3 Identifying Device Cybersecurity Requirements for IoT Devices

This section provides guidance to organizations in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device.

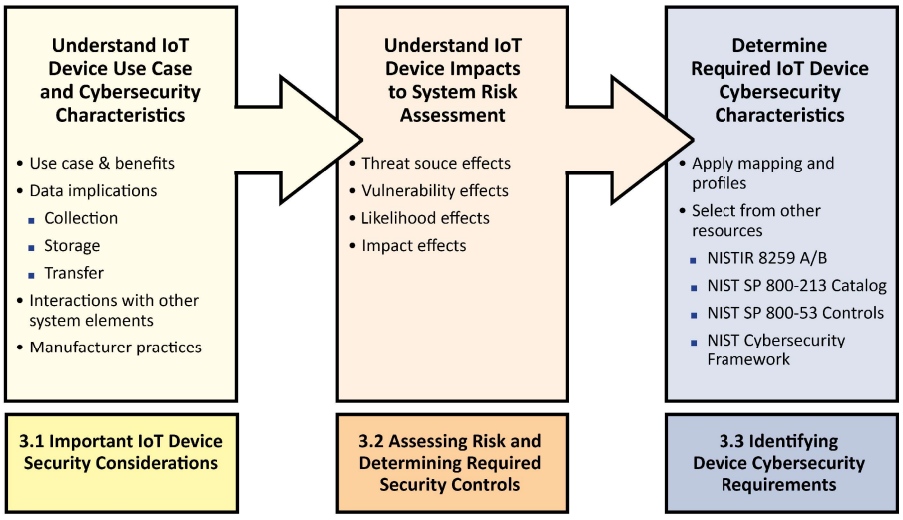

Figure 4: Organizations Can Use this Section to Identify IoT Device Cybersecurity Requirements

Section 3.1 provides an overview of important IoT device cybersecurity considerations. The questions in section 3.1 help organizations contemplate the IoT device's use case, providing a foundational understanding of how the IoT device might impact risk to the system. Section 3.2 discusses how an understanding of the IoT device and its use case can impact the system's risk assessment and the subsequent allocation of security controls to the information system. Section 3.3 focuses on determining applicable device cybersecurity requirements based on the risk assessment and controls allocation from Section 3.2. The section presents sources of device cybersecurity requirements. Organizations may reference these sources when selecting applicable IoT device cybersecurity requirements.

Each organization should develop a process for identifying and articulating IoT device cybersecurity requirements that aligns with their existing policies and procedures (e.g., acquisitions, security, system administration). The guidance presented in this publication provides a starting point for organizations—as well as additional resources organizations can use—in identifying IoT device cybersecurity requirements. The steps described in this section happen before an IoT device is purchased and/or integrated. At this stage, the IoT device itself may not be in the organization's possession, which may result in some considerations, particularly those related to *how* risks can be mitigated, not being entirely known. Information about additional IoT device and support limitations should be identified through further engagement with the available producers and vendors.

3.1 IoT Device Cybersecurity Considerations

The decision to integrate an IoT device into a system may occur for a variety of reasons (e.g., to achieve business objectives, further technical advancements, provide administrative support). The reason the IoT device is being acquired will influence its use case. For one organization, IoT sensors may be sought to help remotely monitor environmental conditions; another organization may acquire IoT office equipment to increase productivity; still other organizations may seek to leverage IoT technology in the delivery of services to citizens.

Organizations should fully understand the specific use case for an IoT device since the use case could impact risk to the system and organization. The following questions can help organizations think through some of the common considerations for IoT devices, but this list is not exhaustive. The answers to these and other questions can ultimately help organizations assess risk and identify IoT device cybersecurity requirements for their use case(s). Accurately and completely answering these questions for many IoT devices will require consultation with IT personnel within the organization.

1. **What is the benefit of the IoT device and how will it be utilized?** Organizations can help ensure that device cybersecurity requirements receive proper consideration by establishing an explicit benefit for integrating the IoT device and understanding how the IoT device will be used. For example, if the IoT device is replacing equipment that did not previously connect to the system, organizations should holistically consider the benefit of the connection to the system compared to the potential risks. It may be the case that a connected motion sensor can detect potential intruders but may also introduce security vulnerabilities that may outweigh the proposed benefits.

