to maintain operations carry greater significance.

A Matter of Perspective: Threats and Risks

Overall, the majority of respondents (59%), regardless of organization size, are only somewhat confident in their organization's ability to secure their IIoT devices. See Figure 8.

Interestingly, members of the OT department—the individuals who are likely the most knowledgeable about IIoT implementation—appear to be the least confident in their organization's ability to secure these devices, while company leadership and management, including department managers, appear to be the most assured, as illustrated in Figure 9.

"Members of the OT department, the individuals who are likely the most knowledgeable about IIoT implementation, appear to be the least confident in their organization's ability to secure these devices, while company leadership and management, including department managers, appear to be the most assured."

The discrepancy in the views of management and leadership from OT in the company's capability to secure IIoT is problematic. Such pronounced disparity surely leads to challenges for the OT group's ability to secure budget for such investments as ongoing security skills-building, technologies and services to help safeguard operations, and resources to respond and recover to incidents. The same data may also suggest an overall leadership and management perspective that current company security investments in IIoT are somehow adequate—or at least deemed adequate enough to counteract current risks to the overall business.

Given the current state of your security program (people, policies, processes, controls and technology) how would you rate your organization's ability to secure your IIoT devices?

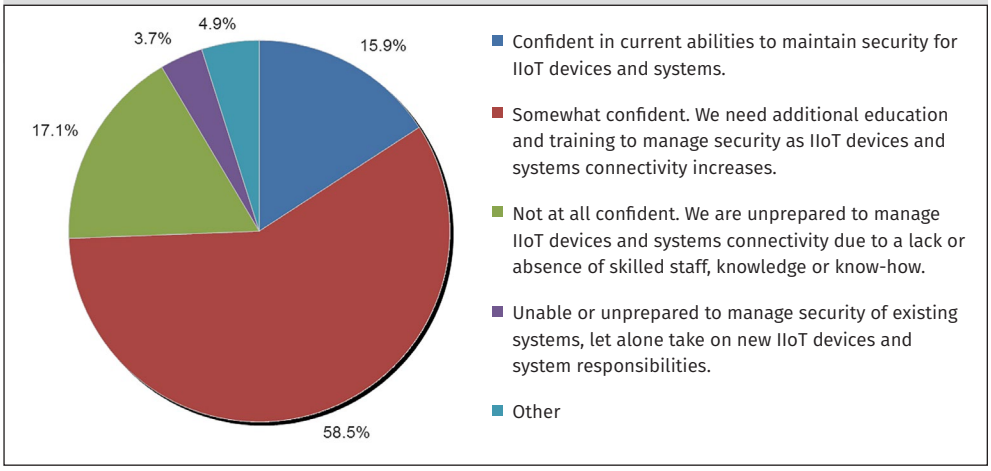


Figure 8. Current State of Security Program Regarding IIoT

Given the current state of your security program (people, policies, processes, controls and technology) how would you rate your organization's ability to secure your IIoT devices?

