(In)security of the Internet of Things (IoT)*

Lucy L. Thomson, Esq. CISSP *

Widespread IoT Cybersecurity Risks Create Daunting Challenges

It is predicted that by 2020 there will be 20.4 billion devices connected to the Internet, impacting all aspects of personal life, and business and industry. IoT innovations promise better business management and greater efficiencies, but the IoT ecosystem that is now being created presents complex challenges. Gartner’s latest Internet of Things Backbone Survey of Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) showed that security was cited as the top barrier to IoT success (35 percent of respondents), as “the explosion of varying types of IoT endpoints creates an attack surface that has never before [been] seen.”

Total spending on endpoints and services reached almost $2 trillion in 2017. Consumers are the largest group of users of connected things with 5.2 billion devices in 2017, 63 percent of the total. Spending for business-to-business (b2b) IoT systems (e.g., manufacturing, health care, agriculture, transportation, utilities, etc.) is expected to reach $267 billion by 2020.

Industrial Internet of Things (IIoT). IIoT includes smart electrical grids, connected health care devices and hospitals, intelligent transportation, smart factories, and other cyber-physical systems. This infrastructure provides essential services, such as energy, water, telecommunications, transportation, and financial services, and is increasingly subject to sophisticated cyber intrusions.

---


* Lucy L. Thomson, CISSP, is the founding principal of Livingston PLLC in Washington, D.C. She focuses her practice on legal and technology issues related to cybersecurity, global data privacy, compliance, and risk management. Previously a senior engineer and privacy advocate at CSC, a global technology company, she worked on two of the government’s largest technology modernization projects. A career attorney at the U.S. Department of Justice, she managed and conducted complex litigation in the Criminal and Civil Rights Divisions. She served as 2012-13 Chair of the ABA Section of Science & Technology Law and is a member of the House of Delegates and the Cybersecurity Legal Task Force. She is co-editor of the ABA Internet of Things (IoT): Legal, Policy, and Practical Strategies, forthcoming 2019, editor of the ABA Data Breach and Encryption Handbook and a contributing author to the ABA Cybersecurity Handbook (2d. Ed.) and Homeland Security and Emergency Management (3d. Ed.). Appointed Consumer Privacy Ombudsman in 25 federal bankruptcy cases, she has overseen the disposition of more than 250 million electronic consumer personal records. She received a Master’s degree from Rensselaer Polytechnic Institute (RPI) in 2001, earned the CISSP and CIPP/US certifications, and holds a J.D. degree from the Georgetown University Law Center.


3. Id.

4. See, e.g., Industrial Internet Consortium, https://www.iiconsortium.org/index.htm. “An Industrial Internet of Things (IIoT) system connects and integrates industrial control systems with enterprise systems, business processes and analytics. It enables significant advances in optimizing decision-making, operations and collaborations among a large number of increasingly autonomous control systems.”
According to the International Data Corporation (IDC), the three industries that are expected to spend the most on IoT in 2018 are manufacturing ($189 billion), transportation ($85 billion), and utilities ($73 billion). Manufacturers will focus largely on improving the efficiency of their processes and asset tracking, while two-thirds of IoT spending by transport will go toward freight monitoring and fleet management. IoT spending in the utilities industry will be dominated by smart grids for electricity, gas, and water. IDC puts spending on cross-industry IoT areas like connected vehicles and smart buildings at nearly $92 billion in 2018.

**Torrents of data at risk.** Internet-connected devices generally sense, collect, process, and transmit a wide array of data, ranging from consumer personally identifiable information (PII) to proprietary company information and infrastructure data used to make critical real-time decisions or to effect a change in the physical world. IDC predicts that 163 zettabytes (ZB), or one trillion gigabytes, of data will be created or copied each year by 2025, ten times more than in 2016. By 2035, the IoT will be composed of a trillion connected devices producing ten trillion data streams. Cisco estimates that by the end of 2019, the IoT will generate more than 500 zettabytes per year in data—and in the years beyond, that number is expected to grow exponentially, not linearly. The amount of data stored on devices will be four and a half times higher than data stored in data centers, at 5.9 ZB by 2021.

The convergence of information technology and physical infrastructure operations in which computers control a broad array of consumer and industrial devices and systems present significant security concerns. Many IoT devices that have little or no computer security and contain documented vulnerabilities are being connected to the Internet and to each other, creating widespread risks. Cyberattacks involving IoT can compromise the security, privacy, and safety of individuals and their homes, businesses, transportation systems, industrial control systems (ICS), and even entire cities or industry sectors.

There is increased risk for wide-scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans.

