Considerations for Managing IoT Cybersecurity & Privacy Risk

NIST Cybersecurity for IoT Program

The NIST's Cybersecurity for the Internet of Things (IoT) Program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the Program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Introduction

The NIST Cybersecurity for IoT Program is drafting guidance on managing IoT cybersecurity and privacy risks within federal information systems and is engaging with stakeholders to develop this publication. The guidance is intended to have broad applicability for common cybersecurity and privacy risks for IoT and to introduce practical risk management considerations for IoT product selection, deployment, and operation. The approach is intended to be flexible, performance-based, and cost-effective, and it may be voluntarily used by diverse stakeholders. This document provides background information on NIST's approach for generating the IoT cybersecurity and privacy guidance, and is intended to encourage discussion and feedback.

NIST has identified five principles that inform the Cybersecurity for IoT Program's approach to developing guidance for IoT cybersecurity and privacy risk management.

- **Risk-Based Understanding.** IoT capabilities, behaviors, deployment environments, and other characteristics can affect cybersecurity risk. Our approach to managing this risk is rooted in an understanding of how IoT can affect it.
- **Ecosystem of Things.** Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.
- **Outcome-Based Approach.** We embrace the Cybersecurity Framework's outcome-based approach. We specify desired cybersecurity outcomes, not necessarily how to achieve those outcomes, which allows organizations to choose the best solution for each IoT device and/or their enterprise environment.
- **No One Size Fits All.** Each organization has its own risk tolerance and mission needs, and no one set of controls will address the wide range of cross-industry and cross-vertical needs and use cases. There is no one-size-fits-all approach to managing IoT cybersecurity risk.
- **Stakeholder-Engaged Processes.** NIST works with diverse stakeholders to advance IoT cybersecurity. This includes collaborating with stakeholders to provide the necessary tools, guidance, standards, and resources.

The guidance will be introductory and non-comprehensive, focusing on the aspects of cybersecurity and privacy risk where guidance can be most beneficial. As some guidance already exists on aspects of IoT cybersecurity and privacy, NIST intends to leverage existing guidance and best practices where possible, and may augment it by tailoring traditional IT material for IoT in other cases.

Listed below are the specific areas in which NIST seeks comments. NIST is looking forward to engaging with stakeholders in person and virtually. For those who cannot engage in-person, we encourage sending feedback to IoTsecurity@nist.gov.

Identifying IoT-Specific Characteristics and Considerations

IoT technologies have been evolving over time: they are the product of an evolution from both the worlds of information technology (IT) and operational technology (OT). Many IoT systems are the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances. IoT can provide computing functionality and network connectivity for equipment that previously lacked these. IoT systems generally face the same types of cybersecurity and privacy risks as traditional IT systems, though their prevalence and severity often differ.

Question

What IoT characteristics may impact managing cybersecurity and privacy risks?

The guidance will cover major considerations that may affect the management of cybersecurity and privacy risk for IoT systems. These are referred to as *risk considerations*. **Note that while each IoT system in its deployment environment will have its own set of risk considerations, there are common risk considerations that can be stated at a more general level to help guide more granular, specific risk management.**

1. **Diversity of IoT Systems.** IoT systems can vary from incredibly small and simple, to incredibly large and complex, such as a system fully integrated within the structure of a campus of buildings. There is also extensive variety in IoT system software: firmware, operating systems, and applications. Each type and version of firmware, operating system, and application offers a unique combination of capabilities.

   In terms of software communication, IoT systems tend to use the same forms of networking as traditional IT systems; however, at the application layer, IoT systems do not have commonly used standards expressing data, issuing commands, or otherwise interoperating. The diversity of IoT systems means there is a great deal more variability in the risks involving each deployed IoT system and the options for addressing those risks.

2. **Managing and Maintaining IoT Systems.** Many organizations are using a large number of IoT systems, but are not necessarily aware that these are considered IoT systems. This is important because organizations may not be aware that these systems are introducing new cybersecurity and privacy risks. Traditional IT systems usually support hardware and software visibility, access, and control. For example, a system administrator can directly access a typical IT system's operating system and reconfigure it to disable unneeded hardware and software capabilities.