2. **What data is collected?** IoT devices can collect many kinds of data, some innocuous, others of concern to organizations. Any data collected could be a risk to the organization. All data collected or reported by IoT devices should be understood, but three main types of data may be of concern:

    a. *Personal data:* Many IoT devices can sense or collect data of, from, or about people, which can constitute personal data and represent privacy sensitive data.

    b. *Confidential organizational/Federal government data:* The IoT device may collect restricted or confidential data, which could influence its risk level. For example, IoT devices may help create or have access to organization-restricted test results, analysis materials, or device prototypes that require special protection.

    c. *Environmental data:* Many IoT devices can sense and/or collect data of, from, or about the physical environment. Organizations should consider whether the collection of environmental data poses any risk to individuals or the organizational mission.

3. **In what technologies will the data be stored and how will it be transmitted?** Many IoT devices maintain connections to cloud services and mobile/web applications that are central to the device's functionality. IoT devices can also connect to additional external services, which may be provided and hosted by a number of third parties. Organizations

should consider where the IoT device might store data —in the device, the manufacturer's network, a manufacturer-contracted entity's network (e.g., cloud service provider[14]), etc. In addition, organizations should consider how the data will be secured in transit as connections to external services and third parties are made and used.

4. **In what geographic areas will the data be shared and/or stored?** The architecture that supports IoT devices is increasingly global. Organizations should consider where data from prospective IoT devices will be transmitted and stored to ensure applicable security requirements are met. An IoT device may connect to and transmit data to systems in many diverse areas, including other cities, states, and countries. These connections may change over time due to the dynamic nature of IoT systems.

5. **With what other third parties will data from, or about, the IoT devices be shared and/or stored?** In some cases, an IoT device will only exchange data with the owner and manufacturer-owned and operated systems. In other instances, the IoT device will share data with third parties. For example, many manufacturers use cloud storage and services from other providers to support their IoT devices' back end infrastructure.

After understanding the contextual considerations about the IoT device discussed above, organizations should consider the following questions about how the IoT device will interact with the organization and information system:

1. **Might the device interfere with other aspects of operations or system functionality?** Unlike conventional IT equipment, IoT devices are more likely to interact with the physical world through sensing and/or actuating. This interaction increases the possibility that an IoT device could affect operations and the environment (e.g., alarms, thermostats, environmental controls, heating elements) as well as the security posture of the system. For example:

    a. *Could the IoT device introduce privacy or safety risks for people?* IoT devices could collect and share sensitive data about people, including, but not limited to, audio and video data. An IoT device can also interact with the physical world (e.g., IoT vehicle) or might be intended to protect human safety (e.g., an IoT smoke alarm), potentially posing safety risks. Considering if an IoT device may introduce privacy or safety risks is critical to planning for risk mitigation.

    b. *Could the IoT device interfere with system reliability or resiliency?* The diversity of IoT device use cases also creates the possibility that the IoT device's expected operational environment may vary from where it is actually deployed. In such an instance, the IoT device might negatively interact with other system elements or

[14] As a reminder to organizations, if an IoT device uses cloud computing technologies, organizations need to refer to NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* [800-144] for additional guidance on cloud security considerations, as well as SPs 800-145, *The NIST Definition of Cloud Computing* [800-145] and 800-146, *Cloud Computing Synopsis and Recommendations* [800-146] for additional guidance on cloud computing and storage technologies. Finally, NIST SP 500-292, *NIST Cloud Computing Reference Architecture* [500-292] may be a useful additional resource for organizations.

operational systems if not properly planned for. For example, an IoT device may go offline to apply a software update. This behavior is acceptable in many circumstances but may impact system reliability if the offline device hurts operations in other parts of the system. Likewise, IoT devices may not be as digitally and physically resilient as their IT or OT counterparts since IoT devices must sometimes attempt to deliver both IT and OT functionality. This can lead to inherent practicality and cost constraints that result in a focus or prioritization of some features or aspects of functionality over others (e.g., safety over cybersecurity) in the design of the IoT device.

