TechTarget | IoT Agenda

E-guide

PRO+ Content

Prevent Enterprise IoT Security Challenges

Your expert guide to preparing your security program for IoT

In this e-guide

In this e-guide:

The Internet of Things is imminent -- and so are the IoT security challenges it will inevitably bring. This guide to IoT security gathers together essential reading to get you up to speed on the emerging information security threats and the best means for thwarting them.

Among the issues this guide covers are IoT security basics and ways to devise an IoT security strategy. It also reviews the particular security challenges that the IoT era brings with it, reviewing such topics as how to maintain the privacy of personal information, like health data, and how the latest wearable IT devices may affect security.

Read this guide to prepare your enterprise for IoT security challenges.

In this e-guide

Section 1: IoT Basics

Just as other phenomena before it, the Internet of Things will surely bring its own set of flaws, threats and related security challenges. However, knowing what you're up against before running into problems will lessen the devastation of any negative effects.

Continue reading

In this e-guide

Internet of Things (IOT): Seven enterprise risks to consider

Ajay Kumar, Contributor – IoT Agenda

The day when virtually every electronic device -- from phones and cars to refrigerators and light switches -- will be connected to the Internet is not far away. The number of Internet-connected devices is growing rapidly and is expected to reach 50 billion by 2020.

However innovative and promising it seems, this so-called Internet of Things (IoT) phenomenon significantly increases the number of security risks businesses and consumers will inevitably face. Any device connecting to the Internet with an operating system comes with the possibility of being compromised, in turn becoming a backdoor for attackers into the enterprise.

In this article, we will discuss the proliferation of the Internet of Things and explore what enterprises can do to manage the security risks associated with IoT devices.

What is the IoT? Why is it growing in popularity?

The IoT sensation is rapidly embracing entire societies and holds the potential to empower and advance nearly each and every individual and business. This creates tremendous opportunities for enterprises to develop

In this e-guide

new services and products that will offer increased convenience and satisfaction to their consumers.

On the user side, Google Inc. recently announced that it is partnering with major automakers Audi, General Motors and Honda to put Android-connected cars on the roads. Google is currently developing a new Android platform that will connect cars to the Internet. Soon, car owners will be able to lock or unlock their vehicles, start the engine or even monitor vehicle performance from a computer or smartphone.

The promises of IoT go far beyond those for individual users. Enterprise mobility management is a rapidly evolving example of the impact of IoT devices. Imagine if suddenly every package delivered to your organization came with a built-in RFID chip that could connect to your network and identify itself to a connected logistics system. Or picture a medical environment in which every instrument in the exam room connected to the network to transmit patient data collected via sensors. Even in industries like farming, imagine if every animal were digitally tracked to monitor its location, health and behavior. The IoT possibilities are limitless, and so are the number of devices that could manifest.

However, despite the opportunities of IoT, there are many risks that must be contended with. Any device that can connect to Internet has an embedded operating system deployed in its firmware. Because embedded operating systems are often not designed with security as a primary consideration, there are vulnerabilities present in virtually all of them -- just look at the amount of malware that is targeting Android-based devices today. Similar threats will likely proliferate among IoT devices as they catch on.

In this e-guide

Enterprises and users alike must be prepared for the numerous issues of IoT. Listed below are seven of the many risks that will be inherent in an Internet of Things world, as well as suggestions to help organizations prepare for the challenge.

1. Disruption and denial-of-service attacks

Ensuring continuous availability of IoT-based devices will be important to avoid potential operational failures and interruptions to enterprise services. Even the seemingly simple process of adding new endpoints into the network -- particularly automated devices that work under the principle of machine-to-machine communications like those that help run power stations or build environmental controls -- will require the business to focus its attention on physical attacks on the devices in remote locations. This will require the business to strengthen physical security to prevent unauthorized access to devices outside of the security perimeter.

Disruptive cyberattacks, such as distributed denial-of-service attacks, could have new detrimental consequences for an enterprise. If thousands of IoT devices try to access a corporate website or data feed that isn't available, an enterprise's once-happy customers will become frustrated, resulting in revenue loss, customer dissatisfaction and potentially poor reception in the market.

Many of the challenges inherent to IoT are similar to those found in a bring your own device environment. Capabilities for managing lost or stolen devices -- either remote wiping or at least disabling their connectivity -- will

In this e-guide

be critical for dealing with compromised IoT devices. Having this enterprise strategy in place will help mitigate the risks of corporate data ending up in the wrong hands. Other policies that help manage BYOD could also be beneficial.

2. Understanding the complexity of vulnerabilities

Last year, an unknown attacker used a known vulnerability in a popular Web-connected baby monitor to spy on a two-year-old. This eye-opening incident goes to show what a high risk the IoT poses to enterprises and consumers alike. In a more dramatic example, imagine using an IoT device like a simple thermostat to manipulate temperature readings at a nuclear power plant. If attackers compromise the device, the consequences could be devastating. Understanding where vulnerabilities fall on the complexity meter -- and how serious of a threat they pose -- is going to become a huge dilemma. To mitigate the risk, any project involving IoT devices must be designed with security in mind, and incorporate security controls, leveraging a pre-built role-based security model. Because these devices will have hardware, platforms and software that enterprises may never have seen before, the types of vulnerabilities may be unlike anything organizations have dealt with previously. It's critical not to underestimate the elevated risk many IoT devices may pose.

In this e-guide

3. IoT vulnerability management

Another big challenge for enterprises in an IoT environment will be figuring out how to quickly patch IoT device vulnerabilities -- and how to prioritize vulnerability patching.

Because most IoT devices require a firmware update in order to patch vulnerabilities, the task can be complex to accomplish on the fly. For example, if a printer requires firmware upgrading, IT departments are unlikely to be able to apply a patch as quickly as they would in a server or desktop system; upgrading custom firmware often requires extra time and effort.

Also challenging for enterprises will be dealing with the default credentials provided when IoT devices are first used. Oftentimes, devices such as wireless access points or printers come with known administrator IDs and passwords. On top of this, devices may provide a built-in Web server to which admins can remotely connect, log in and manage the device. This is a huge vulnerability that can put IoT devices into attackers' hands. This requires enterprises to develop a stringent commissioning process. It also requires them to create a development environment where the initial configuration settings of the devices can be tested, scanned to identify any kind of vulnerabilities they present, validated and issues closed before the device is moved into the production environment. This further requires a compliance team to certify that the device is ready for production, test the security control on a periodic basis and make sure that any changes to the

device are closely monitored and controlled and that any operational vulnerabilities found are addressed promptly.

4. Identifying, implementing security controls

In the IT world, redundancy is critical; should one product fail, another is there to take over. The concept of layered security works similarly, but it remains to be seen how well enterprises can layer security and redundancy to manage IoT risk. For example, in the health care industry, medical devices are available that not only monitor patients' health statuses, but also dispense medicine based on analysis performed by such devices. It's easy to imagine how tragic consequences could result were these devices to become compromised.

The challenges for enterprises lie in identifying where security controls are needed for this emerging breed of Internet-connected devices, and then implementing effective controls. Given the diversity that will exist among these devices, organizations will need to conduct customized risk assessments, often relying on third-party expertise, to identify what the risks are and how best to contain them. While an interesting recent example was the case of former Vice President Dick Cheney disabling the remote connectivity of a defibrillator implanted in his chest, unfortunately most enterprises won't have the luxury of taking these devices offline. In any event, organizations which embrace IoT must define their own information security controls to ensure the acceptable and adequate protection of the IoT evolution. As the trend matures, best practices will certainly emerge from industry professionals.