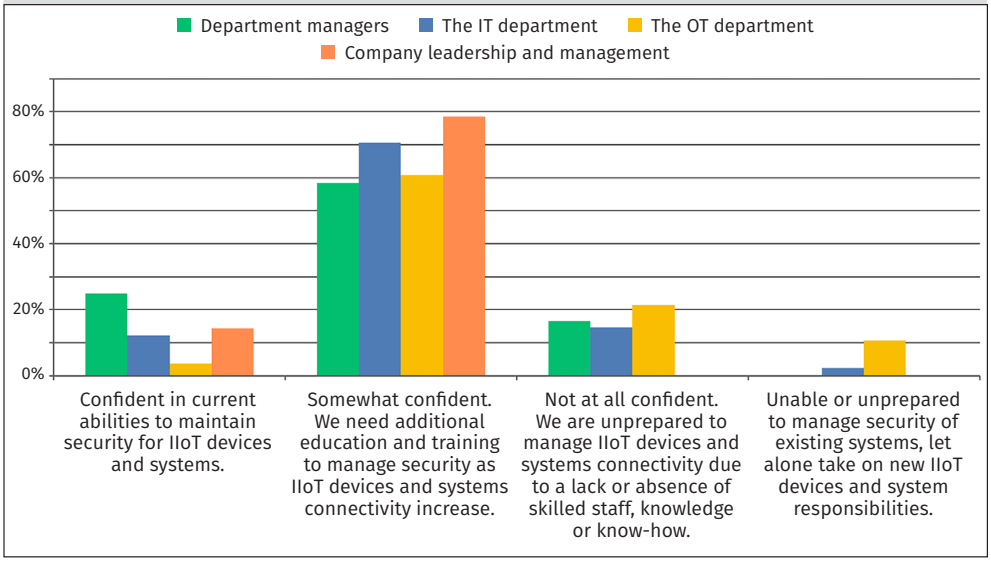


Figure 9. Confidence by Role for IIoT Risk Management

Threats and Vulnerabilities

Confidence in being able to secure an organization's IIoT infrastructure depends on understanding the threats and risks to be faced, especially in light of the complexity that stems from allowing external connectivity for OT systems and adding a growing number of devices that expand effort to manage asset inventory, device and system configuration, and change management. The results are presented in Table 6.

In line with Figure 2 (on page 8), patching and product upgrades are trouble spots and are expected to remain so for the next two years. The recognition by so many that IIoT devices will be vulnerable and remain vulnerable due to lack of patching exposes how investments in infrastructure hardening may continue to be viewed as a sufficient security strategy to adequately protect IIoT systems.

Risk

Respondents (48%) acknowledge that the two-year outlook for the leading risk to IIoT security is not performing "security by design" through a design, build, operate and maintain life cycle. The opportunity to address cyber risk starts at the beginning of the system development cycle and procurement phases, with an emphasis both on the network infrastructure design and the endpoint selection. Collectively, the top five in respondent's concerns are actually a mix of risks introduced by a combination of IIoT vendors, integrators and end users, requiring shared responsibilities to mitigate and remediate risk in these systems. See Table 7.

Table 6. IIoT Concerns over the Next Two Years

	Greatest Challenges in the Next Two Years	Response
1	Difficulty or lack of patching IIoT devices and systems, leaving them vulnerable	55.95%
2	Accidental exposures resulting from user error and system complexity	41.67%
3	Difficulty controlling, locating, tracking, preventing and managing IIoT connectivity to critical infrastructure and other mission-critical systems	39.29%
4	Failure to incorporate good security practices into the IIoT design, build, operate and maintenance lifecycle models for systems	39.29%
5	IIoT "Things" used as infection vectors to spread in the enterprise	34.52%
6	Multivendor environment without device and technology standardization	29.76%
7	Denial of service attacks on IIoT devices and systems that cause damage or loss of life	25.00%
8	Shortage of vendor investments to incorporate security into the design of IIoT devices, systems and supporting products	19.05%
9	Sabotage and destruction of connected IIoT devices and systems	13.10%

BEST PRACTICES

Threats are constantly evolving, and for IT and non-IIoT devices, there are instances where product patching could have at least raised the difficulty for an attacker to meet an objective. For this reason, implementing disciplined change management, careful endpoint selection, reducing endpoint and network complexity, and closely monitoring IIoT connections and communications all remain highly suitable recommendations, in addition to the best practice of developing and executing ongoing IIoT patching procedures.

Table 7. Greatest Concerns for IIoT Security Over Next Two Years

	Risk	Response
1	Lack of security considerations in product and system installation, configuration, service, support and maintenance	47.6%
2	Shortage or absence of adequate security considerations in IIoT product design and manufacturing	39.3%
3	Pace or lack of updates for vulnerabilities to OS, firmware or other software for IIoT devices	38.1%
4	Creating new attack surfaces that expose or enable additional vulnerabilities such as related to the command and control (C2) channel to a IIoT device and system	34.5%
5	User–introduced vulnerabilities for IIoT devices through oversight, misconfiguration and user-error	32.1%
6	Potential loss of sensitive data enabling more sophisticated attacks	23.8%
7	Shortage or absence of adequate security considerations in system design and manufacturing	23.8%
8	Negative impact on system safety posture or ability to maintain safe operation or shutdown	22.6%
9	Impacts from conflicting operational priorities in solutions that span safety, security, reliability, resilience and privacy	19.1%
10	Lack of relevant, sensible and enforceable industry standards on IIoT devices and systems	17.9%
11	Other	1.2%

Continued Investment in the Network

Most respondents continue to invest in network-related controls. See Table 8.

