Securing the Internet of Things

The Internet of Things (IoT) is exploding in size and complexity, connecting a huge universe of consumer, industrial, and digital devices to the network.

The rapid evolution of IoT is exciting, but securing it has become a major challenge for organizations in every sector. And as connected devices proliferate, the attack surface grows larger.

That means that organizations will need teams of professionals with the skills to safeguard and protect their IoT networks and environments. It's an exciting field that's expanding rapidly, and jobs are in high demand.

But how to get started?

This white paper helps answer that question by:

- Explaining what's prompting the expansion of IoT
- Providing an overview of the resulting risk landscape
- Offering best practices on how to protect your organization from such risks
- Sharing how Cisco Security certifications can help optimize your IoT security posture

The big bang: Why this is happening now

There are some five billion connected devices in the world today, according to Gartner. And 50 billion IoT endpoints are expected to populate the planet by the year 2020.

Nearly 30 percent of businesses worldwide have at least limited IoT deployments, by Strategy Analytics' count. And IDC suggests that IoT will be a US$7 trillion industry by 2020.

IoT promises to boost corporate profits worldwide by 21 percent in 2022. That's because IoT can help businesses lower costs by realizing new efficiencies, and boost new revenues by supporting new business models.

"Digitization is changing every part of today's enterprise," notes Tejas Vashi, director of product strategy and marketing for Learning@ Cisco at Cisco Services. "To take advantage of new business opportunities, organizations are moving quickly to designing and deploying new technologies like cloud, mobility, analytics, IoT, and next-generation security."

Indeed. IoT is just part of a larger trend here. And that trend is digital transformation.

Communications and networking technology are helping organizations do things in entirely new ways. And that's both a huge opportunity and a major threat for businesses.

IDC estimates the economic value of digital transformation to be $20 trillion, or more than 20 percent, of the global gross domestic product. Of the more than 1,600 companies IDC studied, the research firm said 67 percent are in the early stages of their transformation as "digital explorers" or "digital players," and fewer than 5 percent of companies are fully transformed.

"The full disruptive impact of digital transformation (DX) has not yet been realized but is well on its way and is going to fundamentally change business markets and how companies attract, delight, and retain customers," IDC notes.

Digital transformation in general, and IoT in particular, can help organizations become more efficient and more responsive to their customers. They also can allow businesses to expand from one-time product sales to models that generate recurring revenue.

Here are a few examples of IoT applications and their benefits:

- Sensors on assembly lines can identify flaws, allowing those problems to be addressed very quickly and sometimes in an automated way.
- Smart garbage cans and vending machines can communicate to cities and businesses that they're full or empty, so workers only have to visit them when needed. That can eliminate truck rolls, resulting in savings in human resources, gasoline, and vehicle maintenance. And it can help reduce carbon emissions and traffic congestion in the process.
- IoT devices of all sorts can collect data for analysis to allow for more informed decision making. And that can make our lives and businesses safer, more comfortable, and more profitable.

Digital transformation and IoT already have given rise to new and successful businesses in a wide variety of areas, including lodging, retail, and transportation. And we've seen existing companies—even very large and well-established ones—reinvent themselves by employing technology to create potentially enormous savings and new ways of doing things.

For example, data collection and analysis can help airlines realize major savings. Estimates suggest that just a 1 percent reduction in jet fuel use could save the airline industry a whopping $30 billion over 15 years. That demonstrates that even seemingly small advances can have very impactful implications.

If you're already on the path to digital transformation, that's great news. You'll probably be much better positioned for both short- and long-term success than your competitors who are slower to adapt to our new digital reality. Companies that don't evolve are likely to go the way of the dinosaur.

Just look at how digital technology has already disrupted the bookseller, camera and film, sporting goods, and taxi services businesses. And that's just the tip of the iceberg.

Some estimates suggest 40 percent of companies that are leaders in their verticals today will be replaced in the next 10 years.

The risk landscape: What you need to look out for

So while failure to undergo a digital transformation is not an option, implementing IoT itself has challenges. That includes figuring out how to secure connected devices and networks, and the data they handle.

This is important because the more connections and connected devices you have, the greater the opportunity for bad actors to steal data, gain unauthorized control of assets, and even potentially threaten safety. Consider how cybercriminals can remotely control and bring down anything from a website to a back-end business system to a connected car to a power grid to implanted medical devices to a country's weapons arsenal.