---

6. Id.

Sixteen government and private industry sectors have been designated as critical infrastructure (CI): Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Health Care and Public Health; Information Technology; Nuclear Reactors; Materials and Waste; Transportation Systems; and Water and Wastewater Systems. Election systems are a CI “subsystem.” See https://www.dhs.gov/critical-infrastructure-sectors; National Infrastructure Protection Plan (NIPP), NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/national-infrastructure-protection-plan.
High penetration of IIoT technology in critical infrastructure industries has resulted in increased risks. The damage that could be caused by IoT devices with inadequate security is far-reaching. IoT security breaches may pose life-and-death risks, the inappropriate use of personal data, or theft and fraud. A hacker attack on a smart grid system could potentially turn off power to millions of households and businesses, creating massive economic harm and threats to health and safety. Other potential consequences of an IoT/ICS incident can range from disruption of operations and services (damaging equipment, reduction or loss of production at one site or multiple sites simultaneously) to catastrophic—jeopardizing national security or public safety (terrorist attack; release, diversion, or theft of hazardous materials; product contamination; or environmental damage).

**The Need for Risk-Based Assessment**

In the short term, executives, policy makers, system owners, security experts, and their counsel must understand the IoT cyber risks and take appropriate action to protect their information systems in order to avoid the serious and even catastrophic consequences that could ensue. Most hacker attacks are opportunistic and target not only the largest businesses but all those that are unprepared. Taking the steps necessary to prevent, detect, and respond to security breaches and incidents should be everyone’s primary goal. Conducting a risk assessment is an essential first step to determine how much risk is being introduced by implementing IoT devices in the environment and what can be done to mitigate it. In this high-risk IoT environment, mitigation of risk is paramount and requires a thorough understanding of the IoT ecosystem. In the longer term, industry and government officials must reach consensus on how to secure the IoT infrastructure.

Every information system is different, and risk assessments must be tailored to the data, design and architecture, hardware and software, and technology implementations of the system or network. Specific threats to and vulnerabilities in the system must be identified, as well as the likelihood that adverse events will actually occur. Organizations can then select appropriate security controls and develop remediation plans so that the risks will be reduced to a reasonable and appropriate level.

**Changing Nature of the Global Threat**

Previously, criminals launched cyberattacks primarily for financial gain; now, nation-states and organized criminal groups are attempting to damage, disrupt, or modify infected IoT and industrial control systems (ICS) and networks. Cyberattacks on organizations generally, and on critical infrastructure in particular, can have catastrophic effects on safety and public health, disrupting or cutting off essential services (e.g., health care and emergency services, food, transportation, energy and power, and water supply and waste management, to highlight just a few).
few). Many of these threat actors have significant resources, funded by nation-states or through sophisticated money laundering operations.

The Intelligence Community’s 2017 Worldwide Threat Assessment\(^\text{13}\) and the Foreign Cyber Threats report\(^\text{14}\) identify prominent cyber adversaries—nation-states (Russia, China, North Korea, and Iran), terrorist groups, and cyber criminals. In addition, “hacktivists” launch cyberattacks that are politically or ideologically motivated. The 2018 Verizon Data Breach Investigations Report (DBIR)\(^\text{15}\) found that almost three-quarters (73 percent) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12 percent. Over a quarter (28 percent) of attacks involved insiders.\(^\text{16}\)

The Cyber Threats report concludes that “[d]espite ever-improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come from remote hacking to establish persistent covert access, supply chain operations that insert compromised hardware or software, malicious actions by trusted insiders, and mistakes by system users.”\(^\text{17}\)

The U.S. Departments of Commerce and Homeland Security released a report that offers a guide to government, civil society, and industry on actions that would dramatically reduce the threat of botnets\(^\text{18}\) and similar cyberattacks. The Commerce/DHS Report concluded:

To address the range of threats, all stakeholders, domestic and international, must more fully address automated, distributed attacks. At its core, that involves reducing the number of unsecured devices with access to the Internet to keep botnets to a manageable size, and developing mechanisms to share information about compromised systems and

---

17. 2017 Cyber Threats report, supra note 17.
18. Bots/botnets are everywhere in technology; they are automated programs/applications designed to perform a specific task, ranging from malicious bots that come with a virus to search engine spiders that crawl the Internet looking for new web pages, as well as, for example, Siri and Cortana. 2018 Verizon DBIR, Leading Threat Actions and Patterns, supra note 15.
emerging attack trends up and down the network stack to the party (or parties) in the best position to respond to the threat.  