This should come as no surprise. IIoT solutions typically rely on persistent connections between endpoints, with uptime being paramount. OT data pushed through these connections is usually carefully selected, deterministic and repeatable. This means that unusual communication patterns and behaviors can be very effective indications of configuration problems, impending fault or failure, or malicious activities intended to disrupt or damage operations. Here, behavioral and rules-based security can help augment employee awareness and training as well as enforcement of policies for the secure use, operation and management of IIoT devices in the enterprise.

The high level of investment in employee awareness and training to build greater security knowledge, skills and abilities is a good indicator that broader capabilities to recognize and mitigate risk go beyond just technology, processes and policies. With nearly 48% of controls deployed in IIoT systems coming from investments in personnel, for the foreseeable future, IIoT is more likely to help secure related job roles than to put these roles at risk of replacement. This also indicates that relevant options and offerings related to security awareness and training are available and comprise today's budgetary spend.

TAKEAWAY

Invest in your personnel, growing their knowledge and skills to effectively manage risk throughout all phases of the IIoT system life cycle (design, build, operate, maintain). Educated personnel can have a positive effect on better system designs, better product selections and better life-cycle management. These investments, combined with vigilance and partner collaboration that extends into a company's supply chain, can also have a material effect on reducing risks often introduced during the procurement, factory-acceptance, installation and site-acceptance processes, as well as service/maintenance activities.

Table 8. Controls to be Deployed or Improved

Control	Response
Network monitoring, emphasizing unusual communication behaviors	57.3%
Employee awareness and training around IIoT	47.6%
Network segmentation using firewalls, data diodes, IT/OT gateways	43.9%
System/endpoint monitoring, identifying new device connecting without permission	37.8%
Security evaluation/test of new IIoT devices prior to placing into production	37.8%
Policies for the secure use, operation and management of IIoT devices in your enterprise	34.2%
Physical and logical inventory of connected systems maintenance	32.9%
Encryption	32.9%
Maintain current patch/updates at the device level	31.7%
Standard Operating Procedures (SOP) that support your IIoT policies	30.5%
Authentication/authorization of connected IIoT devices to the network/systems (use of PKI)	28.1%
Restriction of physical access to critical control systems and mission-critical applications	23.2%
Endpoint protection methods	20.7%
Cloud-based methods for monitoring, management and control of devices	18.3%
Secure APIs	18.3%
Embedded system security solutions	11.0%
Geolocation services enabled at the device level for tracking	11.0%
Overlay zones and conduits	9.8%
Other	4.9%

Convergence: Growth and Budget

Most organizations look for 10 to 25% growth in their connected devices. This applies across all sizes of organizations, although smaller organizations also appear less sure of their projected growth than larger organizations, as evidenced by the higher percentages of "Unknown" responses. See Figure 10.

This growth rate will cause the systems to which IIoT devices connect to double in size roughly every three to seven years, resulting in increased network complexity as IT and OT become more connected, demands for bandwidth, and the need for personnel skilled in best security practices related to the design, build and operation of IIoT systems.

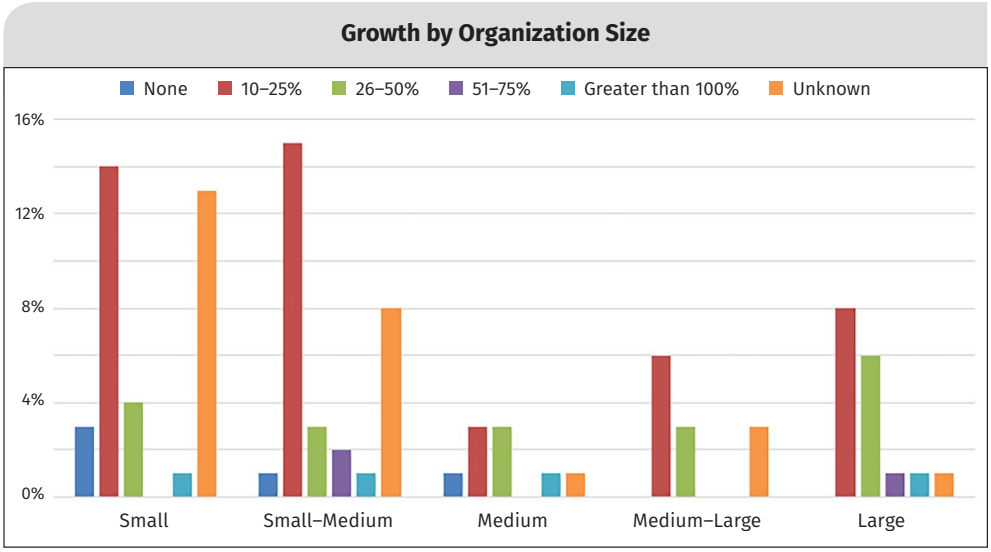


Figure 10. IIoT Growth by Organization Size[10]