More than a billion malware detections and incidents, affecting more than 100 million IoT devices, occurred during the June through November 2016 time period alone, according to The CommLaw Group.

IoT devices pose an inside-out risk as well. They can be enlisted to help stage attacks.

In October 2016's Mirai botnet attack, cybercriminals leveraged an army of insecure IoT devices to level a Mirai denial-of-service (DoS) attack on an Internet infrastructure company. Tens of millions of connected devices, including closed circuit TV cameras, DVRs, and routers owned by a range of companies and individuals who were unaware of the attack, were employed. And many high-profile online services and websites were attacked and became unavailable as a result.

The Internet infrastructure company targeted in this case said it commonly sees distributed denial-of-service (DDoS) attacks. But, it added, the use of Internet-enabled devices is now opening the door to a whole new scale of attack.

As Robert Westervelt, security research manager at IDC, recently commented: "As industrial companies pursue industrial IoT (IIoT), it's important to understand the new threats that can impact critical operations. Greater connectivity with operational technology exposes operational teams to the types of attacks that IT teams are used to seeing, but with even higher stakes. The concern for a cyberattack is no longer focused on loss of data, but safety and availability. Consider an energy utility as an example—cyberattacks could disrupt power supply for communities and potentially have impact to life and safety."

One challenge to securing these environments is that many IoT endpoint manufacturers simply have not built security into their products. That's in part because they know that people want inexpensive devices, and adding security to them adds cost. Also, the limited processing power of some endpoints restricts encryption.

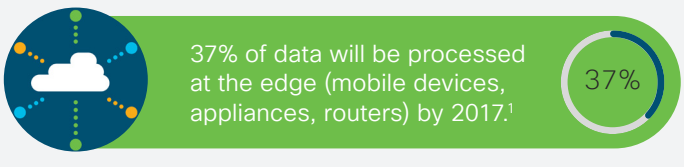
IoT creates new security challenges

To secure connections among people, processes, data, and things, security needs to be as ubiquitous as the Internet of Things. Physical and cybersecurity solutions must work intelligently together and protect the networks, devices, applications, users, and data that make up the IoT.

Increase in connected devices

Increase in amount of data

Move to automation

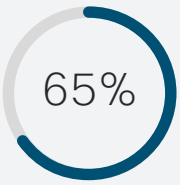


Processing data at the edge

1. Cisco Consulting Services, "Internet of Things" Global Study, 2014.

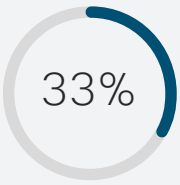
IoT creates more attack vectors

Increased connectivity creates more attack vectors for bad actors to exploit. With such a dynamic threat landscape, security is constantly changing, increasingly complex, and critical to success.

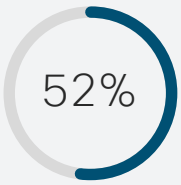


of companies said they couldn't stop the breach because it evaded their existing preventative measures.[2]

of companies couldn't identify where in their network the breach occurred.[2]



of companies took more than two years to discover a breach occurred.[2]



of companies said they lost reputation, brand image, and marketplace value due to a breach.[2]

But it's not just inexpensive consumer goods that lack IoT security. Even industrial controllers that operate in every industrial environment lack basic security controls like authentication and encryption. That means most industrial control system (ICS) attacks don't need to exploit software vulnerabilities. They just need to access the controllers, and then they can change configuration, logic, and state.

"Billions of connected devices are pervasive throughout manufactured products and on the shop floors where they are made," the National Association of Manufacturers (NAM) notes. "This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies."

But, NAM adds, the "more that shop floors become imbued with intelligent machines, the more those machines will contain data worth stealing."

Meanwhile, manufactured goods themselves increasingly have communications capabilities. Things like heating, ventilation, and air conditioning systems can use communications capabilities to interact with both their users and their makers.

This is a positive development for manufacturers. It helps enable them to move from a model based on one-time sales to a recurring-revenue model. But in the process, it expands the manufacturing industry's threat surface.

