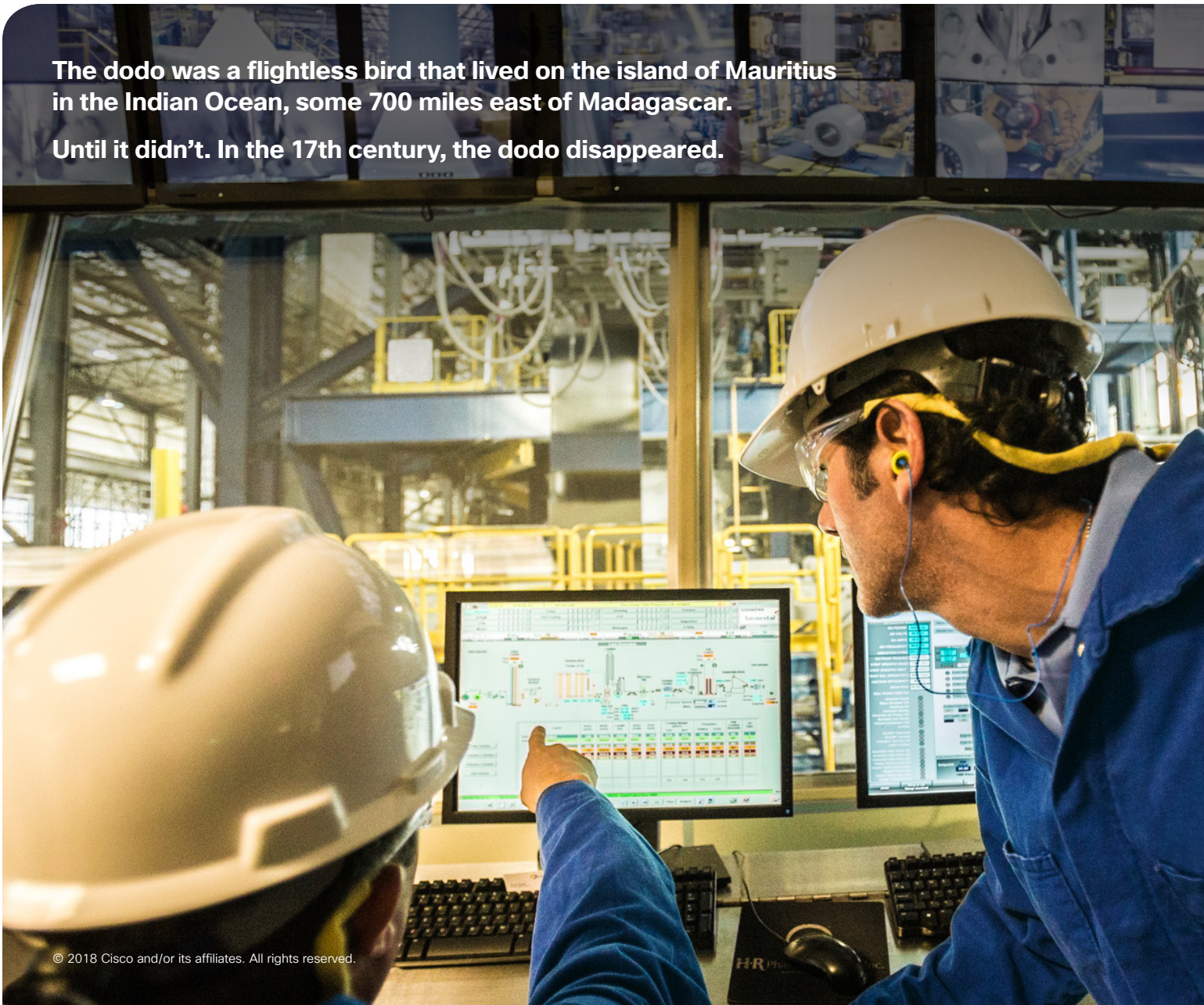
White paper
Cisco Public

Securing Industrial IoT-Enabled Critical Infrastructure



Whether you are a team leader, or a current or potential IT, OT or security professional, you need to understand all of the issues involved in keeping critical IIoT setups safe.