Risks to Confidentiality, Integrity and Availability

Confidentiality. Protecting ‘confidentiality, integrity, and availability’ are the three cornerstones of every security program. In light of the massive data breaches in recent years, much attention has been given to protecting the confidentiality of personal data and sensitive and confidential information. The largest data breaches—spanning the financial, health care, retail, and government sectors—illustrate the heightened risk to millions of individuals when large datasets of sensitive personal information are compromised: Marriott/Starwood, 5 billion personal records compromised (2018); Equifax, 145.5 million records breached (2017); Sony Online Entertainment, 102 million (2011); JP Morgan Chase, 76 million (2014); Anthem BlueCross BlueShield, 69 to 80 million (2015); and Office of Personnel Management (OPM), 22.5 million security clearance records breached, 5 million fingerprints stolen (2015).

Integrity. One of the most important observations of the 2015 Worldwide Threat Assessment is that future cyberattacks will be conducted to compromise the integrity of information, with a potentially devastating impact on key information systems that constitute the underpinnings of the economy:

In the future [ ] we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decision-making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving. Cyberattacks that successfully change or manipulate business records or decision-making systems could paralyze companies, bring operations to a halt, and undermine the trust in entire industry sectors. Databases are vulnerable to attacks and can be accessed through insecure IoT devices.

Availability. In recent years, cyberattacks designed to restrict the availability of websites and services have been launched, primarily with distributed denial of device (DDoS) attacks in

20. Confidentiality—protection of information against unauthorized disclosure, whether intentional or accidental. Integrity—protection of information against corruption, tampering, or other alteration; this capability includes safeguarding the accuracy and completeness of information. Availability—ensuring that information and systems can be reliably and promptly accessed and used when they are needed.
21. In total, 11,239,084,942 records have been compromised in 8,908 breaches reported since 2005. Chronology of Data Breaches, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches. A website that goes by the name “information is beautiful” provides a visualization of thousands of the major data breaches over the past decade and serves as a useful resource to identify and learn about the massive data breaches that have affected the private sector and government. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.
which multiple compromised computers, often infected with a Trojan virus, are used to overwhelm a single targeted system, computer viruses that delete user data, or ransomware that encrypts data and demands payment for the encryption key to restore access to the data. According to the Verizon Data DBIR, DDoS attacks accounted for 56 percent of the incidents reported in 2017.

The Complex IoT Technology Infrastructure

Security is only as strong as its weakest link, and this is particularly true of the IoT. Its distributed architecture presents a plethora of vulnerable points in processing and storage where sensitive and proprietary data can be stolen and critical infrastructure can be compromised.

Experts agree that many low-power IoT devices are inherently insecure. Because low cost and speed to market are priorities, security is often not built into the IoT design, or it may be minimal. Vulnerabilities are not eliminated and software is not updated regularly. When these devices hit the market, they do not have the ability to respond to the complex evolving threat landscape. Home security systems and household appliances, for example, whose device life cycle is much longer (more than ten years) than the software on the devices (about two years) may introduce risk for years to come when vendors fail to provide patching or support for the software in the future. IoT devices are also being used in ways they were not designed for, particularly medical devices that were originally intended to be stand-alone.

What Makes IoT Devices Vulnerable to Cyber Attacks? Common IoT Attack Vectors

The IoT heightens existing concerns about cybersecurity and introduces new risks. Many IoT devices and systems are the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances. From a security perspective, experts have identified “attack surfaces” associated with IoT devices. Vulnerabilities in IoT devices create new attack vectors (i.e., entry points) for hackers. To fully appreciate how so much can go wrong with IoT security, it is important to understand the fundamental classes of security defects in the context of “attack surfaces” and what security measures exist to mitigate them.

Attack surfaces in the IoT infrastructure fall into three categories, all of which are further explained in the following sections: (1) IoT devices (a “thing”), including the operating system (OS) and software on the device; (2) a network of “things,” devices, and sensors; and (3) the IoT ecosystem and the context in which the IoT network will operate.

23. Malware disguised as legitimate software that will enable a cybercriminal to gain access to a user’s system and spy on him/her, steal sensitive data, and gain backdoor access.
27. The Commerce/DHS Botnet Report describes in more detail the current status of the technical and policy domains of the Internet and worldwide communications ecosystem. Supra note 22, at 9–21. NIST analyzes three categories in terms of “trust concerns” with IoT. NIST IoT Trust Concerns, supra note 12.
1. Security of the “Thing”

Most IoT systems contain four architectural elements: sensors, a control center, actuators, and a communications network linking those elements. Sensors typically collect information, the communications network delivers the information to the control center, the control center evaluates the information and issues commands, the communications network delivers the commands to the actuators, and the actuators perform some action. In the most simple terms, a “thing” is an object equipped with sensors that gather data that will be transferred over a network and actuators that allow things to act (for example, to switch a light on or off, open or close a door, increase or decrease engine rotation speed, and more). Connected things produce huge volumes of data which need to be securely transmitted and protected from cybercriminals.