Also, connected devices frequently have easily exploited vulnerabilities, like default passwords that never get changed, remote access backdoors meant for use by field service technicians (but which can also be an "in" for cybercriminals), and weak authentication. Some device manufacturers take a stab at security by employing trusted boot capabilities, encrypting network traffic, or using Secure Shell (SSH). But if they and the organizations that buy them don't implement these measures in the right way, such efforts can be ineffective.

Another part of IoT security challenge is simply that IoT is new, and rooted in both the information technology and operational technology worlds. Yet IT and OT have traditionally been siloed. And there's no real precedent for how to bring them together.

Additionally, some of the people involved in supporting IoT implementations may not be clear on the goals and requirements of those efforts. And they probably don't understand everything that goes into endpoint data management and analytics, and into IoT security.

2. "2014: A Year of Mega Breaches," Ponemon Institute, 2015.

Best security practices: What you must do

All of the above should be taken into consideration when building, securing, and supporting IoT implementations.

Securing IoT starts before the pieces are even put in place. It begins during the equipment and software selection process. Clearly, it's important to select equipment and software with built-in security when feasible.

Organizations also should be sure to change the default usernames and passwords on their IoT devices. Those that are left unchanged can be easily identified by botnets that scan for known usernames and passwords. And if they hit the jackpot, your devices can come under their control.

Businesses also need to update their IoT devices with the latest operating systems and patches. That will ensure that they're up to date with a variety of features, including the latest security ones.

There's also the issue of application and application programming interface (API) security. The best-prepared businesses will have the right processes and tools in place to monitor and secure app and API access.

Securing the network, of course, is also an important part of the IoT security puzzle. Connectivity is the linchpin of IoT services, and it's important to protect against such attacks as man-in-the middle hacks and session hijacking, which can intercept communications between the device and the cloud application.

There's no one-size-fits-all approach to IoT network security, of course, but the solution should certainly involve data encryption, network authentication, and secure private networks.

Device data should always be encrypted when it's being transported to guard against attacks. While IoT devices don't support such application-level encryption, the cellular industry addresses it by using Global System for Mobile Communications (GSM) standardized encryption between mobile networks and devices.

In this case, the network initiates an encrypted communication with a ciphering mode request, and the device uses ciphering keys and encryption algorithms on the SIM card to securely transmit and receive data. Because the keys are never exposed outside the SIM card and the true identity of the end device is never revealed, this solution is highly secure.

Network authentication, meanwhile, helps ensure that devices communicate only with the applications they should. That involves verifying and authorizing devices on both the network and applications within the network.

And safeguarded private networks isolate and shield IoT device data from other parts of the Internet. This also protects the enterprise from exposure if device data is attacked.

Businesses may be familiar with this idea from their use of virtual private networks, but VPNs aren't an affordable option for low-cost IoT devices. A better choice is using cellular customer access point names to extend a highly secure local area network from the enterprise data center across the mobile network to remote IoT devices. Businesses can then allocate private IP addresses and specify additional levels of authentication and authorization.

Security is top of mind in any IoT project discussion and planning. For end-to-end protection and visibility, security should be built into any IoT strategy and solution from the ground up, instead of bolted onto the converged network later as an afterthought. As part of its commitment to this approach, Cisco announced its IoT Threat Defense cybersecurity architecture at the 2017 IoT World Forum. This framework is an umbrella program that focuses on the security segmentation of OT and IT networks, visibility, remote access, and services.

IoT has implications for both the IT and OT parts of an organization. That's why staff members from both the IT and OT teams should work together in deciding what IoT security posture is right for their organizations. IT and OT engineers should then collaborate in setting up security policies and procedures to implement IoT security for their applications, devices, and networks.

The human factor: Who you'll need to do it

But the collaboration of IT and OT team members with existing skillsets will only get us so far. That's because creating, securing, and supporting IoT implementations requires new talent.

Both IT and OT need digital expertise. So, training staff members to address IoT is essential for organizations as they stage their digital transformations.

The converged architecture involved in IP-connected factories, for example, introduces a talent gap not met by current IT or OT professionals. As a result, individuals from each discipline need to learn the technology from the other. They also need to add soft skills in such areas as communication, collaboration, project management, and more.