The digital revolution sweeping across business and government worldwide may well cause organizations and careers to fade away or even flame out, but an educated workforce can stay on top of these challenges. The Internet of Things (IoT) is merging information and operational technologies. Industrial networks (operational technology, or OT) are blending with enterprise networks (information technology, or IT). Add to that a massive surge in the numbers of connected devices and machines that are the hallmark of IoT.

Industrial IoT leverages the power of IP networking to converge industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems with enterprise business logistics. Amid all of these profound changes, one of the biggest needs is security for industrial IoT (IIoT) networks and connected ICS and SCADA components. In industrial environments, connected devices aren't some futuristic concept. Manufacturers have been using sensors on the factory floor for a decade or more. Today, the gap between IT and OT continues to close.

With sensors already installed and analytics technologies becoming more widespread, it's a whole new frontier.

Whether you are a team leader, or a current or potential IT, OT or security professional, you need to understand all of the issues involved in keeping critical IIoT setups safe.

This digital shift presents a tremendous opportunity for every kind of industrial organization. As a business or project leader for an IIoT initiative, it is paramount for you to understand the complexity of IIoT networks and security requirements. And for every IT and OT security professional like you. Adjust to this change and evolve quickly, and soar beyond the digital dodos.

To help you get a handle on IIoT security, you need to understand the following concepts:

- The convergence of IT and OT
- An overview of IIoT industry growth
- The components of IIoT
- The IIoT security issues you need to know about
- The IIoT security skills you need today
- A review of what Cisco is doing to help skill the market, including our new IIoT security training course and relevant IIoT certifications

Understanding just what IIoT consists of will make its security issues much more obvious. It is a wired or wireless network of physical objects, systems, platforms, and applications.

Global IIoT: One hot market

The global IIoT market should reach $933.62 billion by 2025.[1] That is a CAGR of 27.8 percent. By 2030, IIoT could add $14.2 trillion in value to the worldwide economy.[2]

Manufacturers across a wide range of industries plan to invest $907 billion a year for five years in IIoT.[3] A lot of this investment will go for sensors and connectivity devices as well as software and manufacturing execution systems.

Thirty-one percent of manufacturers are adding IoT upgrades to their internal operations.[4] Another 56 percent are thinking about doing so. They want to cut operational costs. Make their supply chains more efficient. Make predictive maintenance even better. In the same recent survey, nearly 90 percent of industrial companies said they are at least looking at ways to use IIoT.[5]

The desire to lower production costs and increase output is moving industry to adopt IoT. So are other advantages, like greater productivity. Process automation. Shorter time-to-market. In addition, lower sensor prices make it cheaper to collect and analyze data. By merging IT and OT, IIoT should boost overall productivity. It also should make operations more efficient. It will improve visibility and make different industrial processes simpler to manage.

Other factors driving IIoT adoption include widespread use of cloud computing and the improved ability of IPv6 to connect machines and sensors. Moreover, cheaper sensors and long-range wireless technology (like LoRa) make IIoT less costly to set up. However, other issues could limit global IIoT growth. These include the lack of a defined protocol or standardization and use of old equipment. Plus, no live technology deployments are possible without good cybersecurity implementation in place.

Bumps in the IIoT road

The IIoT revolution and its vast potential are tantalizing, certainly. There's always a fly in the ointment, though. At least two flies, in this case, and one of them has been mentioned already. It is security. Frankly, IIoT presents a security challenge on a scale never seen before.

Understanding just what IIoT consists of will make its security issues much more obvious. It is a wired or wireless network of physical objects, systems, platforms, and applications. Inside all of these components is technology that enables each one to talk to the others, pick up intelligence about the external environment, and share it all with people.

1. Grand View Research, "Industrial IoT Market Size Worth $933.62 Billion by 2025 | CAGR: 27.8 Percent," April 2017.
2. Accenture, "Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth," January 2015.
3. PwC, "Industry 4.0: Building the Digital Enterprise," April 2016.
4. PwC and MAPI, "Monetizing the Industrial Internet of Things," July 2017.
5. Ibid.