2. **Would the IoT device introduce unacceptable risks to the organization or result in non-compliance with cybersecurity requirements?** Some IoT devices might be unable to support the organization's current security controls as they are implemented due to their design, requiring organizations to implement compensating controls (e.g., additional organizational controls or alternative technical controls) to manage risk. Organizations should consider the proposed IoT device use case and whether the risk introduced is acceptable. In some use cases, the IoT device might provide an additional point of access to the system from which an attacker could pivot to other system elements or networks.

3. **Does the IoT device have known security and/or privacy vulnerabilities?** Like all connected products, IoT devices attract attention from security professionals and researchers who identify security and/or privacy concerns. Manufacturers also commonly publish similar information concerning their devices. Understanding known vulnerabilities can inform an organization's acquisition, risk assessment, and possible integration of an IoT device. For example, if known vulnerabilities exist that the manufacturer cannot mitigate, organizations would have to identify and address risks introduced by the IoT device through other means.

As discussed extensively in NISTIR 8228, IoT devices can have significantly different feature sets compared to conventional IT devices. These differences in device capabilities and support for security controls can create challenges for organizations if not adequately planned for, especially if the capabilities diverge significantly from what is expected. Organizations should refer to NISTIR 8228 and consider if the IoT device will create any security and privacy challenges for the information system and organization. One common way challenges arise is when an IoT device does not fully support *key device cybersecurity requirements*. Organizations may reduce these challenges by considering important aspects of how the IoT device should connect and function to ensure the device conforms with expectations, and, thus, may define, inform, or otherwise impact key device cybersecurity requirements. In particular, organizations should consider:

1. **What organization-specific information is important to defining key device cybersecurity requirements?** Organizations often invest in specific solutions or implementations that would be the preferred support for various security controls. Identifying this kind of organizational information can help guide a purchase and reduce conflicts in applying security controls if the IoT device is integrated into a system. Since IoT devices can interact with an organization in many ways (e.g., via the network, but also in a physical way), many different kinds of organization-specific information can

impact what is acceptable to an organization, which mitigations are practical and appropriate, and the determination of device cybersecurity requirements. Some examples of organization-specific information include, but are not limited to:

1. *Does the organization require Personal Identity Verification (PIV) card-based authentication or does it allow password-based authentication in limited circumstances?* Support for critical cybersecurity technologies and operations that are used to implement security controls may be important for an organization in deciding which, if any, IoT device to use for a particular purpose. Organizations should note that some of this support, such as support for PIV may be related to standards and guidelines like the Federal Information Processing Standards (FIPS)[15].

2. *Does the organization purchase products from particular manufacturers or 3rd parties?* Such situations may limit the IoT devices readily available to the organization. This may, in turn, limit availability of IoT devices that best support the needs and goals of the organization.

3. *Are there any environmental considerations (e.g., exposure to the elements, human presence, sensitive data that could be collected) in the environment of operation?* Environmental considerations can help guide device cybersecurity requirements, particularly around physical protections. For example, if an IoT device is meant to be placed outdoors, a durable housing may be needed to withstand excessive heat, cold, and moisture while still providing data availability and integrity.

2. **Does the IoT device lack key device cybersecurity requirements?** Key device cybersecurity requirements are those the organization has determined that the IoT device must possess in order for the device to be integrated in the system and make external connections to other systems or the Internet. Lack of key device cybersecurity requirements indicates that the IoT device cannot support existing information system controls, which subsequently introduces unacceptable levels of risk[16]. To support information system security controls, the organization may need to consider if other system elements (e.g., a gateway, hub, cloud service) can provide the capabilities missing from the IoT device but should keep in mind those *key* device cybersecurity requirements

[15] NIST's current FIPS can be found at https://www.nist.gov/itl/current-fips. Relatedly, organizations should be aware of the Cryptographic Module Validation Program (CMVP) when considering appropriate cryptographic modules for IoT devices. More information about the CMVP can be found on the project webpage at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

[16] Since key device cybersecurity requirements are tied to a "unacceptable" level of risk when omitted, their identification will be related to both the IoT device and its use case, but also the organization and, among other considerations, its risk appetite (i.e., the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value [IR8286]). A higher risk appetite when using the IoT device may lead to fewer key device cybersecurity requirements since, at a minimum the organization is more willing to omit support for a security control despite the risk it introduces. An organization with a lower risk appetite may be less willing to accept risks left unmitigated by the lack of device cybersecurity requirements and thus not willing to omit the requirement if lacking from an IoT device. Proper understanding of risk appetite and other cybersecurity considerations will require input from IT security personnel.

that cannot be provided elsewhere, otherwise compensated for, or omitted without introducing unacceptable risk to the organization.