TAKEAWAY

Every new connection expands an attack surface to the IIoT solution and other systems with which it interacts. While investments in personnel skills building is already recognized as important, ongoing personnel readiness will become a critical factor as threats evolve. Invest in security knowledge, skills and abilities (KSA) that encompass OT-based security demands to help reduce the risks that are already showing up in today's IIoT systems as they expand in size and complexity, and be prepared to evolve skills as the threat landscape changes.

Most respondents do not know whether their organization has an established budget for IIoT, as illustrated in Figure 11. This appears to be the case regardless of organization size, number of connected devices or projected growth in connected devices.

Organizations must invest some of their budget to enhance security for IIoT solutions, whether that investment takes the form of an IIoT-specific budget, or is created as separate from the overall IT or security budget. IIoT solutions create unique risks associated with rapid growth in the expanding volume of endpoints, broader connectivity, and ultimately higher degrees of remote accessibility as a byproduct of the benefits IIoT produces. Existing security budgets that remain fixed or are not properly matched against changing risks will likely be, or quickly become, inadequate for addressing IIoT risks in the short and long term.

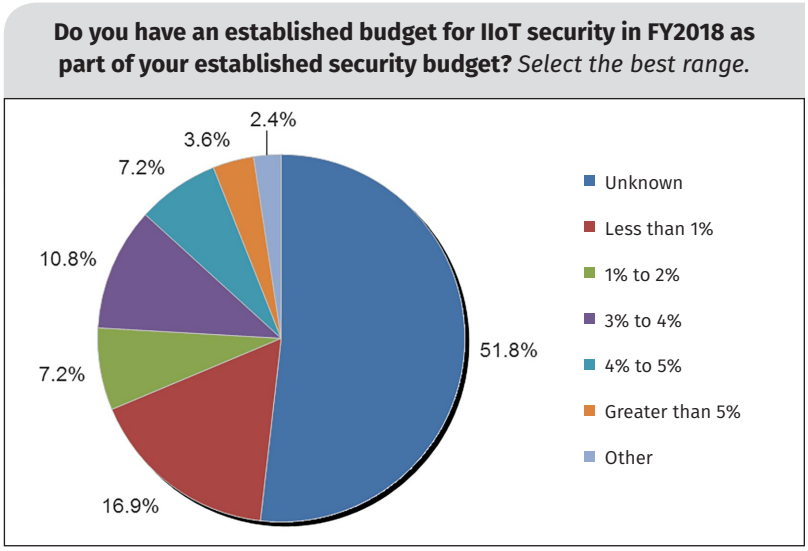


Figure 11. Budget for IIoT

[10] No respondents indicated experiencing 76–100% growth.

Conclusion

Critical systems must operate tirelessly as well as economically. IIoT-engineered solutions are being embraced because they promise to help stakeholders better meet operational objectives and facilitate improvements to system safety, reliability, resilience and privacy—all key factors in what the Industrial Internet Consortium (IIC) calls the *trustworthiness* of systems. These elements make IIoT solutions compelling, leading to greater and faster adoption rates across industries.

Today, an investment in IIoT offers improved productivity, increased performance and efficiency for greater intelligence and enhanced visibility into operations—but at what risk? The need to maintain a clear focus on business risks cannot be overstated as IIoT initiatives race ahead faster than asset owners and operators can react. Organizations need a road map that can guide stakeholders—users, integrators and vendors, asset owners and operators—in blending together formal definitions, data standards, common protocols, connectivity requirements and best practices to achieve the interoperability needed to have IIoT systems work together securely. The confusion over what constitutes an endpoint is just one example of why a framework specific to IIoT is needed.