IIoT's sheer complexity, diversity, and potential size, plus the critical nature of many of these connected machines make it a total security nightmare. How do you keep all of these networked things safe from hackers?

Sensors of all types abound in IIoT. There are all of the various parts of the network too. Hooked into IIoT are mobile devices like smart phones or tablets, as in the consumer-focused IoT. There is also software for a wide range of functions. But where IIoT really moves into security overdrive, in a manner of speaking, is in all of the machines that either already are connected or could be.

This list has no limits. It includes any machine already existing or devised in the future. Car and truck engines. Wind turbines. Boat engines. Shipping cargo containers. Robots. Additive (3D) printers. Oil and gas drills. Combine harvesters. Assembly line conveyors. Steam pressure valves. HVAC compressors. Traffic lights and cameras.

IIoT's sheer complexity, diversity, and potential size, plus the critical nature of many of these connected machines make it a total security nightmare. How do you keep all of these networked things safe from hackers? Every component and every connection is a potential vulnerability. And in some instances, a security breach is a matter of life or death. Hospitals have been taken offline by ransomware. As wireless-enabled medical implant technology becomes more widespread, it will become possible to attack connected pacemakers or insulin pumps.

Suppliers of specialized industry equipment are pushing to connect their business systems to more quickly take advantage of new capabilities. In the rush, many are doing so without a security background. Or without fully understanding the security implications of how their new, connected devices and sensors affect the overall security of the organization or factory that they're being installed in.

As a result, security issues in newly networked or connected equipment can shut down a part of the factory, or even the whole factory itself. Common points of vulnerability are as follows:

- Misconfigured devices
- Devices that do not have appropriate security controls around them
- Devices that bypass plant security measures
- Devices with malware or security flaws built into them

Almost half of manufacturing executives surveyed recently were not confident that their assets were protected from external threats.[6] Yet half of the organizations polled perform weakness assessments for industrial control systems less than once a month, and 31 percent have never done this kind of test.

Relying on linked products brings a new set of risks to manufacturers too. Almost half (45 percent) of those surveyed said their organizations use mobile applications, and 35 percent said sensor controls. Yet 40 percent had not yet added connected products to their cyber incidents response plan.

6. Modern Materials Handling, "Deloitte and MAPI study: Connected Industrial Control Systems Expose Manufacturers to Cyber Threats," November 2016.

More sophisticated state-sponsored or terrorist attacks on critical infrastructure can damage and disable the target government or organization. The December 2015 cyberattack on the Ukraine power grid paralyzed the entire system.

Seventy-six percent of manufacturers said they already transmit product data using Wi-Fi, while 52 percent reported that their connected products store or send confidential data like Social Security numbers or banking information.[7] And the flaw discovered with the Wi-Fi Protected Access II (WPA2) security protocol that allows attackers within range to access supposedly encrypted data is placing that information at risk.[8]

No enterprise today would start an IoT deployment without security considerations. Yet IoT security will account for less than 10 percent of overall IT security budgets, while IoT-related threats are expected to account for more than 25 percent of reported enterprise incidents by 2020.[9]

Cybercriminals are always hunting for financial gain, intellectual property, and even business plans or strategies. Over the previous 12 months, the surveyed manufacturers said the highest number of events came from within their organizations (46 percent). Thirty-nine percent came from outside sources, and 15 percent from partners or vendors. Top threats included the following:

- Phishing/pharming (32 percent)
- Errors or omissions (26 percent)
- Abuse of IT systems (25 percent)
- Use of mobile devices (24 percent)[10]

More sophisticated state-sponsored or terrorist attacks on critical infrastructure can damage and disable the target government or organization. The December 2015 cyberattack on the Ukraine power grid paralyzed the entire system. And the follow-up attack in 2016 caused the nuclear plant monitoring system to go dark for hours.