In this e-guide

5. Fulfilling the need for security analytics capabilities

The variety of new Wi-Fi-enabled devices connecting to the Internet will create a flood of data for enterprises to collect, aggregate, process and analyze. While certainly organizations will identify new business opportunities based on this data, new risks emerge as well.

Organizations must also be able to identify legitimate and malicious traffic patterns on IoT devices. For example, if an employee tries to download a seemingly legitimate app onto his or her smartphone that contains malware, it is critical to have actionable threat intelligence measures in place to identify the threat. The best analytical tools and algorithms will not only detect malicious activity, but also improve customer support efforts and improve the services being offered to the customers.

To prepare for these challenges, enterprises must build the right set of tools and processes required to provide adequate security analytics capabilities.

6. Modular hardware and software components

Security should be considered and implemented in every aspect of IoT to better control the parts and modules of Internet-connected devices. Unfortunately it should be expected that attackers will seek to compromise the supply chain of IoT devices, implanting malicious code and other

In this e-guide

vulnerabilities to exploit only after the devices have been implemented in an enterprise environment. It may prove necessary to adopt a security paradigm like the Forrester Zero Trust model for IoT devices.

Where possible, enterprises should proactively set the stage by isolating these devices to their own network segment or vLAN. Additionally, technologies such as microkernels or hypervisors can be used with embedded systems to isolate the systems in the event of a security breach.

7. Rapid demand in bandwidth requirement

A study conducted by Palo Alto Networks Inc. revealed that between November 2011 and May 2012, network traffic jumped 700% on networks the vendor observed, largely due to streaming media, peer-to-peer applications and social networking. As more devices connect to the Internet, this number will continue to grow.

However, the increased demand for Internet will potentially proliferate business continuity risks. If critical applications do not receive their required bandwidth, consumers will have bad experiences, employee productivity will suffer and enterprise profitability could fall.

To ensure high availability of their services, enterprises must consider adding bandwidth and boosting traffic management and monitoring. This will not only mitigate business continuity risks, but also prevent potential losses. In addition, from the project planning standpoint, organizations would need

to do capacity planning and watch the growth rate of the network so that the increased demand for the required bandwidth can be met.

Conclusion

The Internet of Things has great potential for the consumer as well as for enterprises, but not without risk. Information security organizations must begin preparations to transition from securing PCs, servers, mobile devices and traditional IT infrastructure, to managing a much broader set of interconnected items incorporating wearable devices, sensors and technology we can't even foresee currently. Enterprise security teams should take the initiative now to research security best practices to secure these emerging devices, and be prepared to update risk matrices and security policies as these devices make their way onto enterprise networks to enable machine-to-machine communication, huge data collection and numerous other uses. This increased complexity within the enterprise shouldn't be overlooked, and threat modeling will be necessary to ensure basic security principal of confidentiality, integrity and availability are maintained in what will be an increasingly interconnected digital world.

Next article

In this e-guide

Internet of Things security concerns prompt boost in IoT services

Sharon Shea, Site Editor – IoT Agenda

As reports amplifying the threats created by Internet of Things devices continue to make headlines, one company is ramping up its security portfolio in preparation for the IoT onslaught.

Symantec pushes more IoT services

Symantec Corp. announced Tuesday it is expanding its security catalog to help enterprises handle the growing number of Internet-connected devices that will inevitably infiltrate the enterprise, likely sooner rather than later. Gartner, Inc. has predicted 4.9 billion "Things" will be used this year, a number the analyst believes will reach 25 billion by 2020.

While Symantec's broader Unified Security Strategy already includes measures for authentication, device security, analytics and management to help prevent devices from being "hacked, tracked and hijacked," Symantec is specifically growing its IoT services portfolio. Symantec claimed it is already securing more than one billion IoT devices, and the addition of three new security measures -- and strong partnerships -- will help it secure even more smart cars, meters, critical infrastructure and a plethora of consumer devices that make up the majority of the IoT device pie.

In this e-guide

ATM manufacturer Wincor Nixdorf was named an early adopter of Symantec Embedded Critical System Protection, which aims to protect IoT devices from zero-day and other attacks by locking down software embedded in the device.

Symantec is also working on creating "Roots of Trust" by combining Symantec's Certificate Authority with its partners' embeddable engines, including Texas Instruments Inc. and wolfSSL Inc., to safely authenticate and encrypt data.

To ensure code operating on IoT devices is authorized, Symantec announced it will provide code signing certificates and a cloud-based signing service that specifically works with IoT code formats.

Symantec also announced it would be working on additional IoT security technology, including a centrally managed IoT portal, and analytics to help detect anomalies and attacks on IoT networks.

Internet of Things security concerns increase

Symantec's announcement comes a week after the release of a report highlighting the potential risks of Internet of Things devices.

Sponsored by NexusGuard Ltd. and conducted by Cybersecurity Ventures, the report exposing Internet of Things security concerns noted that by the end of 2017, more than 20% of businesses will adopt IoT services to secure Internet-connected devices and networks, which will in turn advance the

In this e-guide

multi-trillion dollar IoT marketplace and boost security research and spending through 2025.

The report also discussed how Internet of Things devices can be used as "jumping off" points for distributed denial-of-service attacks.

"These vulnerable devices can be exploited during software updates and used as launch proxy servers that can be targeted at businesses which are then extorted for monetary payment," the report reads. "DDoS is often the 'first wave' of attacks by hackers who use them to distract companies from other more targeted intrusions."

Researchers also found attacks exploiting the Simple Service Discovery Protocol (SSDP) were growing in prevalence, mirroring the separate findings of NSFOCUS and Akamai Technologies, Inc. earlier this year.

SSDP attacks are especially dangerous, the report said, because they "utilize vulnerable routers to amplify an attack beyond normal bandwidth limits while also hiding the original source of the attack."

Nexusguard researchers reported seeing 64 Internet-based scans for SSDP services over the past week, as well as tracking 559 exploited "edge devices" -- devices that act as an entry point to a network.

"IoT brings new layers of interconnectedness and efficiency, but the risks cannot be ignored," Steve Morgan, CEO at Cybersecurity Ventures, said. "We created this report to highlight the risks that come with IoT devices, as more and more of these objects are connected to the Internet and built with exploitable lightweight security."

In this e-guide

The report also touched on other Internet of Things security concerns, including a lack of security, waning manufacturer support and ending patching cycles.

"By its very design, the Internet of Things is built with lightweight security," Terrence Gareau, chief scientist at Nexusguard, said. "These devices rely heavily on shared libraries and rapid development cycle. Because of their constraints, many IoT devices have limited options for firmware upgrades and other risk management features. The fact that they are also "always-online" makes them highly susceptible to intrusion and attacks."

Next article

In this e-guide

Section 2: Embedded System Risks

IoT devices and embedded systems are at the core of IoT's popularity, but unfortunately security isn't. Learn about the risks of IoT and how to keep these IoT security challenges from undermining your enterprise.

Continue reading

In this e-guide

Pervasive sensing: How it affects enterprise and IoT security

Ernie Hayden, Executive Consultant – Securicon, LLC

Imagine walking into a movie theater. Have you ever wondered how many sensors are in that space? Well, everyone with a smartphone essentially has a sensor in their possession. What about those with Fitbits and other sports monitors? Those are sensors, too. What about the sensors used for heating/ventilation and air conditioning controls for the movie theater? What about fire protection sensors?