IIoT has blurred traditional IT and OT infrastructure boundaries and their historically crisp edges and perimeters, such as those defined by the hierarchical Purdue Model and other industry standards such IEC 62443.[11] These models and standards are limited in their ability to provide adequate guidance for segmenting and safeguarding contemporary systems because none account for the borderless automation and control system architectures that IIoT has brought to industry.

Today's OT connections and interdependencies not only connect to the Internet, but for true IIoT solutions, they rely on it as a conduit to reach enabling Internet-based services. And as of this writing, no internationally recognized standard yet embodies a comprehensive reference architecture that can aid companies in their pursuit of reducing security risks to IIoT solutions. However, some progressive companies are starting to provide independent guidance, and there are even broader multicompany efforts such as those by the Industrial Internet Consortium (IIC) that continue to advance recommendations for good IIoT design practices via efforts such as the Industrial Internet Reference Architecture (IIRA) v 1.8.[12]

Multivendor interoperability issues also hamper adequate visibility into the security posture of IIoT devices and systems. Many devices do not conform to consistent standards, such as communication protocols, enabled or disabled services, or methods for configuration, all of which make engineering, security, and management across these endpoints and the overall system difficult. OT-specific applications provide diagnostic and prognostic information that could flag abnormal activities for action, while IT-oriented network-level tools do not typically use such information.

---

[11] https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf

[12] www.iiconsortium.org/IIRA.htm

While the IIoT community grapples with the operational constraints imposed by the inconsistent state of its technology as implemented by the growing assortment of device vendors, what can organizations do to improve their IIoT security? The results of this survey suggest that organizations should:

- Evaluate and vet product and services vendors, suppliers, consultants, contractors and service personnel for basic security skills and ensure that security responsibility is well understood and maintained.
- Challenge any and all IIoT providers to demonstrate clear indicators of security quality and maturity in the solutions they provide, including evidence and artifacts of continuous improvement to the security posture of a product and system.
- Establish clear and open lines of communication within the supply chain to ensure proactive, two-way information exchange relating to matters that can affect risks to IIoT systems.
- Strengthen their life-cycle management procedures, especially for asset inventory and management, configuration management, and change management to address the complexities of IIoT. Respondents cited the failure to incorporate good security practices in the IIoT life-cycle models for systems as among the top threats for the next two years. One source that—though not specific to IIoT—can be tailored to meet the needs of such systems might be the CIS Critical Security Controls,[13] a recommended set of actions for cyber defense.
- Review their internal and external approach to both network engineering and network security. IIoT depends on the network to enforce security at the endpoint (and across the system.) Organizations need to determine the maturity of their security as measured by the use of good design practices, such as segmentation and separation and by operational procedures, such as monitoring and access control.
- Harmonize the viewpoints of IT and OT teams and any third-party remote product and service providers, especially as related to IIoT security requirements, threats and risks. IIoT will eventually narrow the cultural gaps that normally exist between IT and OT. These solutions require shared responsibilities. IT controls the network, which enables IIoT to reach Internet services. OT best understands the business impact from a compromised IIoT system or endpoint. Both IT and OT need to understand the risks imposed by new or existing IIoT devices connecting to the Internet and the corporate network. And, both need to know how to track and manage these risks as a team.
- Converge internal stakeholder views concerning IIoT business drivers, language and perspectives of what constitutes cyber risk and establish a uniform set of funded priorities across corporate leadership, management, and IT and OT teams. If the OT team says the IIoT infrastructure is not defensible but management believes that it is, such a difference can result in IT or security budgets that do not grow sufficiently to ensure the growth of secure IIoT.

[13] www.cisecurity.org/controls

About the Authoring Team

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Doug Wylie (advisor) directs the SANS Industrials and Infrastructure business portfolio, helping companies fulfill business objectives to manage security risks and develop a security-effective workforce. His lengthy career spans a wide array of industries. He served as Rockwell Automation's director of product security risk management, where he founded and led its industrial cyber security and risk management program. Doug works around the world with companies, industry and standards bodies, and government entities to help safeguard converged IT-OT systems from contemporary cyber security threats. He holds the CISSP certification and numerous patents, as well as being an accomplished writer, speaker and presenter.

Sponsor

SANS would like to thank this survey's sponsor:

ForeScout

With special thanks to:

ARC Advisory Group

industrial internet CONSORTIUM