As industrial verticals become IoT-enabled, it becomes ever more imperative to protect critical infrastructures in power grids, transportation and air traffic control, water management, energy pipelines, and public spaces.

Why does IIoT introduce more security vulnerability?

SCADA systems used to operate in a hierarchical network that was isolated from the outside and also from enterprise networks and were thus considered as protected by "air gap" security.

When all is interconnected via a common Ethernet backbone, the benefits of IIoT also introduce new threats to the infrastructure. First, vendor controllers

7. Ibid.
8. Cisco Blogs, "Perspective About the Recent WPA Vulnerabilities (KRACK Attacks)," October 2017.
9. Internet of More Things infographic, "Why Security Is Essential for the Growing Internet of Things," July 2017.
10. Modern Materials Handling, "Deloitte and MAPI study: Connected Industrial Control Systems Expose Manufacturers to Cyber Threats," November 2016.

Due to the talent gap created by the convergence of enterprise and industrial networks, more training is needed to protect these new infrastructures successfully.

and end devices are interconnected with those from other vendors. The production network is now open game to the many vulnerabilities from the other networks.

New skills will be needed to secure this new frontier. In response, management cannot simply throw its current IT and OT staff into the mix, nor even its security professionals. Due to the talent gap created by the convergence of enterprise and industrial networks, more training is needed to protect these new infrastructures successfully. Moreover, there is the cultural divide between IT and OT, which must collaborate in order to deliver successful business outcomes.

The second speed bump besides security

The second speed bump on the IIoT highway is bringing IT and OT together. IIoT is shaking up the traditional IT/OT silos. These two were once separate and did not often communicate with each other. Now they must blend and become one. It's a huge and critical step in IIoT transformation and a major cultural shift on both sides.

The rub? Most organizations do not know how to merge IT and OT. And they are not at all certain how bringing these two areas together will add value. How will it lead to new business models? Or new services and revenue sources?

Due to its historic role of information processing, IT is better positioned to take the lead. Data from IIoT-connected sensors or machines are simply more information streams to parse, interpret, and monetize. But IT must collaborate with OT during the transition. After all, many of the sensors, devices, operations, and software that make up IIoT reside on the OT side. And frequently, IT can lack understanding of the OT requirements and operating environment that must be maintained.

For example, a steam valve system that controls water flow through a cooling apparatus has operated, and will continue to operate, within the OT domain. Hands-on intervention used to be required to take its readings and make decisions. With IIoT, the data is collected, analyzed, and acted upon via the interconnected network and IT software that monitors all of the valve system's parameters. In this scenario, data generated from these OT-managed devices and sensors is delivered across the IT system to take critical, real-time action according to specific guidelines.

Proponents must make a good case to OT about IIoT's benefits. Bolstering their argument, returns on IIoT investments are accelerating. Nearly half of manufacturers reported seeing rewards, with 41 percent reaping as much as five percent of 2016 revenues.[11] Manufacturers also expect to see gains from developing and selling IoT capabilities in their own products or services.

11. Modern Materials Handling, "Deloitte and MAPI study: Connected Industrial Control Systems Expose Manufacturers to Cyber Threats," November 2016.

To no one's surprise, many organizations are not sure how to define the skill sets or certifications that they need. As a result, almost one-third (31 percent) of major global corporations reported they face a big IIoT skills gap.

Nearly 42 percent of those polled expect their IoT investments to yield between 10 percent and 20 percent of their annual revenues over the next five years.

Asking OT executives to align with current IT initiatives and break out of existing silos is a tall order. But it can happen, provided both IT and OT professionals get training in the new skills they need to devise, build, and manage IIoT.

IT + OT = New breed of tech pros

Indeed, Accenture predicts that IIoT will benefit workforces of the future by augmenting skills and redefining tasks.[12] According to PwC, IIoT needs skilled IT professionals and technologists to function.[13] It also requires programmers, developers, and network engineers. They are the ones who connect everything and make sure it stays that way. Universal connectivity, after all, is a key characteristic of IIoT.