We are progressively engulfed with sensor technology, and it is something a security professional may want to pay attention to.

What is pervasive sensing technology?

So, what is "pervasive sensing?" It is not a common term-of-art in security. However, it is beginning to gain traction -- especially in the industrial controls area. David Nagel of George Washington University wrote the first technical paper on the subject. In his seminal work in 2000 Nagel observed: "Pervasive sensing is taken here to mean the widespread, and possibly dense, deployment, and the continuous, either latent or real-time, employment of diverse sensors, networked to systems or people, for the gathering of information of practical use or mere interest..."

In this e-guide

Nagel added that the "pervasive" use of sensors comes from the "rapidly increasing connectivity" of devices and the prevalence of sensors that offer low costs, low power requirements, and a small physical footprint.

In 2006 the RAND Corporation highlighted pervasive sensing in a report on the technologies expected by 2020. Its definition was more along the lines of an Orwellian *1984* perspective, stating that "Pervasive sensing is the presence of sensors in most public areas and the ability to network sensor data to accomplish real-time surveillance."

A more prevalent contemporary commentary on the subject of pervasive sensing comes from Emerson Process Management, a division of Emerson Electric Company that specializes in automation technology. Emerson's definition of pervasive sensing, according to this company blog post, is:

"Pervasive sensing is simply the use of sensors to capture data on anything in a plant that could affect its operation. It is driven to a large extent by the increasing availability of inexpensive sensors -- many of them wireless. Pervasive sensing comes down to use of multiple sensors everywhere, often (but not always) wireless."

The Emerson definition of pervasive sensing represents today's practice of adding sensors and rather than connecting them via wire and cables, using wireless sensor networks to take advantage of lower costs, ease of installation and added data about processes, systems and in some cases, even people.

In this e-guide

This may seem like new science, but it is really another term for the Internet of Things (IoT), or the Industrial Internet of Things (IIoT) when applying this approach in an industrial environment like a factory relying on automation.

Why does pervasive sensing matter to security?

IoT security concerns have been highlighted by security researcher Bruce Schneier and even the U.S. Federal Trade Commission. But there seems to be more interest in the convenience of IoT and pervasive sensing rather than skepticism towards these new "lick and stick" sensor applications that literally can expand sensor arrays on thousands of devices.

In one of its marketing articles, Emerson Process Management reported that an Eastern European oil processing plant is deploying a fully wireless infrastructure to allow the addition of 12,000 pervasive sensing instruments -- up from 7,000 -- in order to improve energy efficiency, more closely monitor equipment and pipe corrosion, and reduce unplanned environmental releases. Consider how much larger the attack surface has become for this plant. The risk posture has increased substantially, but what security controls are being included or implemented to protect the systems, processes and data?

In this e-guide

IoT security risks and pervasive sensing

Every sensor added to a plant process can be either a benign data point strictly used for indication, or it can be connected to a control system and ultimately operate an actuator like a valve positioner or a circuit breaker. It really depends on how it is attached to the plant systems and how configuration management is assured with all these devices. And, with new sensors being procured with corporate credit cards rather than a more disciplined purchase-order process, this can lead to some interesting unintended consequences.

So what are the risk implications with all these sensor arrays? The next part of this series will examine the primary implications of pervasive sensing that security professionals should keep in mind before deploying sensors throughout their enterprises.

Next article

In this e-guide

Embedded systems security a growing concern amid rise of IoT

Michael Heller, Senior Reporter – SearchSecurity

Some fear the rapid increase in nontraditional Internet-enabled devices could mean more potential enterprise entry points for attackers. Many of these devices fall into the category of embedded systems, and experts in that field fear a worst-case security scenario for organizations because of embedded technology's troubling security history.

Traditionally, an embedded system device is a type of appliance with a minimal chipset and a "lite" version of an operating system, often Linux. The most popular examples for enterprise would be USB sticks, which were used to initially load the infamous Stuxnet malware, networked printers, and even now hard drive firmware, which is where the recently revealed Equation spyware lived.

However, the devices in that category are expanding rapidly with the arrival of the Internet of Things (IoT), which bestows networking capability to a broad spectrum of devices that have never had that capability before, such as office appliances like thermostats and refrigerators. As a result, enterprises may soon find they have a whole host of new attack points on their networks, but experts aren't sure that the new generation of embedded devices has overcome the security flaws of their predecessors.

In this e-guide

According to Benjamin Jun, CTO of San Francisco-based security consultancy firm Chosen Plaintext Partners, embedded systems have historically used a lot of proprietary components and not shared much common circuitry with other systems, meaning when bugs were found, they were less likely to be fixed due to cost or resource restraints.

Modern embedded systems have moved away from this paradigm by sharing some of the same internal systems components, such as ARM chips, with other popular mobile devices, Jun said, but embedded devices must often be supported for years or even decades, which causes a new set of problems.

"Mobile phones iterate quickly, but embedded systems tend to live much longer," Jun said. "The process of rapid obsolescence in mobile doesn't translate to devices that are expected to last 10 to 20 years. The teams that debug these things move on, so the security process is limited."

Beyond the level of support that embedded systems need, Jun said that even when there are software updates available, enterprises may overlook these devices because the cost per node is much lower in terms of support and upgrading.

"Laptop costs are pretty high, but those costs can be justified, because you have the idea that productivity will rise with more laptops. But, what about printers, or smart thermostats?" Jun said. "How much are you going to spend to secure something where the incremental value is assumed to be low?"

In this e-guide

According to Jun, one of the more overlooked embedded threats are VoIP conference phones and other devices with microphones, where the mic can be turned on to record sensitive information without notice.

But that's just the beginning, Jun added. The prevalence of the IoT will mean that enterprises will face security concerns related to a much wider variety of devices. This means that in addition to devices like USB sticks and printers, wearables and other cutting-edge devices may find their way onto corporate networks, often without built-in security controls.

Similarly, it also means new risks from devices like smart thermostats or refrigerators, where the responsibility for support can be blurry, according to Jun, because they may be owned by a building manager and not under the purview of the corporate IT department.

Secure design

Experts noted that only time will tell if new embedded devices will be better supported over the long term than past embedded systems have been, but the key to secure embedded devices is in securely designing them from the beginning.

"You have to design the hardware and firmware from the ground up to prevent access from malware or physical tampering," said Ken Jones, vice president of engineering and product management at IronKey, a division of Oakdale, Minn.-based Imation Inc. "It's extremely common that firmware can be updated in the field to fix bugs and security vulnerabilities, but once you

In this e-guide

have that process and don't think it through fully, you've opened a Pandora's box of problems."

According to Jones, secure design includes protection against physical tampering of the device, encryption and firmware digital signatures.

Many older embedded systems require updates be performed in the field, said Jones, so enterprises should prefer systems that use digitally signed firmware that is not only checked prior to installation, but also before it runs for the first time. This can be difficult though, Jones noted, so organizations may need to crack down on embedded device policy.

"From an enterprise perspective, it is all about what you allow to connect to your network, using endpoint protection that can block everything except whitelisted products," Jones said. "It behooves companies to be very restrictive about what can be connected. I think we'll see a lockdown on what will be allowed on the network."