NIST has observed that due to the nature of various IoT devices, such as the need to be portable, IoT designs can pose barriers to cybersecurity. An overview of key device constraints and security concerns are described in following table.

<table>
<thead>
<tr>
<th>NIST IoT Cybersecurity Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consideration</td>
</tr>
<tr>
<td>Power Consumption</td>
</tr>
<tr>
<td>Low Cost</td>
</tr>
<tr>
<td>Life Cycle</td>
</tr>
</tbody>
</table>


**Configuration.** Vulnerabilities in the design and configuration of IoT devices lead to security breaches. Many IoT devices come with fixed or hardcoded credentials, utilities, and services that cannot be disabled, updated, or patched. Even if software is securely developed, improper configuration when deploying systems can expose them to compromise. Many of the vulnerabilities discovered are years or decades old and firmware packages may use old and/or unsupported versions of third-party components.

**Weak passwords.** Manufacturers have default, easy-to-guess user ID/password combinations to log in to IoT devices, and users may leave the device’s log-in credentials unchanged. Because the default passwords are published online, they are among the known
attack vectors for the devices. Passwords may be hardcoded into the IoT firmware, and the tools necessary to disable them are not present; thus, a user cannot feasibly change the password.

**Lack of encryption.** Many IoT devices do not support encryption. Hackers can intercept unencrypted data as it is transmitted to and from IoT devices.

**Insecure wireless connections.** These can be hijacked and used by hackers to install malware, gain control of the device or system, and steal personal data or corporate information or cause widespread damage to physical systems.

**Backdoors.** IoT devices may have a backdoor built in, ostensibly to make it easier to provide support for them. These “hidden” access mechanisms that consist of the user ID and password to an open port can also provide an entry point for hackers.

**Subversion of the software development process.** Not only is software development difficult to manage from a vulnerability perspective, but efforts to actively subvert software are increasing. For example, developers are in some cases specifically targeted for attack. Malware has been detected in certain open source software libraries.

**Patches and software updates.** Unlike traditional personal computers, there are few security upgrade processes for “things,” such as patches or updates. When vulnerabilities are identified after IT devices are deployed, these devices may be difficult or impossible to patch.

**Sensor data.** Sensor data may be tampered with, stolen, deleted, dropped, or transmitted insecurely, allowing it to be accessed by unauthorized parties. Various sensors, such as cameras and microphones, may be surreptitiously turned on.

**Applications.** Hackers can insert malware (malicious code) into applications (apps) to gain access to the device and to sensitive information. Some malware can cause users’ personal information to be publicly disclosed without their knowledge.

### 2. A Network of “Things”

The distributed architecture of IoT presents a plethora of vulnerable points in processing and storage where sensitive and proprietary data can be stolen and critical infrastructure can be compromised. Things connected to the Internet are entry points for criminals. IoT multiplies the normal risks associated with any data communication. Each device increases the “surface area” available for breaches, and interoperability expands the potential scope of breaches. Every node is a potential entry point, and interconnection can spread the damage. What is more, cybercriminals can get the access to the “brain” of the whole IoT system and take control of it.

IoT devices have been compromised to create botnet armies used for distributed denial of service (DDoS) attacks or to attack underlying systems. The limited capability of client devices or sensors and the high frequency of communication between sensors and hubs makes security

---


critical in an IoT solution. Ensuring protection of device identity, user identity, and data must be among the primary checkpoints while architecting the solution.  

3. The IoT Ecosystem and the Context in Which IoT Devices Operate

Many vulnerabilities are the result of the IoT ecosystem in which the IoT devices are implemented. IoT devices are being used in ways they were not designed for. NIST has emphasized that it is important to ask whether the IoT device will be fit for the purpose in that environment, context, and at a specific point in time. NIST has identified three high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices: (1) many IoT devices interact with the physical world in ways conventional IT devices usually do not; (2) they cannot be accessed, managed, or monitored in the same ways conventional IT devices can; and (3) the availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than for conventional IT devices.

This is particularly an issue with the already large installed base of IoT devices. As the DHS/Commerce Botnets report noted: “The scale and diversity of deployed devices make easy fixes difficult and provide additional attack surfaces for malicious activity,” continuing that “Systems may also be vulnerable because support is unavailable. This is often the case for old devices.”

IoT devices and systems create huge amounts of data. Data may be stored locally on IoT devices or transmitted to a cloud platform for processing. Cybersecurity vulnerabilities can put torrents of data at risk. The table below shows for various attack surfaces the types of data that could be compromised or stolen in a hacker attack that exploits vulnerabilities on IoT devices. Addressing this problem is critically important for executives and system owners who must protect their sensitive and confidential data. For example, account data and credentials such as user names and passwords could be stolen, giving criminals access to the IoT device and potentially entry to the entire network. Breach of personally identifiable data (PII) could occur if data is stored on the device or in the IoT unencrypted. PII in a database could be stolen in a SQL injection attack on a website.