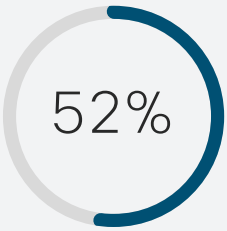
IT engineers should become acquainted with industrial networking and application protocols. Gaining knowledge about wireless deployment is also essential for such industrial verticals as mining, transportation, and utilities. Understanding the options around IoT security and being able to implement the most relevant ones for a particular organization are also vitally important.

Meanwhile, OT engineers need to adjust from the hierarchical Purdue model with which they're so familiar for enterprise control to a flattened IP connected world. That's essential to understand IP networking protocols and their implications, as well as the importance of sharing data across the ecosystem.

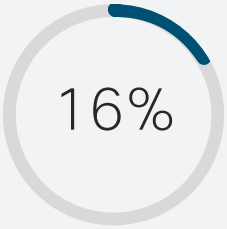
Adapting to this new way of doing things will be beneficial not only to businesses, but to IT and OT team members as well. Such individuals who fail to embrace their new reality and gain the necessary new skillsets could find their jobs replaced by automated systems. Those who move to address this new challenge, however, will create new opportunities for both their organizations, and their own personal and professional growth.

"The logical conclusion to the relentless march of automation is that it will transform the role of people at work," according to the 20th annual PwC Global CEO Survey. "Different skills will be needed, some roles will disappear, and others will evolve. Some organizations will need fewer people, but others will need more—we will see a rebalancing of human capital as organizations adjust."

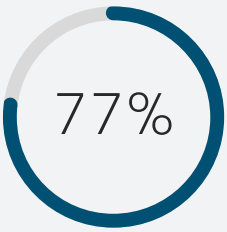
PwC goes on to report the following:



of the CEOs it surveyed plan to increase headcount in the next 12 months, up from 48 percent in 2016.



of leaders plan to eliminate jobs over the coming year.



of CEOs consider the availability of critical skills as the biggest business threat.

Meanwhile, Progress Software Corporation's State of IoT 2015 Global Developer Study found that 51 percent of developers and chief information officers surveyed said they are uncertain they have the skills or resources to deliver on the promise of IoT.

And Gartner reports that OT executives in particular today are facing a major talent gap. It says insufficient staffing and the lack of expertise are the top-cited barriers for organizations currently looking to implement IoT. In addition, it points out, there's a lack of process and no talent frameworks for IoT job roles and related training and credentials.

Of course, IT and OT engineers with updated skillsets aren't the only ones needed to help ensure successful IoT efforts. Organizations also require IoT business leaders, business and solutions analysts, data engineers, and solutions architects. And they require project leaders and cross-functional team leaders in quality assurance, software development, support, and more.

That said, organizations should first hire or identify a digital champion. This individual should be able to communicate the company's IoT vision. And he or she should have the personality to motivate employees to make the major changes in systems and processes that IoT implementations will require.

That individual and the rest of the team should then set out to add and build the needed talent to get the job done.

"The rise of IoT is the digital catalyst," notes Vashi of Learning@Cisco. "It opens up new worlds of possibilities because organizations can now extract data from network-connected devices and sensors. This data was never available before. Insights from this data might add enormous value to organizations. But they must reshape their current infrastructures in order to use the data effectively. And they must hire and train the right people to bring their digital change strategies to fruition."

> Businesses and other organizations will also need people to stay abreast of evolving and upcoming regulations around data privacy, IoT security, and other relevant compliance issues. That will require involvement from team members on both the leadership, legal, and technical teams. And that will entail new skillsets as well.

Skills for securing IoT

So what are these skillsets, and who will be the individuals who obtain them? Many of these jobs will be roles that have never existed before. However, the majority of these roles will be filled by seasoned professionals acquiring new skillsets relevant to address IoT.

However, as noted above, many organizations are struggling to understand what skills are and will be required to allow for successful IoT implementations. The good news is that Cisco offers a reference framework for those skillsets, and the training and certification programs to arm individuals and existing team members with the tools they need to address digital transformation and IoT implementations.

Here are some statistics from recent reports that demonstrate the challenges—and opportunities—that exist on the talent front:

The Internet of Things is creating jobs at such a rate that the IT industry is projected to grow by

before 2020. And many of these jobs have new requirements.

There were one million job openings last year for cybersecurity experts. And the shortfall of cybersecurity experts is expected to reach

1.5 million globally by 2019.