3. **Will the implementation or maturity of device cybersecurity capabilities and/or non-technical supporting capabilities fail to satisfy key device cybersecurity requirements?** Some IoT devices may completely lack key device cybersecurity requirements, potentially making the IoT device unusable by the organization. Other IoT devices may provide device cybersecurity requirements but not in the manner expected by the organization. For example, an IoT device may have a unique device identifier, but it may not be in a format the organization uses with other equipment. The organization will need to plan for how this identifier will be incorporated into its asset management processes. When an IoT device's cybersecurity capabilities lack maturity, the task of securing the device may be much more difficult. For example, an IoT device may encrypt data, but use a deprecated encryption module due to device resource constraints. In this case, the organization may need to apply significant compensating controls.

4. **What are the physical, logical access, network, and other requirements of the IoT device and how do they relate to key device cybersecurity requirements?** An understanding of how the IoT device will interact with the digital and physical worlds is important to understanding whether the device should be used by the organization and, if so, the cybersecurity risks and corresponding mitigations that are practical, possible, and appropriate. For example, knowing the endpoints (both internet domains and local devices) the IoT device must connect to can help an organization ensure all connections the device will make (and the logical access via those endpoints) are acceptable within the organization's security policy. Physical requirements, such as the need to access the device for maintenance or diagnostics may conflict with how some devices are deployed (e.g., if they must be placed in an inaccessible location making physical maintenance difficult or impossible).

In addition to the specifics of the device and how it works, organizations should also consider the practices of the manufacturer in the development and on-going support of the IoT device. Secure development, supply chain, and maintenance (e.g., vulnerability management and patching) practices can help mitigate the introduction of vulnerabilities and possibly reduce likelihood and/or impact of adverse events. Consider:

1. **Does the manufacturer use secure development[17] and supply chain practices[18] to support their operations?** The use of secure development and supply chain practices in the manufacture of IoT devices will not solve all cybersecurity issues but will help reduce

[17] Additional information and guidance on secure development as it relates to software can be found in NIST's *Secure Software Development Framework* (SSDF) [SSDF].

[18] More guidance for organizations in "identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage information and communication technology (ICT) supply chain risks" can be found in SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [800-161].

cybersecurity issues with IoT devices and provide additional assurances to organizations of the cybersecurity posture of the manufacturer and IoT device.

2. **How robust and mature are the manufacturer's vulnerability disclosure and remediation practices?** Organizations should consider whether the manufacturer has an established vulnerability disclosure program with a history of timely updates and should look to these disclosures to inform themselves of known vulnerabilities.

3. **What are the expectations around delivery of software updates in response to discovered vulnerabilities?** Since removal of vulnerabilities is important to maintaining an organization's risk posture, understanding expectations around update delivery can avoid the introduction and exploitation of vulnerabilities by allowing organizations to adequately plan for the delivery (or absence) of an update to apply.

The questions in this section assist organizations in understanding key aspects of the use case of the proposed IoT device as well as the risk that could be introduced by incorporating it into an existing system. The list of questions is not exhaustive.

3.2 Assessing Risk and Determining Required Security Controls

Organizations should remember that the incorporation of an IoT device can alter the information system's risk assessment. Any change in the risk assessment may require the allocation of additional security controls or the introduction of compensating controls to reduce risk to acceptable levels. Section 3.1 provides a starting point for considerations about IoT devices that may help organizations determine the risk associated with an IoT device. Organizations assess risk to IoT devices using the organization-defined approach based on guidance in NIST SP 800-30 but supplement the risk model for IoT using the guidance in this section.

Figure 5 below illustrates how to update a risk model specifically for an IoT device, closely aligned and adapted from the risk model with key risk factors identified in SP 800-30 Rev. 1 [800-30]. This updated risk model would then be used with other information to assess risk to the system, including the IoT device as an element.