---

32. NIST IoT Trust Concerns, supra note 12.
34. See Commerce/DHS Botnets Report, supra note 22, at 16.
**IoT Attack Surfaces > Vulnerabilities > Data at Risk**

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Vulnerability</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Interface</td>
<td>Weak password policy</td>
<td>Credentials</td>
</tr>
<tr>
<td></td>
<td>Lack of account lockout</td>
<td></td>
</tr>
<tr>
<td>Local Data Storage</td>
<td>Data Stored Without Encryption</td>
<td>PII</td>
</tr>
<tr>
<td>Device Firmware</td>
<td>Sent Over HTTP</td>
<td>Credentials</td>
</tr>
<tr>
<td></td>
<td>Hardcoded passwords</td>
<td>Application Data</td>
</tr>
<tr>
<td></td>
<td>Hardcoded encryption keys</td>
<td></td>
</tr>
<tr>
<td>Device Physical Interfaces</td>
<td>Unauthenticated root access</td>
<td>***</td>
</tr>
<tr>
<td>Web Cloud Interface</td>
<td>SQLi</td>
<td>PII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account Data</td>
</tr>
<tr>
<td>Vendor Backend APIs</td>
<td>Permissive API Data Extraction</td>
<td>PII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account Data</td>
</tr>
<tr>
<td>Source: OWASP Attack Surface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Types of Attacks Involving IoT Devices**

While everyone is familiar with the massive data breaches that have made headline news, compromising sensitive and confidential data and putting hundreds of millions of individuals at risk of identity theft and fraud, less attention has been focused on cyberattacks that caused physical damage or bodily injury. Numerous cyberattacks on IoT devices have been reported.

As the use of IoT devices continues to grow, the likelihood of IoT breaches becomes more likely. Information is becoming the primary means of production, and as institutions forge ahead to adopt sweeping changes based on IoT technologies, the risks are legion and not well understood.

The methods of attack used to both steal data and cause damage to ICS and IoT devices are remarkably similar. Thus, the indictments of a Russian national charged in one of the largest known data breach prosecutions and the Russians charged by Special Counsel Robert Mueller are instructive; these cases provide fascinating details about how an IoT and ICS attack may unfold. The FBI-DHS Technical Alert on Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors illustrates the steps involved in hacker attacks in a readily understandable format.

Criminals can use or control IoT devices in a wide variety of ways: to compromise an IoT device; use IoT devices to conduct denial of service attacks; use the IoT device to make money (crypto-mining); take control of IoT devices and the controls of critical infrastructure and cause physical damage; and damage or destroy the IoT devices themselves.


This FBI Alert warns that cyber actors are using compromised IoT devices as proxies\textsuperscript{38} to:

- Send spam e-mails
- Maintain anonymity
- Obfuscate network traffic
- Mask Internet browsing
- Generate click-fraud activities
- Buy, sell, and trade illegal images and goods
- Conduct credential stuffing attacks, which occur when cyber actors use an automated script to test stolen passwords from other data breach incidents on unrelated websites
- Sell or lease IoT botnets to other cyber actors for financial gain

Cyber actors typically compromise devices that have weak authentication, unpatched firmware or other software vulnerabilities, or employ brute force attacks on devices with default usernames and passwords. Many IoT cyber incidents involve exploitation of devices with little or no security, known vulnerabilities, and violations of well-accepted security practices.

Weaponizing IoT Devices to Launch Distributed Denial of Service (DDoS) Attacks.

Intruders have initiated DDoS attacks that flood the victim’s computer with useless information and prevent legitimate users from accessing it. This type of attack will use up all of the available communications bandwidth on a corporate network, making it unavailable to employees.

In an October 2016 DDoS attack, the Mirai botnet scoured the web for IoT devices protected only by factory-default usernames and passwords. It then enlisted those vulnerable IoT devices such as Internet-connected cameras and DVRs to send junk traffic and temporarily overwhelm popular Internet sites, including Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix; these websites could no longer accommodate legitimate visitors or users. The Mirai botnet compromised more than 100,000 CCTV cameras to support DDoS attacks.

When the botnet source code was later released, it revealed 68 username and password pairs used by dozens of IoT products, including Internet routers, security cameras, printers, and digital video recorder (DVRs). In other cases, Internet-connected cameras used as baby monitors were hacked by exploiting default administrative passwords, violating the owners’ privacy.  