220,000 There's a need to train 220,000 new control engineers every year for manufacturing plant operations alone.

There are just 500,000 developers worldwide working on IoT. So we'll need a whole lot more developers as connected devices and applications proliferate in the years ahead. Some estimate the demand on that front will reach

4.5 million within five years.

Cisco IoT Security Services Framework

To secure the Internet of Things it is essential to use a holistic approach, working through the entire value chain of your network. Every layer must be secure—technology, process, and people.

Technology

Application Security

Secure Interface Design
Custom Code Security
Secure Development Lifecycle
Secure Communication
Threat Training and Awareness

Endpoint and Sensor Security

Device Provisioning and Management
DRM
Malicious Code Protection
Anti-tamper
Network and Device OS Segmentation

Infrastructure and Cloud Security

Secure Cloud Build and Virtualization
Encryption and Cryptography
Network Design and Communication
Access Control

Process

Operational Security

Policy and Procedures
Secure Device Distribution
Physical Security
Vulnerability Management
Data Classification
Privacy and Data Lifecycle Management
Upgrade and Maintenance Capabilities
Compliance and Assurance
Third-Party Risk Management

People

Security Strategy

Standards and Interoperability
Security Architecture
IT Governance and Risk Management

The Cisco CCNA Industrial certification and Cisco Industrial Networking Specialist certification programs provide candidates with an understanding of the convergence of IT and OT that's fundamental to survival in the digital revolution.

These certifications are for plant administrators, control system engineers, and traditional network engineers in the manufacturing, process control, and oil and gas industries. These are individuals who will be involved with the convergence of IT and industrial networks.

Participants in these programs receive the necessary skills to successfully implement and troubleshoot the most common industry standard protocols while taking advantage of best practices needed for today's connected networks. This curriculum combines theoretic knowledge with practical lab exercises. It provides the real-world skills that allow IT and OT professionals to make sure that their current infrastructures are optimized while developing a converged platform for flexibility to support future business outcomes.

Securing the Internet of Things

"IoT is exploding in popularity across all industries," notes Daniel Chan, product manager for Cisco Services. "Organizations are scrambling to identify, hire, and train top talent to help them design, deploy, manage, and secure IoT networks. But IoT engineers are not one-size-fits-all. The key to taking advantage of this boom in interest is to identify what IoT skills your target market is looking for, and then taking steps to strengthen your training and skillset to match the demands of your ideal position."

Cisco Cybersecurity certifications

Cisco also offers Cybersecurity training and certification. This program addresses cybersecurity skills needed in such team roles as:

- Chief Security Officers (CSOs)
- Managers
- Secure infrastructure architects and engineers
- Secure infrastructure engineers, technicians, and administrators
- Security operations team members

The Cisco CCNA Security certification lays the foundation for such job roles as network security technician, administrator, or support engineer.

The next level up, the CCNP Security certification, offers employers proof of job-ready training and skills from experienced, professional-level network security engineers. The CCIE Security certification recognizes individuals who have the knowledge and skills to implement and support extensive Cisco network security solutions, using the latest industry best practices and technologies.

The most recent Cisco Cybersecurity certification is CCNA Cyber Ops, which focuses on the role of the security analyst working in a Security Operations Center. It introduces IT personnel to valuable skills, allowing them to monitor IT security systems, detect cyberattacks, gather and analyze evidence, correlate information, and coordinate responses to cyber incidents.

The role of the Security Operations Center Analyst is to determine through various types of event monitoring whether an intrusion or security-related event has occurred or is currently occurring. The telemetry data analyzed by these individuals is commonly obtained through various "feeds" presented chronologically to the analyst as they occur.

"The industry shift we are facing today is really the transition toward what is called digital business. You do everything digitally. You purchase stuff digitally. You order your services digitally," says Antonella Corno, senior manager with Learning@Cisco. "That's the digitization of business, and we are here at Cisco to support the technologies that are needed and, through Learning@Cisco, to train people on the skills that are needed to achieve those goals."

Take advantage of Cybersecurity certification opportunities. Visit us online:

- Cisco Cybersecurity training and certifications
- Cisco CCNA Industrial certification
- Cisco Industrial Networking Specialist certification
- Is the CCNA Industrial certification right for me?
- Cisco certification community