   Question

   What is a realistic expectation for controls built-in to the device? What is realistic for controls outside the device?

   In contrast, many IoT systems are inflexible and opaque—often, these are referred to as "black boxes". Possible implications include:

- IoT system hardware may not be serviceable, meaning that it cannot be repaired, customized, or replaced.
- Administrators may not be able to manage and maintain the IoT system's firmware, operating systems, and applications. Unavailable functions may include the ability to acquire, verify the integrity of, configure, store, retrieve, execute, terminate, remove, and replace or update software. Note that this includes the inability to install additional software, such as cybersecurity and privacy controls.
- IoT systems may not be able to log their operations, including cybersecurity and privacy events.
- System administrators may have little or no visibility into the current state and composition of IoT systems.

The collection of data that is consistent with an IoT system's primary purpose – i.e. acquiring data at a traffic light – may have unintended consequences that go largely undetected, such as the persistent monitoring of local residents. Further, IoT systems brought into an organization in support of a mission objective – for example, provision of health care – may not be registered via the normal IT registration process.

On the other hand, IoT systems often enable remote access to physical systems. Such physical systems may previously have only been at risk from people with direct physical access. Vendors, manufacturers, and other third parties may have remote access to IoT systems for management, monitoring, maintenance, and troubleshooting purposes.

3. **IoT System Complexity.** Some IoT systems can be considered "systems of systems," with a high degree of complexity as one IoT system contains many others; some of these may, in turn, be composed of additional IoT systems. Some IoT systems are dynamic, meaning that their composition changes over time. For example, an IoT system may have many sensors, with sensors frequently being added to and removed from the system.

   The more complex an IoT system is, the more likely it is that system administrators will lack visibility, access, and/or control over one or more of its components, and that the IoT system will have a wider range of capabilities, which increases its exposure to threats and its number of potential vulnerabilities.

4. **Built-In Cybersecurity and Privacy Controls.** Many IoT systems lack the range of built-in cybersecurity and privacy controls usually present in traditional IT systems. These IoT systems are not designed to ward off logical and physical attacks. Examples of how IoT system controls often differ from traditional IT system controls include:
   - Assumption that anyone with physical access to the IoT system is authorized to have logical access.
   - Assumption that only authorized personnel and systems will attempt to logically access an IoT system. Strong authentication and authorization mechanisms are often unavailable.
   - Assumption that the IoT system's communications channels can be trusted, including those used for remote access. Communication eavesdropping, interception, manipulation, impersonation, and other forms of attack are assumed not to occur.
   - Patches and other updates to correct vulnerabilities and other problems with software may not be available.
   - The ability to change the cybersecurity and privacy-related software configuration may not be available or may not offer the capabilities a particular organization wants.

- Some IoT systems may not be designed to identify suspicious or malicious inputs and outputs (data values).

Question

How else might IoT introduce additional cybersecurity and privacy risks?

5. **Potential Consequences of Compromise.** For IoT systems, the ability to make changes to physical systems and thus affect the physical world can greatly expand the consequences of a system compromise. Another noteworthy consequence is compromised IoT systems being used in botnets to perform distributed denial of service (DDoS) attacks and other malicious activity. Traditional IT systems are often used in botnets too, but IoT systems may be more attractive to attackers because their compromises may be less likely to be detected.

   The ubiquity of IoT sensors and devices in public and private environments can contribute to the aggregation and analysis of enormous amounts of data about individuals. These activities may curtail individuals' autonomy or lead to information being revealed that individuals didn't anticipate or want – and may actually be well beyond the originally intended scope of the IoT system's operation.

Risk Management Considerations

NIST is looking at defining key organizational-level considerations to address the identified IoT cybersecurity and privacy risks, grouped into three areas: governance, risk management, and asset management. For each group, the guidance will explain how the risk aspects may generally need to be taken into account within the context of the relevant NIST Cybersecurity Framework (CSF) categories.

Question

Did we miss any considerations? How can these risk considerations be integrated into a risk management approach?