More sophisticated botnets have followed. Known as Reaper or IoT Troop, hackers built on portions of Mirai’s code but with a key difference—instead of merely guessing weak passwords, it used numerous known security flaws in the code of insecure IoT devices to exploit a long list of devices. The Reaper malware has pulled together a “grab-bag” of IoT hacking techniques that include nine attacks affecting routers from D-Link, Netgear, and Linksys, as well as Internet-connected surveillance cameras.

The Path Forward—The Security Strategy for Executives, Corporate Boards, and Government Officials Includes Risk-Based Assessment

In light of the number of massive data breaches and well-documented IoT vulnerabilities, the need for all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program is immediate and compelling. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards. While cybersecurity challenges may seem daunting, existing frameworks, standards, and best practices provide a roadmap that public officials and business executives can follow to reduce the risks substantially.

Failure to implement appropriate security can and will lead to significant losses for businesses and owners and operators of critical infrastructure. Business could be temporarily disrupted, or if a sustained attack or breach of security occurs, the continuity of business could be severely affected and, in the worst scenario, organizations could be forced out of business.

41. Id.
42. The American Bar Association (ABA) adopted the following Resolution in 2014:
   The American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.
Ultimately, an organization could face substantial and hard-to-quantify liability if a data breach occurred. Instead of waiting for a breach to take place, proactive measures must be implemented that will significantly lessen the likelihood of a compromise. These actions can potentially lead to reduced likelihood of liability.

**Comprehensive Information Security Program**

A cybersecurity program is comprised of a series of activities. These activities include, for example, governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures, and privacy compliance requirements; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training.⁴³

An effective cybersecurity program requires trained personnel to evaluate the security impact of actual and proposed changes to the system, assess security controls, correlate and analyze security-related information, and provide actionable communication of the security status across all levels of the organization. Administrative, technical, organizational, and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined, implemented, and enforced.

**Cyber response plans.** To minimize the effects of cyber intrusions, it is necessary to plan a response. Organizations must be prepared if a cyberattack or data breach occurs, or if an event interrupts their operations.

**IoT Risk Assessment**

The FBI has emphasized that “[a]s our reliance on IoT becomes an important part of everyday life, being aware of the associated risks is a key part of keeping information and devices secure.”⁴⁴ NIST observed that “[m]any organizations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may affect cybersecurity and privacy risks differently than conventional information technology (IT) devices.”⁴⁵ In the high-risk IoT environment, mitigation of risk is paramount and requires an understanding of the IoT ecosystem because the options may be significantly different for IoT devices than conventional IT devices.

Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed.

Assessing risk requires organizations to identify their threats and vulnerabilities, the harm they may cause the organization, and the likelihood that adverse events arising from those threats and vulnerabilities may actually occur. Threats and risks exist with both physical and virtual assets, and since the two are becoming increasingly interconnected, all aspects of the cybersecurity threat must be addressed. Once organizations are aware of their existing IoT usage and possible future usage, they need to understand how the characteristics of IoT affect

---


⁴⁴. FBI Alert, IoT as Proxies, supra note 45.

⁴⁵. NISTIR 8228 (Draft) Managing IoT Cyber and Privacy Risks, supra note 33.
managing cybersecurity and privacy risks, especially in terms of risk response—accepting, avoiding, mitigating, sharing, or transferring risk.

Every information system is different, including its design and architecture, hardware and software, and technical implementation. Company and government officials must tailor their risk assessments to the data, architecture, and technology of the big data system they own, oversee, or manage.\textsuperscript{46} An IoT risk assessment should focus on specific characteristics and vulnerabilities of the IoT devices being implemented, as well as the environment(s) where the system is deployed.

**Implementing Technology and IoT Devices with Known Vulnerabilities Is Not “Reasonable Security”**

Many data breaches and IoT incidents involve exploitation of known vulnerabilities and violations of well-accepted security practices. Standards of care are beginning to emerge.

Federal law enforcement agencies have brought cases against organizations that failed to employ reasonable security and put sensitive personal data at risk. Businesses have faced regulatory fines and investigations, civil damage actions, administrative proceedings, and criminal indictments.

The Federal Trade Commission (FTC) enforces laws prohibiting unfair and deceptive practices. It has taken enforcement action against companies that suffered a data breach and failed to employ “reasonable security.” In particular, four FTC enforcement actions have been directed to security problems with IoT devices. These cases focused on inadequate security of wireless computer routers and Internet cameras that violated consumers’ privacy \textsuperscript{47} in insecure home routers and “cloud” services that put consumers’ privacy at risk \textsuperscript{48}, video cameras designed to allow consumers to monitor their homes remotely exposed the private lives of hundreds of consumers to public viewing on the Internet \textsuperscript{49}, and Internet-

