The Internet of Things

Activities in the U.S. Government

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the
U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational
Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business
Privacy Plan (McGraw Hill)

Introduction

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits.

The growth of network-connected devices, systems and services comprising the IoT provides efficiencies and personalization of experience that is attractive to both manufacturers and consumers. Network connected devices, systems, and services are also increasingly integrated with and relied upon by our Nation's critical infrastructure, leading to a national dependency. The characteristics of the IoT ecosystem also result in multiple opportunities for malicious actors to manipulate the flow of information to and from network connected devices. Important processes that once were performed manually, and therefore enjoyed a measure of immunity against malicious cyber activity, are growing more vulnerable. Recent large scale distributed denial of service attacks foreshadow increasing in the US and elsewhere.

In 2008, the U.S. National Intelligence Council warned that the Internet of Things (IoT) would be a disruptive technology by 2025. The Council said that individuals, businesses, and governments were unprepared for a possible future when network interfaces reside in everyday things. Almost six years later, this warning remains valid, though it now seems certain that the IoT will be disruptive far sooner than 2025—if it is not so already. More recently in January 2014, the Director of National Intelligence (DNI) stated that "[t]he complexity and nature of these systems means that security and safety assurance are not guaranteed and that threat actors can easily cause security and/or safety problems in these systems."

Several statistics validate the Government's concerns: the number of Internet-connected devices first outnumbered the human population in 2008, and that number continues to grow faster than the human population. By 2013, there were as many as 13 billion Internet-connected devices, and projections indicate that this will grow to 50 billion or more by 2020, generating global revenues of greater than $8 trillion by 2020. Many of these systems are visible to any user, including malicious actors, as search engines are already crawling the Internet indexing and identifying connected devices.

The IoT is the latest development in the decades-old revolution in communications, networking, processing power, miniaturization, and application innovation and has radically altered communications, networks, and sensors. The IoT is a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world. However, the IoT differs from previous technological advances because it has surpassed the confines of computer networks and is connecting directly to the physical world. Just as modern communications have fundamentally altered national security and emergency preparedness (NS/EP), the IoT has had a similar transformative impact.   Throughout the communications revolution, a plethora of existing and new technologies have led to astonishing improvements in the efficiency and effectiveness of Government and private sector operations and capabilities; yet the IoT differs in the pace, scale, and breadth of deployment of interconnected devices, which has resulted in immense benefits to individuals and organizations. Despite the benefits, the IoT is accompanied by risk associated with increased dependencies, expanded number of devices, and associated interconnections that will create a large attack surface with numerous potential threat vectors.

The increased attack surface and our Nation's dependence on these new systems, either directly or through the critical infrastructure systems in which they are embedded, has made the IoT and new systems natural targets for criminals, terrorists, and nation states that wish to exploit them. These dependencies will continue to increase as the IoT permeates all sectors of the economy and all aspects of people's lives.

While all users have to cope with this expanded attack surface, IoT applications in the NS/EP domain must be hardened against the potential risks. As IoT manufacturers and vendors Interests Out to 2025.

Source: https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf

The Federal Trade Commission IOT Report

January 27, 2015

The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits. However, the FTC report also notes that connected devices raise numerous privacy and security concerns that could undermine consumer confidence.

“The only way for the Internet of Things to reach its full potential for innovation is with the trust of American consumers,” said FTC Chairwoman Edith Ramirez. “We believe that by adopting the best practices we’ve laid out, businesses will be better able to provide consumers the protections they want and allow the benefits of the Internet of Things to be fully realized.”

The Internet of Things universe is expanding quickly, and there are now over 25 billion connected devices in use worldwide, with that number set to rise significantly as consumer goods companies, auto manufacturers, healthcare providers, and other businesses continue to invest in connected devices, according to data cited in the report.

The report is partly based on input from leading technologists and academics, industry representatives, consumer advocates and others who participated in the FTC’s Internet of Things workshop held in Washington D.C. on Nov. 19, 2013, as well as those who submitted public comments to the Commission. Staff defined the Internet of Things as devices or sensors – other than computers, smartphones, or tablets – that connect, store or transmit information with or between each other via the Internet. The scope of the report is limited to IoT devices that are sold to or used by consumers.

Security was one of the main topics addressed at the workshop and in the comments, particularly due to the highly networked nature of the devices. The report includes the following recommendations for companies developing Internet of Things devices:

- build security into devices at the outset, rather than as an afterthought in the design process;
- train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;
- ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
- when a security risk is identified, consider a “defense-in-depth” strategy whereby multiple layers of security may be used to defend against a particular risk;
- consider measures to keep unauthorized users from accessing a consumer’s device, data, or personal information stored on the network;

- monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.

Commission staff also recommend that companies consider data minimization – that is, limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely. The report notes that data minimization addresses two key privacy risks: first, the risk that a company with a large store of consumer data will become a more enticing target for data thieves or hackers, and second, that consumer data will be used in ways contrary to consumers' expectations.