Governance Considerations

Organizational objectives and priorities should be set at the governance level, including considerations for risk tolerance. These objectives and priorities serve as the basis for an organization's cybersecurity and privacy policies. The definition and scope of IoT for cybersecurity and privacy purposes should be clearly defined in an organizations's policy to avoid confusion and ambiguity. This should be complemented by accordingly updating the organization's cybersecurity and privacy policies, procedures, processes, and roles and responsibilities to encompass IoT, including addressing any legal or regulatory requirements applicable to IoT.

A primary consideration is how the organization will define or scope IoT for cybersecurity and privacy purposes, so that it is clear which systems are to comply with IoT policies, laws, and regulations. Organizations may need to specify examples, taxonomies, or other ways of better indicating which systems in their sector and environment are considered IoT and how different types of IoT systems should be treated.

An organization should:

- Know the main types of IoT devices and sensors and what each type does to collect, store, and communicate data;
- Inform itself of the main risks and benefits - for themselves and all stakeholders - of the different types of IoT devices and sensors; and

- Assure that an appropriate entity within the organization has people, processes, and policies in place to manage the IoT lifecycle (from sourcing and acquisition to disposal and destruction), as well as the consequences of any failure during the lifecycle.

Risk Management Considerations

NIST is considering advising that organizations should adjust their existing risk management strategies and processes, including risk assessment and supply chain risk management processes, to take IoT into account. There is no one-size-fits-all method for managing IoT cybersecurity and privacy risk. Many IoT systems have unique combinations of characteristics, which affects risk – further, many IoT systems do not support all the cybersecurity and privacy controls typically offered by traditional IT systems.

Another important distinction for IoT systems and risk is the need to take into consideration the specific environment the IoT systems are implemented into, and not just evaluate the risks for the IoT systems in isolation. For example, attaching an IoT actuator to one physical system may cause an entirely different level of risk than attaching the same actuator to another physical system.

Adding IoT considerations to existing cybersecurity and privacy risk management programs involves numerous activities, including the following:

- Identifying IoT system capabilities and characteristics;
- Assessing IoT system risk; and
- Determining how to respond to that risk by accepting, avoiding, mitigating, sharing, or transferring it.

Question

What use cases would be most helpful for illustrating and understanding IoT risk management considerations?

NIST proposes that organizations in early stages of addressing cybersecurity and privacy risk management should focus on addressing what makes IoT different from other technologies, as discussed with the risk considerations.

Asset Management Considerations

For the purposes of the guidance, asset management refers to performing typical asset management functions for all IoT systems, such as uniquely identifying each system. Such asset management presents a challenge because organizations have to figure out how to track a number of heterogeneous devices that may not be designed to have unique identifiers or participate in automated asset management processes.

NIST proposes that IoT systems and their discrete components should be added to an organization's asset management practices. Doing so is dependent on the organization having a clear definition of IoT so it can recognize IoT systems and components, both before and after acquisition, and building and maintaining an inventory of IoT systems and components that captures their relevant capabilities and characteristics. Organizations may find it helpful to define IoT capabilities and characteristics in order to promote consistent, well-structured information gathering regarding IoT systems and components.

Relevant Cybersecurity Outcomes

Mitigation options are often considerably different for IoT components and systems than traditional IT devices and systems because many IoT components cannot support the range of cybersecurity and privacy controls typically built into traditional IT devices. Alternatives to controls within IoT components

include network-based controls, physical security controls, and control services (e.g., cloud-based services from a third-party provider). Compared to traditional IT devices and systems, which tend to use similar sets of controls, there is a great deal of variability in the options for securing each IoT component and system.

Potential Issues with Achieving Cybersecurity and Privacy Outcomes

NIST plans that the guidance will discuss potential issues with achieving cybersecurity and privacy outcomes for IoT components and systems, and provide information on how these issues can potentially be addressed. As appropriate, the section will indicate the relative importance of each outcome, as well as the relative difficulty in achieving it for IoT.

Question

What cybersecurity and privacy outcomes would be hardest to achieve for IoT systems?

Contact Information

The NIST Cybersecurity for IoT Program will continue engaging with stakeholders as this guidance is developed. Updates on Program activities and collaboration opportunities are available on the NIST Cybersecurity for IoT Program website.