Alexander Damisch, senior director of IoT Solutions at Alameda, Calif.-based Wind River Systems Inc., agreed with this assessment. Damisch recommended that enterprises securely design their infrastructure, which would include requiring devices be authenticated before sending or receiving data on the corporate network; because it can be difficult to detect malware in embedded firmware, monitoring traffic is key.

"This would mean that IT takes over personal devices to an extent, which people don't like," said Damisch, "but the other option is that they simply don't get access. The key is that it isn't personal blocking, the system is

designed that way," which Damisch said could help employees accept the practice easier.

Damisch also advocated isolating vulnerable embedded systems behind gateways or on a virtual system, which he said is often a more cost-effective option, and allows for updating gateway rules to stop new threats where embedded systems may falter, because they aren't designed to be updated that often.

"Redesigning is difficult, so you find the weak point and either put it on the virtual system, or put gateways in front so all traffic is monitored and encrypted," Damisch said. "Security is something that starts with the development process."

Next article

In this e-guide

Seven ways to manage and secure business wearables

Lisa Phifer, Owner – Core Competence Inc.

Wearable devices could be coming to an organization near you, so it's time for IT administrators to assess the management and security capabilities around wearables in their business. Companies with sales workforces or field workers, or in verticals such as healthcare and manufacturing, may soon find uses for wearables that can provide employees with a hands-free, portable app experience.

Given the unique properties of wearables, it will take time for vendors in the enterprise mobility management (EMM), WLAN, and wireless intrusion prevention system markets to fully integrate these new kinds of devices into mobile policies and device settings and alerts.

However, there are many opportunities for IT to use existing platforms to manage and secure wearable devices. IT departments should get a head start on developing a wear your own device (WYOD) strategy, and the following seven suggestions are a good way to begin.

1. Companies can adjust their EMM policy to combine restrictions with geofencing. IT can disable Bluetooth between wearable devices and IT-managed smartphones or tablets, either altogether or in high-risk areas.

In this e-guide

2. Use EMM application blacklists to disable wearable-specific apps on managed smartphones. Better yet, IT-managed containers and tools such as Apple's Managed Open In feature can control the flow of data between enterprise apps. IT has several resources available to prevent users from sharing business data in personal apps specific to their wearables.
3. When wearables lack enterprise-grade authentication, IT can use WLAN access control lists and intrusion prevention systems to block or allow enterprise network access to business wearables.
4. If your organization allows WYOD, consider using authentication such as biometrics, proximity and geofencing. These approaches are useful for enabling the device itself and for using wearables as an authentication token to unlock or start other business resources.
5. Analyze network traffic to detect and measure the workload that wearable-generated data streams create. However, employers may want to avoid logging wearable device traffic too extensively, given that if often includes personally identifiable information.
6. Use wireless intrusion prevention systems (WIPS) to detect and report on irregular connections and potential attacks that could exploit business wearables. As with any new consumer electronics, wearables are likely to harbor at least a few vulnerabilities, and it's important to identify and address any low-hanging fruit.
7. IT can already manage a few wearable devices as if they were smartphones -- most notably, Android-based smart watches. For the others, IT can use regular EMM to assess and enroll devices, provision security policies, applications and data containers, and apply actions such as find and wipe when business wearables are lost or stolen. Craft custom policies for these devices to balance risk and

usability, and work with early adopters to refine those policies for future use.

As more wearables enter the workplace, EMM, WLAN and WIPS providers will adjust their services to allow better wearable device management. However, IT can't ignore security concerns in the meantime, as there are already several useful options out there to manage wearable access.

In this e-guide

Next article

In this e-guide

Section 3: Security Strategy

The key to IoT security is preparation. In this section, explore who's responsible for securing IoT and get help devising an IoT plan that will keep your company safe and sound.

Continue reading

In this e-guide

What's the key to IoT device discovery in the enterprise?

Michael Cobb, Renowned security author

My organization is worried about the Internet of Things (IoT) particularly because of the lack of federated control around all of these connected devices and systems. Are there ways to control IoT device discovery and prevent the many issues associated with non-upgraded IoT devices?

Cisco predicts that around 50 billion devices will be connected to the Internet by 2020. There may be many benefits of having virtually every device -- from cars to household appliances, and even clothes -- connected to the Internet, but it represents a huge security risk to businesses and consumers, and it's already causing problems. Hackers are beginning to use inadequately secured gaming consoles, routers and modems to launch distributed denial-of-service (DDoS) attacks. Most are Universal Plug and Play (UPnP)-enabled, the underlying protocols of which can be abused. Akamai Technologies found 4.1 million Internet-facing UPnP devices were potentially vulnerable to being employed in DDoS attacks or abused in other ways. For example, the Moose malware tries to take over home routers by trying thousands of weak passwords; once it has taken over a device, it steals login details when people visit Twitter, Facebook and other social networking sites. Incorrectly configured home data storage devices (network-attached storage) are also providing hackers with an easy-to-access source of saleable data. As more and more everyday objects are

In this e-guide

connected to the Internet, the situation will only get worse. Are consumers really going to install the latest security patch for their fridge or think to erase data on their TV before reselling it on eBay?

Although sensors and computerized automation have been around for a long time, these systems have largely been disconnected from operational systems and the Internet. The transition we're seeing to more open network architectures, and particularly IoT, requires enterprises to re-evaluate their security policies and procedures to ensure these devices aren't open to abuse or sensitive data leaks. IoT devices should be risk assessed prior to being added to the network -- IOActive found the traffic control system used in Washington, D.C. transmits everything in plaintext and could easily be manipulated to allow an attacker to take complete control of the system.

Any approved device capable of connecting to the Internet has to be added to the enterprise's information asset register and included in the patch management process, as well as included in any penetration tests, as they are a possible attack vector. Configuration settings should always be hardened; IoT devices typically use default accounts and passwords, making them easy to compromise. Physical security also needs to be put in place. Business continuity plans will need updating, and bandwidth requirements will certainly need to be checked to ensure critical applications and processes can still access their required bandwidth, otherwise IoT devices could cause a self-induced denial of service.

The data paths between IoT devices need to be secure. If the data is sensitive, it will need to be encrypted, which means key management and identity management infrastructures are needed to control the relationships

In this e-guide

between devices; with 50 billion IoT-connected devices, it'll be impossible to securely authenticate each device relying on just a password. Where possible, enterprises should isolate these devices to their own network segment or VLAN. This will not only help to control IoT device discovery and contain any breaches, but will also make traffic management and monitoring easier. Monitoring the network traffic generated by IoT devices is going to be the best way to spot and stop malicious activity and attack traffic.

As with all things Internet, the commercial benefits and opportunities that IoT devices offer will see vendors rushing products to market before security concerns have been fully addressed. At present, IoT devices lack a common set of compliance requirements, though some organizations are working on various specifications. The Open Interconnect Consortium is defining a connectivity framework that includes consistent implementation of identity, authentication and security controls, while the AllSeen Alliance is working on an open framework to enable activities such as device discovery of adjacent devices, pairing, message routing and security.

IoT is a fast-evolving technology and enterprises need to put security in place from the beginning -- not as an afterthought -- otherwise IoT creates the possibility of attacks on a massive scale.

Next article

In this e-guide

How to cook up the right IoT security strategy for your enterprise

George Lawton, Contributor – SearchSOA

Enterprise architects need to rethink their security strategies as they begin leveraging the Internet of Things (IoT). Taking advantage of the capabilities of embedded system connectivity depends on opening up enterprise infrastructure to a much larger set of devices, all of which have the potential to introduce new IoT security vulnerabilities.