The report takes a flexible approach to data minimization. Under the recommendations, companies can choose to collect no data, data limited to the categories required to provide the service offered by the device, less sensitive data; or choose to de-identify the data collected.

FTC staff also recommends that companies notify consumers and give them choices about how their information will be used, particularly when the data collection is beyond consumers' reasonable expectations. It acknowledges that there is no one-size-fits-all approach to how that notice must be given to consumers, particularly since some Internet of Things devices may have no consumer interface. FTC staff identifies several innovative ways that companies could provide notice and choice to consumers.

Regarding legislation, staff concurs with many stakeholders that any Internet of Things-specific legislation would be premature at this point in time given the rapidly evolving nature of the technology. The report, however, reiterates the Commission's repeated call for strong data security and breach notification legislation. Staff also reiterates the Commission's call from its 2012 Privacy Report for broad-based privacy legislation that is both flexible and technology-neutral, though Commissioner Ohlhausen did not concur in this portion of the report.

The FTC has a range of tools currently available to protect American consumers' privacy related to the Internet of Things, including enforcement actions under laws such as the FTC Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act; developing consumer education and business guidance; participation in multi-stakeholder efforts; and advocacy to other agencies at the federal, state and local level.

In addition to the report, the FTC also released a new publication for businesses containing advice about how to build security into products connected to the Internet of Things. "Careful Connections: Building Security in the Internet of Things" encourages companies to implement a risk-based approach and take advantage of best practices developed by security experts, such as using strong encryption and proper authentication.

The Commission vote to issue the staff report was 4-1, with Commissioner Wright voting no. Commissioner Ohlhausen issued a concurring statement, and Commissioner Wright issued a dissenting statement.

Source: https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

Securing the Internet of Things Security Tip (ST17-001)

Original release date: November 16, 2017

The Internet of Things is becoming an important part of everyday life. Being aware of the associated risks is a key part of keeping your information and devices secure. The Internet of Things refers to any object or device that sends and receives data automatically through the Internet. This rapidly expanding set of “things” includes tags (also known as labels or chips that automatically track objects), sensors, and devices that interact with people and share information machine to machine.

Why Should We Care?

Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to other machines and trigger additional actions. Examples include devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; control systems that deliver water and power to your workplace; and other tools that track your eating, sleeping, and exercise habits.

This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed.

What Are the Risks?

Though many security and resilience risks are not new, the scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones. Attackers take advantage of this scale to infect large segments of devices at a time, allowing them access to the data on those devices or to, as part of a botnet, attack other computers or devices for malicious intent. See Cybersecurity for Electronic Devices, Understanding Hidden Threats: Rootkits and Botnets, and Understanding Denial-of-Service Attacks for more information.

How Do I Improve the Security of Internet-Enabled Devices?

Without a doubt, the Internet of Things makes our lives easier and has many benefits; but we can only reap these benefits if our Internet-enabled devices are secure and trusted. The following are important steps you should consider to make your Internet of Things more secure.

Evaluate your security settings. Most devices offer a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of software, or if you become aware of something that might affect your device, reevaluate your settings to make sure they are still appropriate. See Good Security Habits for more information.

Ensure you have up-to-date software. When manufacturers become aware of vulnerabilities in their products, they often issue patches to fix the problem. Patches are software updates that fix a particular issue or vulnerability within your device's software. Make sure to apply relevant patches as soon as possible to protect your devices. See Understanding Patches for more information.

Connect carefully. Once your device is connected to the Internet, it's also connected to millions of other computers, which could allow attackers access to your device. Consider whether continuous connectivity to the Internet is needed. See Securing Your Home Network for more information.

Use strong passwords. Passwords are a common form of authentication and are often the only barrier between you and your personal information. Some Internet-enabled devices are configured with default passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Choose strong passwords to help secure your device. See Choosing and Protecting Passwords for more information.

The following organizations offer additional information about this topic:

Online Trust Alliance: https://otalliance.org/smarthome
Open Web Application Security Project (OWASP):
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
https://www.owasp.org/index.php/IoT_Security_Guidance
Atlantic Council: http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
Networks of 'Things' (NIST Special Publication 800-183):
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
Department of Homeland Security: https://www.dhs.gov/securingtheIoT
Stop.Think.Connect.: https://www.dhs.gov/stopthinkconnect

Authors: Stop.Think.Connect. and National Cybersecurity and Communications Integration Center (NCCIC)

Source: https://www.us-cert.gov/ncas/tips/ST17-001

Strategic Principles for Securing the Internet Of Things (IoT) Version 1.0

U.S. Department of Homeland Security

November 15, 2016

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IoT is almost without limit.

Prioritizing IoT Security

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security. In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure. In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the need for urgent action. IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally.... there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.

The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely-adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

- Incorporate Security at the Design Phase
- Advance Security Updates and Vulnerability Management
- Build on Proven Security Practices
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

As with all cyber security efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security. Specifically, these principles are designed for:

- IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
- IoT manufacturers to improve security for both consumer devices and vendor managed devices;

- Service providers, that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
- Industrial and business-level consumers (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.