Need help thinking about all of the skills involved in IIoT? Imagine a highly autonomous assembly line. The production line can automatically reconfigure and optimize itself, and mass-produce customized products in custom-sized batches, with full tracking and connectivity to sales and ordering systems, enterprise resource planning (ERP) systems, work-in-process (WIP) inventory, supply-chain systems, and delivery and order-tracking systems. Machines use robotic vision and AI to execute intricate processes. Throw in collaborative robots, or cobots, which are robots that work alongside human beings.

This technology setup demands not only multiple skill sets but blending skills across silos and specializations. The result is a whole new category of technology professionals. They understand the merging of IT and OT. They recognize that IIoT is really about digitizing business processes far more than it is about digitizing things or even their connections. Engineers, network specialists, application developers, data architects, UI designers, and business people must talk to and understand each other's role for IIoT to work.

To no one's surprise, many organizations are not sure how to define the skill sets or certifications that they need. As a result, almost one-third (31 percent) of major global corporations reported they face a big IIoT skills gap. These organizations also said they need new technical skills (51 percent), better data integration and analytics capabilities (41 percent), and the ability to rethink business models (33 percent).[14]

12. Accenture, "Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth," January 2015.
13. PwC, "Industry 4.0: Building the Digital Enterprise," April 2016.
14. Business Performance Innovation Network and the CMO Council, "The Impact of Connectedness on Competitiveness," April 2017.

Think of protecting the infrastructure in terms of how to build and defend your castle.

Security: The key IIoT skill

IIoT turns older machines into data-generating network endpoints. It links them with new equipment. Then it ties all of the preceding into back-end ERP systems and supply chains. As a result, almost everything within an organization is now open to attacks from bad actors online.

Think of protecting the infrastructure in terms of how to build and defend your castle.

Whereas building the moat around the castle helps to defend against external attacks, internal threats are also an issue. Connected devices need to be hardened as well as be protected by physical security.

This collection of programmable logic controllers (PLCs), distributed control systems (DCSs), and SCADA is functionally partitioned into cell or area zones. Hierarchical in the past, now they can be interconnected by the Industrial Ethernet. Communication among these cell/area zones and levels must be secured and monitored for vulnerability.

As the Industrial Ethernet forms the backbone of this converged network, there are many network infrastructure security features provided by Cisco Industrial Ethernet switches.

Virtual private networking is commonly used to segment various functional cell/area zones. It can also be used as secure remote access to manage IIoT networks. Next-generation firewall (NGFW) and next-generation intrusion-prevention system (NGIPS) features are then applied to secure communications between segmented zones. These network segments are further protected by implementation of advanced access control with Cisco Identity Services Engine (ISE) as well as industrial application inspections.

Implementation of the IEEE 802.1X standard for wireless security is essential for many industrial verticals. Lastly, it is essential for security professionals to understand security standards and regulations for various industries and how to monitor the critical infrastructure for incidents and response.

IT and OT professionals who want to keep IIoT secure must know IIoT standards along with machine protocols. They should know how to harden existing control systems, which, again, were never designed to be connected to enterprise networks but now are.

And, of course, they must possess general cybersecurity skills to perform the following:

- Analyze networks and systems for potential vulnerable areas.
- Spot intrusions, leaks, or data breaches quickly, preferably as they happen.
- Stop incidents and repair any damage to network or system integrity.
- Develop secure software to thwart future cyber events.

To upskill yourself or your team, you need to prepare properly for IIoT security.

- Identify, quantify, and mitigate cybersecurity risks to system availability, integrity, and confidentiality. This may include applying security patches to equipment, as well as utilizing other security controls on equipment that cannot be directly patched against an identified vulnerability.

The upshot? This situation represents a huge career opportunity for you. But you will need hands-on training in the right IIoT security skills and the professional certifications to show that you have developed those skills.

Cisco's IIoT security training and prerequisites

To upskill yourself or your team, you need to prepare properly for IIoT security.

First, you need to understand the IIoT converged network, one that connects anywhere from hundreds to thousands of industrial devices with control systems, gateways, process controllers, human-machine interfaces (HMIs), ERP systems, business services, vendor support and ecosystem suppliers, and partners. Securing IIoT is therefore the first order of business.