"Many IoT devices and applications that will be deployed soon, will not be engineered using secure development best-practices, leaving vulnerabilities that can be exploited to capture sensitive data," said Brian Russell, an engineer who focuses on cybersecurity solutions for Leidos, a national security, health and engineering solutions company, and who leads the Cloud Security Alliance's Secure Internet of Things Initiative. "It's going to be important that IoT manufacturers begin to acquire the expertise needed to ensure security across the product lifecycle."

The tools used to manage and enable all phases of IoT security are very immature. Billy Rios, founder of Laconicly, an IoT security consultancy, said, "We don't even have tools to help us accomplish simple tasks, like finding where all of our devices are on the network or ensuring the device user accounts have robust passwords. The software security on these devices is horrible."

In this e-guide

Hardcoded (backdoor) credentials, insecure protocols, weak authentication and data integrity are all extremely common. Forensics is really difficult. Rios explained, "Most organizations lack the tools and expertise to conduct incident and forensics investigations on these devices, so the devices are typically ignored when it comes to incident handling and forensics investigations."

Thinking outside the firewall

One big challenge is that IoT devices will bypass firewalls completely and create long-term connections to third party services, some of which aren't even outwardly known to the enterprise. Mark Stanislav, Sr. security consultant of strategic services at Rapid7, a security services consultancy, said "Enterprises deploying off-the-shelf IoT devices should be concerned about the level of network access those devices have, how much data they are transmitting, and what level of maturity the organization who builds the device has around information security."

If an IoT device were to be compromised, most organizations would have little hope of knowing what had occurred since there is very limited visibility into the inner-workings of IoT software and hardware. Many of these IoT devices would offer great capabilities for an attacker who is able to compromise a single device, and then work to move laterally throughout the network if not properly contained and segmented. "Data, whether video, audio, environmental or otherwise sensitive, can often be siphoned through a compromised IoT device and may provide criminals with valuable information to leverage over organizations," added Stanislav.

In this e-guide

The biggest difference in protecting IoT lies in thinking outside the firewall, since IoT implies being connected to the public Internet. Daniel Kador, co-founder and CTO of Keen IO, an IoT analytics service provider, said, "The question is not how to prevent devices from being compromised - they will be. The question is how to deal with it once it happens."

Addressing the patch gap

As the enterprise identifies new ways to create business value from connected devices, it may be tempting to leverage devices that were never intended to be connected or updated. Lorie Wigle, vice president, IoT Security Solutions at Intel Security said, "IoT deployments often include connecting devices that were not originally intended to be on a network and hence do not have any security designed into them. And industrial IoT devices, in particular, have very long lives with uptime or availability as their highest priority."

This means that patching can be problematic or even inappropriate. Another security concern is that IoT servers are generally not in access-restricted machine rooms, which means physical security is a greater concern as attackers can prod and poke at them, insert USB sticks and press buttons in ways that IT cannot control.

In this e-guide

Improving security assessment

Organizations need to evolve more Agile processes for assessing the sensitivity of IoT data that might be exposed in the wild, said Zach Supalla, founder and CEO at Spark IO, an open source IoT toolkit provider. IoT devices produce a lot of data, some of which is sensitive, and some of which is not. Applying appropriate security is somewhat trivial, but because a lot of applications are not sensitive, the biggest problems will be when the managers developing a product aren't sure what to secure and what not to secure.

In some respects, new IoT capabilities benefit from security through obscurity today. There are so many different specifications and protocols used that it is difficult for malicious hackers to create malware that can attack a large number of devices easily. Keen IO's Kador said, "We're in a pre-standardization phase right now, so it doesn't make much sense for black hats to spend much time here when they can focus on Windows exploits. But once we see standardization around IoT specs, expect a rising wave of exploits targeting those specs."

It's also a good idea for enterprises to take an inventory of their existing IoT vulnerability exposure. Laconicly's Rios said most enterprises don't realize that they already have a number of IoT devices in their environments. Smart environmental controls and energy management are extremely common. On any given corporate campus, there are a variety of sensors feeding information to smart HVAC, lighting, energy and access control systems.

In this e-guide

Rios said he has come across a number of conference room availability appliances that show the conference room schedule in real corporate enterprises. What many don't realize is these devices are horribly insecure. It should be concerning to enterprise architects that many of these devices retrieve availability information from Exchange servers, which means they usually have a set of corporate credentials on them.

Resource constrained devices

IoT security can be more challenging to implement because it is leveraging extremely resource constrained device, said Spark IO's Supalla. A computer running a general purpose operating system like Windows or Linux will have no problem establishing an encrypted connection with another server. But a microcontroller inside a coffeemaker doesn't have the same resources and access to the same crypto stacks, and it also might not have access to enough entropy to generate truly random numbers for cryptographic keys. These are solvable problems, but they require thoughtful implementation and expertise.

Enterprises might consider leveraging IoT toolkits which can help ensure best practices in the ways that connected devices access APIs and enterprise systems. For example, Spark IO, helps engineers and organizations develop connected products where all of the low-level plumbing is already taken care of so the engineer can focus on the application. Security and scalability are built in so that they are not issues that the engineer has to worry about.

In this e-guide

Enterprises should consider using the limitations of IoT devices to improve the security architecture with white listing technologies, said Intel Security's Wigle. Since IoT devices are not general purpose, think about deciding what applications and code can run on them rather than continuously updating what can't run on them. For example, Intel Security has more than 200 customers who build its white listing and change control solutions into their products.

Taking advantage of IoT security initiatives

IoT security analysis is still in the early phases. Enterprises might consider following the numerous industry and government to improve IoT security:

- The Cloud Security Alliance is working with a number of security experts to define IoT Security Guidance for Early Adopters.
- Other organizations such as OWASP, Builditsecure.ly, WhiteScope, and I am the Cavalry have also begun to contribute significantly to helping organizations build a secure IoT.
- The Open Interconnect Consortium has both an open source platform, IoTivity and standards development underway.
- The Industrial Internet Consortium is providing security guidance for companies;
- NIST is working on security for cyber physical systems.
- Cisco provided a "Grand Challenge" for IoT security efforts recently.

In this e-guide

- Intel Security also has a developer program for extending security management to other companies, called the Security Innovations Alliance, that allows solutions to plug into the ePolicy Orchestrator.

Rapid7's Stanislav said, "The biggest security strength of IoT innovation currently is the focus on standardization of firmware, APIs and software operating on these devices. In this nascent era of IoT, a Wild West of technologies create devices from thousands of vendors who share very little technological-DNA. While innovation is enabled through a lack of restraints on IoT device creation, it must ultimately change for sustainability and security maturity to occur."

Next article

In this e-guide

A rallying cry for IoT security standards, data governance

Jim Romeo, Contributor – SearchUnifiedCommunications

The light switch in your room sends the turn-on request to the Internet, and the lamp on the ceiling receives it from there.

That's how Gleb Nitsman, senior product manager for software developer DataArt, illustrates the Internet of Things (IoT).

"Suddenly the Internet becomes overfilled with billions of machine-to-machine requests that data centers and network facilities have to process in a timely manner," he said. This crossfire of data and networks is a vulnerable culture for industrial firms who rely on its future. For IoT, the battle cry for security and governance is on.