There is, however, no one-size -fits -all solution for mitigating IoT security risks. Not all of the practices listed below will be equally relevant across the diversity of IoT devices. These principles are intended to be adapted and applied through a risk-based approach that takes into account relevant business contexts, as well as the particular threats and consequences that may result from incidents involving a network-connected device, system, or service.

Incorporate Security at the Design Phase

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed.

By focusing on security as a feature of network-connected devices, manufacturers and service providers also have the opportunity for market differentiation. The practices below are some of the most effective ways to account for security in the earliest phases of design, development, and production.

What are the potential impacts of not building security in during design? Failing to design and implement adequate security measures could be damaging to the manufacturer in terms of financial costs, reputational costs, or product recall costs. While there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.

Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable. Build the device using the most recent operating system that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Use hardware that incorporates security features to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.

Promote Security Updates and Vulnerability Management Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies. In designing these strategies, developers should consider the implications of a device failure, the durability of the associated product, and the anticipated cost of repair. In the absence of the ability to deploy security updates, manufacturers may be faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

FOCUS ON: NTIA Multi-Stakeholder Process on Patching and Updating The National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the “Internet of Things Upgradability and Patching” to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption.

SUGGESTED PRACTICES:

Consider ways in which to secure the device over network connections or through automated means. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities. Consider coordinating software updates among third-party vendors to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

Develop automated mechanisms for addressing vulnerabilities. In the software engineering space, for example, there are mechanisms for ingesting information from critical vulnerability reports sourced from the research and hacker communities in real time. This allows developers to address those vulnerabilities in the software design, and respond when appropriate. Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities.

A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.

Develop an end-of-life strategy for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.

Build on Recognized Security Practices Many tested practices used in traditional IT and network security can be applied to IoT . These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices. Start with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

Refer to relevant Sector-Specific Guidance, where it exists, as a starting point from which to consider security practices. Some federal agencies address security practices for the unique sectors that they regulate. For example, the National Highway Traffic Safety Administration (NHTSA) recently released guidance on Cybersecurity Best Practices for Modern Vehicles that address some of the unique risks posed by autonomous or semi-autonomous vehicles. Similarly, the Food and Drug Administration released draft guidance on Postmarket Management of Cybersecurity in Medical Devices.

Practice defense in depth. Developers and manufacturers should employ a holistic approach to security that includes layered defenses against cybersecurity threats, including user-level tools as potential entry points for malicious actors. This is especially valuable if patching or updating mechanisms are not available or insufficient to address a specific vulnerability. Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.

The Department of Homeland Security’s (DHS) National Cybersecurity and Communications Integration Center (NCCIC), as well as multi-state and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

Prioritize SecurityMeasures According to Potential Impact Risk models differ substantially across the IoT ecosystem. For example, industrial consumers (such as nuclear reactor owners and operators) will have different considerations than a retail consumer. The consequences of a security failure across different customers will also vary significantly.

Focusing on the potential consequences of disruption, breach, or malicious activity across the consumer spectrum is therefore critical in determining where particular security efforts should be directed, and who is best able to mitigate significant consequences.

Should IoT security measures focus on the IoT device? Since the purpose of all IoT processes is to take in information at a physical point and motivate a decision based on that information (sometimes with physical consequences), security measures can focus on one or more parts of the IoT process.

SUGGESTED PRACTICES:

Know a device's intended use and environment, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary. Perform a "red-teaming" exercise, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures.

Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Reliance on the many low -cost, easily accessible software and hardware solutions used in IoT can make this challenging. Because developers and manufactures rely on outside sources for low -cost, easily accessible software and hardware solutions, they may not be able to accurately assess the level of security built into component parts when developing and deploying network-connected devices. Furthermore, since many IoT devices leverage open source packages, developers and manufacturers many not be able to identify the sources of these component parts. Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers, and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

SUGGESTED PRACTICES:

Conduct end-to-end risk assessments that account for both internal and third party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.

Consider creating a publicly disclosed mechanism for using vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

Consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues.

A list can serve as valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption. IoT consumers can also help contain the potential threats posed by network connectivity by connecting carefully and deliberately, and weighing the risks of a potential breach or failure of an IoT device against the costs of limiting connectivity to the Internet.

In the current networked environment, it is likely that any given IoT device may be disrupted during its lifecycle. IoT developers, manufacturers, and consumers should consider how a disruption will impact the IoT device's primary function and business operations following the disruption.

Does every networked device need continuous, automated connection to the Internet? In 2015, the Federal Trade Commission published a guide called “Start with Security: A Guide for Businesses” to help them determine this very question. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device – and systems; for example, nuclear reactors, where a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.

SUGGESTED PRACTICES:

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions.

Make intentional connections. There are instances when it is in the consumer's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://ics-cert.us-cert.gov/recommended_practices.