\begin{footnotesize}
\begin{itemize}
\item[46.] NIST Guides for Conducting a Risk Assessment—NIST published the *Framework for Improving Critical Infrastructure Cybersecurity*, a set of industry standards and best practices to help organizations manage cybersecurity risks as part of their risk management processes, https://www.nist.gov/cyberframework. NISTIR 8228 (draft) *Managing (IoT) Cybersecurity and Privacy Risks* will help organizations understand and manage cybersecurity and privacy risks associated with IoT devices throughout their life cycles. The NIST Guide for Conducting Risk Assessments, Spec Pub 800-30 Rev. 1 (Sept. 2012), provides a step-by-step process for organizations on how to (1) prepare for risk assessments; (2) conduct risk assessments; (3) communicate risk assessment results to key organizational personnel; and (4) maintain the risk assessments over time. See IoT Security Maturity Model: Description and Intended Use, Industrial Internet Consortium, IIC:PUB:IN15:V1.0:PB:20180409, (Apr. 9, 2018), https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf. “As an informed understanding of the risks and threats an organization faces is the foundation of choosing and implementing appropriate security controls, the model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.”
\end{itemize}
\end{footnotesize}
connected toys that collected personal information about children without obtaining parental consent (VTech Electronics).\(^{50}\)

The FTC guidance, *Start with Security, A Guide for Business*, analyzes lessons learned from the more than 50 law enforcement actions the FTC has announced, and describes the security lapses that led to those cases. The penalties for failing to employ reasonable security to protect personal data are onerous, ranging from substantial fines to third-party audits spanning the next 20 years.

In the first state attorney general action against a wireless security company for failing to implement adequate security in its IoT devices, the New York State Attorney General recently settled with wireless lock company Safetech, manufacturer of a smart electronic padlock.\(^{51}\) Safetech did not encrypt its users’ passwords when transmitted from a smartphone to the locks. Moreover, it did not force users to reset default passwords, which could be discovered easily by brute-force attacks, leaving consumers susceptible to hacking and physical theft.

**Strengthening Security**

Even as warnings about IoT cybersecurity risks continue to be issued by the defense and intelligence community, policy makers, and cybersecurity experts, development and implementation of the IoT continues to explode.

- There are no comprehensive laws or regulations addressing the security of IoT devices.
- There is no oversight on the licensing of IoT device manufacturers.
- There are no governing authorities evaluating the security of IoT devices.

One legislative proposal, *The IoT Cybersecurity Improvement Act of 2017*, S. 1691, is designed to address the market failure by establishing minimum security requirements for federal procurements of connected devices.\(^{52}\)

**Security by Design.** In light of the documented vulnerabilities in the IoT, companies and government agencies must take immediate action to strengthen their security posture. To properly support an organization’s risk management program, security must be incorporated into the architecture and design of the organization’s information systems and supporting information technology assets.\(^{53}\)

This includes constant monitoring of systems, security status, and risks, often referred to as continuous monitoring. It is essential to protect against the broad range of serious threats to information systems.\(^{54}\) Robust continuous monitoring will provide executives and security


\(^{52}\) Introduced on Aug. 1, 2017, 115th Congress (2017-18).


\(^{54}\) [The SANS CIS Critical Security Controls: Guidelines provide guidance to maximize the impact of government and private sector security efforts, and identify 20 critical priority controls, most of which can be continuously monitored. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, v. 7.0, [https://www.sans.org/critical-security-controls/guidelines](https://www.sans.org/critical-security-controls/guidelines) (the website provides a wealth of valuable information about the leading information security methodologies and how they relate to each other).](https://www.sans.org/critical-security-controls/guidelines)
professionals with the information necessary to make cost-effective, risk-based decisions. Artificial intelligence (AI) is providing the capability to detect anomalies and thwart hacker attacks before damage is done or to enable an effective response quickly. Potential threats must be investigated, and targeted attacks can be detected in advance or addressed as they occur, enabling a highly proactive security posture.

**Addressing IoT risk through the procurement process.** As part of a comprehensive security program, the procurement process can be used to strengthen the security posture of organizations and their third-party business partners. The ABA Vendor Contracting Cybersecurity Checklist frames the issues that contracting parties should consider consistent with common principles for managing cyber risk.55

When contracting for products and services, organizations can specify cybersecurity requirements that third-party vendors must meet. Including cybersecurity in the procurement process can ensure that those purchasing and supplying delivery systems consider cybersecurity beginning with the design phase of system development. This will further ensure that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation, and support phases of the product life cycle, improving overall reliability and reducing cyber risks. Contract representations and warranties can ensure that important cybersecurity conditions are agreed to and will be followed by third-party vendors.