"With the IoT, the network's vulnerability creates the potential for connected devices in smart factories to be subjected to attack," said William Bain, ScaleOut Software CEO and founder in Bellevue, Wash. "Manufacturing facilities must implement pervasive security strategies to protect themselves from cyberthreats, for example, by encrypting all communications on critical infrastructure systems, using secure network protocols, and incorporating firewalls to isolate IoT devices from external networks. It is important to have a designated network administration team that constantly monitors the network and investigates potential threats. Lastly, IoT devices must meet

In this e-guide

appropriate standards for security and data governance to seamlessly fit within the organization's overall security strategy."

A sensitive point of exposure is critical processes that enterprises reveal on the Internet. That's a concern for Aron Semle, product manager for Kepware Technologies in Portland, Maine. "IoT will enable companies to do this by accident, so security needs to be in the forefront of everyone's mind and a key tenant when designing the network."

Semle added that the IoT networks operate under the guise of the Internet rather than a proverbial IT network. He said that a lot of what "saves" the industry today from typical security threats is that systems don't look like modern IT-based systems.

"Many don't expose Web servers and REST or SOAP APIs," he said. "IoT will change this." But Semle is concerned about raw data coming from manufacturing plants, and the IP this data holds. Regardless of the protocol -- MQTT, CoAP, AMQP, OPC UA and more -- there are standard ways to protect this data in transit, and when stored on the IoT system, he said. "So although this can't be ignored, I don't see it as a huge issue. The real focus should be on limiting the attack surface of IoT-enabled control networks."

Nowadays, more than ever, we live in a mobile world. We have smartphones with apps, tablets and a multitude of devices that rule our worlds, personally and professionally. Steve Durbin, managing director of the Information Security Forum noted that an increasing security threat comes from the BYOD movement and our emerging mobile mindset; mobile applications are

In this e-guide

increasingly managing all facets of our lives. The demand for mobile products is so rapid, security pros struggle to keep up with it.

"To meet this increased demand, developers are working under intense pressure, and on paper-thin profit margins, which is sacrificing security and thorough testing in favor of speed of delivery and the lowest cost," said Durbin. "This is resulting in poor-quality products that can be more easily hijacked by criminals or hacktivists."

Durbin added that while the IoT is still in its infancy, we have an opportunity to build in new approaches to security if we start preparing now. So the light switch that turns on remotely or the parameters that are monitored from miles away all need to be incorporated into security plans to ensure networks are safe.

"Security teams should take the initiative to research security best practices to secure these emerging devices, and be prepared to update their security policies as even more interconnected devices make their way onto enterprise networks," Durbin said. "Enterprises with the appropriate expertise, leadership, policy and strategy in place will be agile enough to respond to the inevitable security lapses. Those who do not closely monitor the growth of the IoT may find themselves on the outside looking in."

Next article

In this e-guide

Enterprise IoT security: Is the sky truly falling?

Jessica Scarpati, Contributor – SearchNetworking

It's hard to find someone more passionate about the Internet of Things than Bruce Perrin.

Perrin, chief operating officer and acting CIO of Phenix Energy Group -- a company based in Palm Harbor, Fla., that is building a crude oil pipeline across Central America -- hopes to incorporate the Internet of Things into "every conceivable environment." That means, for instance, instead of employees fumbling with key cards or PIN codes to move throughout a facility, building access would be controlled by facial recognition software.

Perrin believes enterprise IoT is the key to improve operational efficiency and reduce human error. Those goals carry an even greater sense of urgency for his company, which has 18 months to lay 220 miles of terrestrial and underwater pipeline and another six months to build the oil tank farms that it supports. In addition to deadline pressures, there is little room for error. Perrin estimates the company would lose $18,000 for every minute of downtime. A full system failure would take nine hours to restore, ultimately costing $9 million in lost revenue.

In this e-guide

"We want to take the human factor out of anything that can be done repetitiously," Perrin says. "It just automates the nonsense in my life so that I can get real work done."

But even as one of IoT's biggest champions, Perrin is acutely aware of the risks of adding hundreds of nontraditional devices to his network -- devices that run various operating systems, use any number of proprietary protocols and often don't have the resources for advanced security configurations. Those concerns have shaped his network design and procurement strategy.

"We are taking a sandbox approach, probably to an almost illogical extreme," Perrin says. "But the CEO said to me one day, 'If people get in here and start screwing around with our system, the first thing we're gonna do is mount your head on my wall and replace you with somebody else.' And I'm not fond of that idea. He's an OK guy, but I don't want to spend the rest of my death looking at him."

Amid horror stories in the consumer market about hacked baby monitors, connected cars that can be compromised or accidental denial of service attacks on smart homes, the buzz about enterprise IoT security risks has grown louder as IT departments move these projects into their labs and production environments.

There have been "no widely known IoT device breaches" executed against an enterprise, contends Verizon's 2015 Data Breach Investigations Report, which argues that any vulnerabilities reported so far were identified by researchers. Yet the fast-moving nature of IoT and the broader threat landscape means that could change at any moment. Networking

In this e-guide

professionals say they are worried, with 60% of those responding to TechTarget's 2015 purchasing intentions survey identifying security as one of the biggest challenges in IoT.

John Becker, chief governance officer at Phenix Energy, says the severity of IoT threats has been largely overhyped. But that hasn't stopped Phenix, and others, from shoring up their security efforts.

"The stuff we read about IoT is really alarmist and sensationalized," Becker says. "I think the bottom line is we need to focus on how systems are designed."

Where is the danger?

It's tempting to look at it this way: A light bulb or HVAC system can't run antivirus software, so IoT must be risky. But that's an oversimplified perspective, says John Pescatore, director of the SANS Institute, an information security training and certification company.

"You know what else you can't run antivirus on? An iPhone -- and iPhones don't get viruses," Pescatore says. "So whenever you hear anybody say, 'Uh oh, you can't run antivirus on that,' you should say 'Yay!' Because that generally means viruses won't run on it either, since antiviral software is essentially a rootkit."

In this e-guide

In some cases, IoT devices are being designed upfront with security in mind -- a far more deliberate effort than what went into the original operating systems for PCs and servers, he says.

And while it's likely that enterprise IoT devices will eventually become attractive targets to cybercriminals, it won't be because they want to flicker the lights on and off.

"I'd definitely be concerned with the HVAC or the sensors themselves being an entry point -- a backdoor for someone to come in and attack my system," says Steve Holtsclaw, vice president of IT at Del Papa Distributing, a beer distributor that has deployed IoT devices inside its warehouses and trucks. "Anything that has an IP address can be reached someway and somehow."

These threats can't be mitigated with the traditional approach to security, says Pete Lindstrom, a research director at IDC.

"We get caught up in frameworks for controls, but we're fighting the previous war. This is a different environment," Lindstrom says. "We have to get smarter about the analysis on the back end."

It means all eyes are on the network to take the lead.

"We used to say, 'OK, everybody. You have to use *this* operating system. And since you're using that operating system, I dictate you have to use *this* security software on it.' Those days are over in the Internet of Things," Pescatore says. "It puts more of a premium on what security you can do from the network when you can't put anything on the endpoint."

In this e-guide

Visibility and management challenges

You need to know what's on your network in order to secure it. It sounds simple enough, but for many IT departments, finding and shutting down rogue devices is an endless game of whack-a-mole. The Internet of Things dials that up a notch, as many vulnerability management systems that can identify "Bob's iPad" or "Carol's Dell laptop" can't recognize a network-connected air conditioner or door lock.