OT professionals need to understand the world of IP technology and networking protocols.

The Cisco Industrial Networking Specialist certification is for you if you are an IT or OT professional in manufacturing, process control, or the oil and gas industries, and you are setting up, operating, or supporting networked industrial products and solutions. This certification ensures that you have the basic skills to manage and administer networked industrial control systems. It teaches you the networking technologies needed in today's connected plants and enterprises.

IT and security professionals need to understand ICS and industrial automation protocols and processes.

The CCNA Industrial certification is for plant administrators, control system engineers, and traditional network engineers in manufacturing, process control, and the oil and gas industries. You will be involved in helping securely merge IT and industrial networks. This certification builds the skills needed to securely implement the most common industry-standard protocols and troubleshoot problems while making use of best practices for modern connected networks.

Furthermore, for IT and OT professionals without prior security concepts, you will need to get CCNA Security-level knowledge as well.

As a security professional, you need to identify and understand IIoT security requirements and to implement network security features to build, secure, and defend critical IIoT-enabled infrastructures.

What does Cisco's IIoT security training offer?

As a security professional, you need to identify and understand IIoT security requirements and to implement network security features to build, secure, and defend critical IIoT-enabled infrastructures.

Students undertaking training will explore IIoT network components and protocols, identify security requirements, and apply hands-on discovery of network protocol and traffic analysis.

As part of the training, the IIoT infrastructure will be analyzed and vulnerabilities detected. Rogue devices will then be deployed to exploit and attack network assets. With that understanding, we proceed to analyze such attacks and walk through the process of securing IIoT infrastructure, classifying assets and identifying their relationships with the network.

Cisco is filling the IIoT security training gap with "Securing Industrial IoT Networks with Cisco Technologies" (ISECIN). On the OT side, this IIoT-specific training is for you if you are a plant security professional or a senior industrial network engineer. It is also ideal on the IT security side for security professionals, chief security officers (CSOs), analysts, operations engineers, systems architects, and integrators.

The course will teach you best practices to secure, monitor, and respond to security events, including IoT security requirements, frameworks, and regulations. You will learn to address vulnerabilities and how to defend against attacks. You will also learn how to use Cisco security technologies, such as TrustSec, next-generation firewalls, and next-generation intrusion prevention systems (IPSs) to secure IIoT networks.

You'll learn a lot more about the IIoT framework, along with regulations, industrial protocols like SCADA, and standards. The training will also teach skills about managing IIoT physical security and device hardening, including zone/cell segmentations, vulnerability assessment, and layered security implementation.

In addition, you will become better prepared to defend against and respond to ongoing attacks on critical IoT configurations in sectors like utilities, transportation, and smart cities.

Unlike other industrial networking programs, this course teaches security concepts and best practices via lab-based, hands-on skills and practical knowledge.

Cisco training and certifications are here to help you on every step of your IIoT career journey.

The IIoT challenge: Are you game?

With its potential to make work more engaging and productive, IIoT is great news for OT and IT professionals. The majority of business leaders (87 percent) think that IIoT will result in net job creation.[15] But most of these additional jobs will involve new types of work and very different approaches to manufacturing than exist right now. Remember, IIoT is digitizing business processes along with things and networks.

This means that every aspect of making, distributing, and selling products is undergoing the digital sea change. And being a dodo is a no-go.

Will you be ready? Will you have the right security skill sets? Will you keep your skills updated as technology and processes improve over time? You must become and remain digital-literate, prepared to take advantage of all of the cybersecurity career opportunities that open up as organizational boundaries fade away.

You will need ongoing access to IIoT training and other IIoT-related certifications that will enable you to advance on your own digital journey. And Cisco training and certifications are here to help you on every step of your IIoT career journey.

For more information, visit:

- ISECIN Training
- CCNA Industrial Certification
- Cisco Industrial Networking Specialist Certification
- Cybersecurity Training and Certifications

15. Accenture, "Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth," January 2015.