Hackers and foreign governments have demonstrated the will, the knowledge, the capacity, and the resources to successfully penetrate information systems and steal the most sensitive data held by private sector and government organizations. The threat is imminent, and immediate action is required to assess the IoT and other risks and implement appropriate security controls to protect the confidentiality, integrity, and availability of data and systems.

---

OWASP Principles of IoT Security

Developed as part of the OWASP Internet of Things Project, these Principles were designed to enable manufacturers, developers, and consumers in any context to make better security decisions when building, deploying, or assessing IoT technologies.

1. Assume a Hostile Edge
   Edge components are likely to fall into adversarial hands. Assume attackers will have physical access to edge components and can manipulate them, move them to hostile networks, and control resources such as DNS, DHCP, and Internet routing.

2. Test for Scale
   The volume of IoT means that every design and security consideration must also take into account scale. Simple bootstrapping into an ecosystem can create a self-denial of service condition at IoT scale. Security countermeasures must perform at volume.

3. Internet of Lies
   Automated systems are extremely capable of presenting misinformation in convincing formats. IoT systems should always verify data from the edge in order to prevent autonomous misinformation from tainting a system.

4. Exploit Autonomy
   Automated systems are capable of complex, monotonous, and tedious operations that human users would never tolerate. IoT systems should seek to exploit this advantage for security.

5. Expect Isolation
   The advantage of autonomy should also extend to situations where a component is isolated. Security countermeasures must never degrade in the absence of connectivity.

6. Protect Uniformly
   Data encryption only protects encrypted pathways. Data that is transmitted over an encrypted link is still exposed at any point it is unencrypted, such as prior to encryption, after decryption, and along any communications pathways that do not enforce encryption. Careful consideration must be given to full data life cycle to ensure that encryption is applied uniformly and appropriately to guarantee protections. Encryption is not total—be aware that metadata about encrypted data might also provide valuable information to attackers.

7. Encryption Is Tricky
   It is very easy for developers to make mistakes when applying encryption. Using encryption but failing to validate certificates, failing to validate intermediate certificates, failing to encrypt traffic with a strong key, using a uniform seed, or exposing private key material are all common pitfalls when deploying encryption. Ensure a thorough review of any encryption capability to avoid these mistakes.

8. System Hardening
   Be sure that IoT components are stripped down to the minimum viable feature set to reduce attack surface. Unused ports and protocols should be disabled, and unnecessary supporting software should be uninstalled or turned off. Be sure to track third-party components and update them where possible.
9. Limit What You Can
To the extent possible, limit access based on acceptable use criteria. There’s no advantage in exposing a sensor interface to the entire Internet if there’s no good case for a remote user in a hostile country. Limit access to white lists of rules that make sense.

10. Life Cycle Support
IoT systems should be able to quickly onboard new components, but should also be capable of re-credentialing existing components, and deprovisioning components for a full device life cycle. This capability should include all components in the ecosystem, from devices to users.

11. Data in Aggregate Is Unpredictable
IoT systems are capable of collecting vast quantities of data that may seem innocuous at first, but complex data analysis may reveal very sensitive patterns or information hidden in data. IoT systems must prepare for the data stewardship responsibilities of unexpected information sensitivity that may only be revealed after an ecosystem is deployed.

12. Plan for the Worst
IoT systems should have capabilities to respond to compromises, hostile participants, malware, or other adverse events. There should be features in place to re-issue credentials, exclude participants, distribute security patches and updates, and so on, before they are ever necessary.

13. The Long Haul
IoT system designers must recognize the extended lifespan of devices will require forward compatible security features. IoT ecosystems must be capable of aging in place and still addressing evolving security concerns. New encryption, advances in protocols, new attack methods and techniques, and changing topology all necessitate that IoT systems be capable of addressing emerging security concerns for years after they are deployed.

14. Attackers Target Weakness
Ensure that security controls are equivalent across interfaces in an ecosystem. Attackers will identify the weakest component and attempt to exploit it. Mobile interfaces, hidden APIs, or resource-constrained environments must enforce security in the same way as more robust or feature-rich interfaces. Using multifactor authentication for a web interface is useless if a mobile application allows access to the same APIs with a four-digit PIN.

15. Transitive Ownership
IoT components are often sold or transferred during their lifespan. Plan for this eventuality and be sure IoT systems can protect and isolate data to enable safe transfer of ownership, even if a component is sold or transferred to a competitor or attacker.

16. N:N Authentication
Realize that IoT does not follow a traditional 1:1 model of users to applications. Each component may have more than one user and a user may interact with multiple components. Several users might access different data or capabilities on a single device, and one user might have varying rights to multiple devices. Multiple devices may need to broker permissions on behalf of a single user account, and so on. Be sure the IoT system can handle these complex trust and authentication schemes.

Source: https://www.owasp.org/index.php/Principles_of_IoT_Security