"The first problem anybody has to solve in the Internet of Things is being able to discover those devices," Pescatore says.

He recently spoke with the chief information security officer of a New England college who discovered 300 rogue devices in a building the college just moved into. His vulnerability scanning software couldn't identify the endpoints. His team tracked them down manually and discovered they were mostly Internet-connected devices like temperature sensors and video cameras left by the previous tenant.

"The unfortunate reality is most of what's being done today, sort of like the early days of Wi-Fi, is a lot of 'don't ask, don't tell.' Like, 'Oh, God. If I start looking, I'll find this stuff and have to do something about it,'" Pescatore says. "Enterprises that have gone the furthest in doing BYOD securely are actually in the best shape for the Internet of Things because most of them put in some form of network access control so they can detect when something connects to their network."

In this e-guide

Compounding this lack of visibility is another problem: fragmentation among IoT device manufacturers themselves.

George Stefanick, a wireless network architect at Houston Methodist Hospital, is intrigued by the possibilities of using IoT in healthcare. His team is conducting a proof of concept with a mobile app that would use Bluetooth beacons and Wi-Fi to recognize when a patient arrives at the hospital, check him into an appointment and provide navigation within the building to his doctor's office.

Although setting up the network to support the initiative has its challenges, it's still familiar territory for Stefanick. The bigger hurdle is evaluating and managing the various IoT platforms that run on top of it.

"I can't have 10 different widgets from 10 different [IoT device] vendors, but right now that's what we're seeing," he says. "We really want to have that one pane of glass."

Unlike the market for PC and smartphone operating systems, IoT platforms are not expected to consolidate. The result: It becomes far more difficult to employ a uniform approach to security, says Phenix Energy's Perrin.

"Every vendor has a proprietary communications methodology, and in order to operate with other companies' components, they have to open up some portion of their functionality to communicate with another device," Perrin says. "That creates significant vulnerabilities because every time you open a port in something, you create a doorway through which the bad guys can walk."

In this e-guide

Del Papa's Holtsclaw runs an enterprise IoT environment based primarily on equipment from Cisco, but he shares similar concerns about the industry at large.

"You've got all these devices and they're on multitudes of platforms -- Linux, Unix, Windows, Android, iOS -- and they're all speaking with a different type of communications [protocol]," he says. "How do you control all that? How do you manage it? How do you secure it?"

Tackling IoT security via the network

IoT introduces new challenges, but many classic best practices in network security -- segmentation, zone-based policies and shutting down stray ports -- still apply. Additional measures depend on an organization's risk tolerance and the culture of the IT department. Enterprises that are managing IoT environments today tackle the threats from various angles, ranging from a focus on authentication standards to a strategy of total lockdown to the use of third-party network appliances.

At Houston Methodist, Stefanick has found inconsistent support among IoT vendors for 802.1x, an enterprise-grade wireless authentication standard that uses the Extensible Authentication Protocol (EAP). As a wireless engineer, he struggles to find IoT devices that use 802.1x.

"When you look at these Internet of Things devices that are coming in, from what we've seen so far is they've all been using pre-shared keys," Stefanick says. "We've actually had to create test networks for a proof of concept in a

In this e-guide

manner that isn't as secure. Our feedback has been, 'Hey, we're not likely going to purchase this until you get more secure, and we need EAP authentication in order to do that.'"

IoT device manufacturers need to be transparent with enterprises about how their products interact with the network, he says.

Perrin is taking a similarly cautious approach at Phenix Energy after seeing vendors hawk so-called enterprise devices with consumer-grade security capabilities. And, like Stefanick, Perrin also avoids anything cloud-based to maintain tighter control.

Beyond that, Phenix is at the more aggressive end of the spectrum. Its office and data center in Honduras is connected via a 10 Gbps private fiber backbone to a redundant site in Palm Harbor. There are only two ports open in the Honduras office: one for telephony and another for Internet-based business activities. Perrin also blocks all traffic originating from countries with high rates of phishing activity, such as Brazil.

"We're effectively cut off, and we've had companies come in and say, 'Well, the only way we can work with you is if you open a port for us,' and we tell them, 'Thank you for coming by and don't bother us again,'" he says. "We won't open a port for them because we can't take that risk."

Perrin also won't use copper cabling along the pipeline where industrial equipment and IoT devices reside.

"We use fiber because you can't breach it without actually cutting it," he says. "And a cut, of course, immediately tells our system and Internet of

In this e-guide

Things devices that something's happened that's not supposed to, and it immediately shuts off data flow across that avenue and on one of our redundant fiber links."

At Del Papa, network-connected sensors monitor lighting, inventory and temperature -- lowering electricity costs and ensuring that the beer is well stocked and chilled properly. Sensors on the racks in the warehouse detect if inventory is low somewhere, which triggers an email alert to restock. Other sensors in the company's trucks can be configured to report if an employee is driving over the speed limit.

With so many of critical operations on the line, Holtsclaw says security remains a huge concern. He is currently testing an IoT gateway from Dell and Intel, which functions as a single point of access between his IoT devices and the Internet.

"It keeps external traffic from coming into those devices that sit directly on your network and talk back to that gateway," Holtsclaw says. "I really see that being a key player on the security side of IoT."

Next article

In this e-guide

Internet of Things security: Who is responsible and how is it done?

Shamus McGillicuddy, Senior Analyst – Enterprise Management Associates

Advocates say the Internet of Things is a multitrillion dollar business opportunity, but it's also a potential disaster for privacy and safety. Before we connect everything around us to the Internet, we need to think about security.

Internet of Things security is difficult to discuss because the concept is so immense. When you make "everything" IP-connected, how do you lock all of that down? Cars, cows, oil rigs, medical devices, refrigerators. There is no perimeter that can encircle all of that.

"The challenge we have is that each of those areas is really pretty separate," said Bret Hartman,

"The technologies working in those areas tend to focus specifically on their own area. It's not going to be one-size-fits-all for [Internet of Things] security."

Companies and individuals will also find that they lose a lot of control over where their data is and where it is going. When consumerization struck the enterprise, power and control over data and connectivity shifted from IT to the user. IT is still adapting to that shock. Now another shift is coming.

In this e-guide

"Power is shifting from the user to machines," said Dipto Chakravarty, executive vice president of engineering and products at ThreatTrack Security Inc. "And when it shifts to machines, connectivity is the inverse to security. The more connectivity you have, the less security you have -- unless you can layer it in properly."

Internet of Things security: It's not easy

Locking down the so-called "things" on the Internet of Things is a daunting task because security takes computing power, and many things have only the bare minimum -- if that.

"Usually these endpoint devices aren't very big. They don't have a lot of compute power to do much, especially around security," Hartman said. "There are IP-addressable light bulbs. There's not a whole lot of processing power left in there for security."

Furthermore, wherever you have an IP-connected thing, you also have an operating system. Operating systems need to be patched. When they aren't, hackers find vulnerabilities. Botnets will find millions of new recruits in the form of zombie appliances and other "things."

These things are all communicating with each other, too. And they influence each other.

"How much is going to go wrong if someone hacks a cow's monitoring system?" asked Eric Hanselman, chief analyst for New York-based 451

In this e-guide

Research. It's all just passive data collection. It's not a big deal." But data about a cow's health might go to another "thing" on a farm that crunches that data and spits out new data. Then that data goes elsewhere, all across IP networks.

"These are typically paths that are poorly protected. The bigger problem is not so much the endpoints, but the fact that the data paths themselves create a new attack platform."

"What if your microwave was taken over and it kept telling your fridge to shut down?" said Chakravarty of ThreatTrack. "You wouldn't know there was something wrong with your microwave. The user is slowly stepping out of the equation. We may be carrying a phone, but it's not just a phone. It's a transmitter and receiver that can propagate information exactly like a router would on a network."

Internet of Things security: How do you do it?

Some engineers say network monitoring is the way to solve the problem.

"It's much more about using the network fabric to watch traffic across all these devices and limit [that traffic] where there appears to be some abuse or potential attack happening, " Cisco's Hartman said. "In an industrial control system, you might change [a robot's] settings with a management console, but you wouldn't expect two robotic arms to reprogram each other. So you can look at that kind of traffic and say this shouldn't be happening. You can control and limit the traffic that goes among these [robots]."

In this e-guide

Internet of Things security will also require encryption key management infrastructure and identity management systems that can scale into the billions, said Earl Perkins, research vice president for Stamford, Conn.-based Gartner Inc.

"We'll have to figure out a way to protect data in an environment like this, whether it's on [an] Internet of Things 'thing' or in an intermediate location," he said. "We'll have to revamp the way we look at encryption key management and identity management. We'll have to combine capabilities from identity management and asset management, because [people] are going to become [their own] personal cloud networks. The Internet of Things that you carry on your person and that you have at home are like a cloud of devices that surround you. You have an identity and the things have identity, but how do you keep [up] with the relationships between you and the identity of those things?"

The Internet of Things will also require a sophisticated approach to risk management. Not all of the devices on the Internet of Things will be new. Organizations are strapping IP connections onto legacy devices and systems to extract data. Those legacy systems will pose a higher risk than something engineered from the ground up to be an IP endpoint.

"You need to add intelligence to be able to deal with the level of risk [presented] by these older types of data sources," 451 Research's Hanselman said.

In this e-guide

Internet of Things Security: Who owns the problem?

Clearly, there is a lot of work to be done in securing the Internet of Things. Before you even tackle the problem, you need to figure out who is responsible for it. Billions of new devices will start collecting and sharing data, and a wide assortment of companies will be enabling that. Who owns the problem?

"The issue is not clear at this point," Hanselman said. It's not even clear who would be held liable for damages associated with Internet of Things security breaches, he said. "If you look at the laws being handed down right now, the loss of privacy doesn't have an established value yet in the U.S."

The law is even murkier when it comes to liability for hacks of things that result in personal injury or real-world property damage, he said. For instance, the law is unclear about liability if someone hacks the braking system of a car, resulting in injury, damage or death. Is the car's manufacturer responsible for the security breach? "There will be case law that will establish this, but right now, they are out on a legal limb," Hanselman said.

In many cases, the manufacturers of the "things" on the Internet of Things won't be responsible for security. Instead, companies that provide the applications or connectivity will have to take charge.

"The problem of making sure the devices are secure will probably reside with those that provide a service through the device," Gartner's Perkins said.

"It could be whoever is providing the application and service itself, or it might be the service provider that provides the network. It may be both. One of the big problems ahead of us is going to be the liability and legal implications of these devices running wild."

Next article

In this e-guide

In this e-guide

Network-based controls: Securing the Internet of things

Johannes Ullrich, Dean of Research – SANS Technology Institute

Enterprise networks are becoming inundated with "smart" things and industrial sensors. But with no antimalware available, and little centralized configuration management, endpoint security is difficult -- if not impossible. Many devices, such as smart meters or the digital video recorders used in surveillance systems, don't connect to enterprise access controls or inventory and patching mechanisms. As a result, it's important to find methods for securing the Internet of things (IoT) and bring your own devices, using network-based controls that can scale and be centrally managed with existing tools.

Policies and technologies to enforce inventory controls are critical for data security and risk management. Most Internet-connected devices can only be managed efficiently via Dynamic Host Configuration Protocol, a network protocol used for automating IP parameters. DHCP can do a lot more than just hand out IP addresses and DNS settings. Its support for additional features is spotty, however. In some cases, firmware updates and configurations can be sent to devices -- DHCP is critical to advertise the location of these files.

DHCP logs and lease files can also provide reasonably good inventories. Restricting DHCP to known devices, or using it to segregate new devices

into subnets, is a commonly used technique to enforce inventory control policies. DHCP server configurations should always tie back to an IP address management and inventory control system. Figure 1 shows a small sample of DHCP logs that include the name of the device asking for an address.

DHCP Logs

```
DHCPREQUEST for 192.0.2.1 from 00:24:e4:dd:ee:ff (WSD-5CA8) via re1
DHCPREQUEST for 192.0.2.2 from 24:a4:3c:aa:bb:cc (unifac) via
re1_vlan2
DHCPREQUEST for 192.0.2.3 from 70:3e:ac:11:22:33 (iPhone) via re1
```

Figure 1: Devices identifying themselves as part of a DHCP request.

In addition to DHCP logging, devices need DNS for IP address management just like any other computer system using IP. While DNS was developed, in part, to save humans from having to remember IP addresses; for devices, DNS allows manufacturers to retain static host names for APIs that resolve to varying or multiple IP addresses. DNS requests can be used to assist in inventorying devices -- the queries can indicate the type of device and how it is used, as shown in Figure 2.

In this e-guide

DNS Requests

```
query: netcom.netatmo.net IN A + (10.5.0.86)
query: api.parse.com IN A + (fd14:5d44:4428:1::35)
query: scalews.withings.net IN A + (10.5.0.86)
```

Figure 2: DNS queries sent by a weather station, an iPhone and a scale.

Firewall Challenges

Luckily, most devices do not have to accept unsolicited connections from outside the perimeter. But many systems still need to establish outbound connections.

Restricting these connections is tricky, especially if a device wants to connect to cloud services or content delivery networks. It's hard, if not impossible, to establish sensible firewall rules in these cases. With HTTP connections, it may be possible to proxy the connections and inspect the data that's sent and received, in an attempt to eliminate data leaks and detect malicious code retrieved by the device.

Often overlooked as a sensor, the Network Time Protocol (NTP) is still used by many devices to synchronize computer clock times on packet-based networks. In some cases, devices use a pre-set NTP server, which may

indicate which device is sending the NTP request. Some systems may attempt to connect to a NTP server assigned via DHCP.

Most security teams have access to these types of network-based controls. To develop better security processes for the Internet of things, all it takes is use of these existing tools to start looking for potential events associated with devices, and enforcement of inventory control policies.

Next article

In this e-guide

In this e-guide

About IoT Agenda

IoT Agenda covers all aspects of Internet of Things technology and strategy as it relates to enterprise IT, including the technologies that enhance and enable internal business processes, and the resulting IoT products themselves -- the "things" that the business produces.

Our coverage from award-winning editors and leading industry experts readies businesses looking to deploy monitors in the field, embed sensors to help them improve products, manage their inventories and supply chains, and distribute intelligence to improve their work environments and production floors.

This is new territory, and IT and business professionals need expert assistance to make the leap. IoT Agenda is the leading site focused on the needs of enterprises grappling with IoT.

For further reading, visit us at http://InternetofThingsAgenda.com

Images; Fotalia