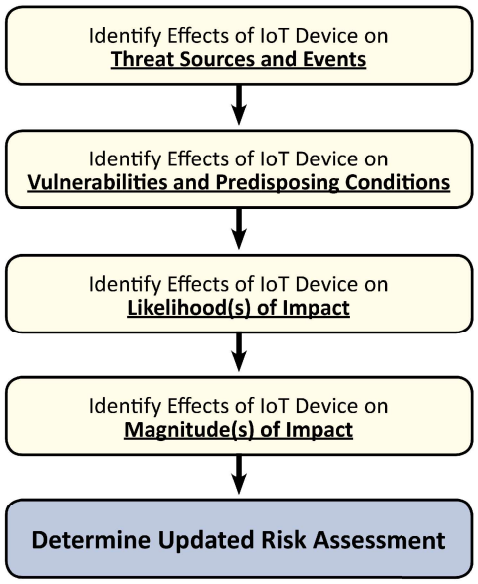

Figure 5: Steps to Updating a Risk Model and Risk Assessment using New Information about an IoT Device.

Ideally the inclusion of an IoT device as a new system element will not significantly alter the information system's risk assessment. Nevertheless, as part of the risk management process, organizations must assess the level of risk introduced by the IoT device. The following discussion of threats, vulnerabilities, likelihood, and impact shall be considered by an organization as part of the risk model of an IoT device to be incorporated into a system and the subsequent updated risk assessment of the system.

3.2.1 Effects on Threat Sources and Events

How does the IoT device affect the threat sources and events that must be considered as part of a risk assessment? An IoT device may bring new features and functions to a system but may also attract new threat sources (i.e., situation, intent, or method that may trigger a vulnerability) and present new threat events (i.e., observable occurrences within the system that causes undesirable consequences or impacts) that must be considered as part of a system risk assessment. For example, IoT devices may introduce new safety- and/or mission-critical considerations to a system. These considerations could make the system more attractive to attacks that previously would not apply (e.g., the system may become a ransomware target) and/or create events not previously possible (e.g., people put in physical danger). Conversely, IoT devices may also not face the same threat sources and events that the rest of a system might. For example, IoT devices with a short lifespan, limited functionality, or limited accessibility may not be subject to some threat sources (e.g., attackers aiming to do medium- to long-term reconnaissance) or some events (e.g., those that require extended, consistent network access). IoT devices will often have many of the same threat sources and events as the existing information system. There may be a set of unique IoT device threat sources and events as well as some information system threat sources and events that do not apply to the IoT device.

In this sense, there are two classes when comparing threat sources and events between the IoT device and information system: the threat sources and events can be the *same* or *different*. *Same*

means the sets are identical such that the IoT device brings no new threat sources or events but faces all the same threat sources and events as previously considered in the system's risk assessment. *Different* sets can be one of several categories:

1. No previously considered threat sources and events apply, only new threat sources and events (may) apply.
2. Some, but not all, previously considered threat sources and events apply, and new threat sources and events apply.
3. Some, but not all, previously considered threat sources and events apply, but no new threat sources and events apply.
4. All previously considered threat sources and events still apply, and new threat sources and events apply.

3.2.2 Effects on Vulnerabilities and Predisposing Conditions

How does the IoT device affect vulnerabilities and predisposing conditions considered as part of a risk assessment? As defined in CNSSI[19] No. 4009, "a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." [CNSSI] Additionally, predisposing conditions are characteristics of the environment, organization, or system that contribute to the likelihood that once initiated, threat events will result in undesirable consequences or impacts. An updated list of threat sources and events may help organizations identify vulnerabilities and predisposing conditions not previously considered as part of the risk assessment. These vulnerabilities could reside in the information system or in the proposed IoT device. Alternatively, considering potential vulnerabilities in an IoT device (e.g., default credentials that cannot be changed) may help the organization identify additional threat sources (e.g., credential stuffing authentication attack). For example, a minimal threat of system elements being compromised and assimilated into a DDoS[20]-executing botnet may have existed before, but a proposed IoT device deployment within the system may introduce vulnerabilities (e.g., default credentials) and predisposing conditions for this threat to exploit. IoT devices may have many of the same vulnerabilities as the existing information system. There may be a set of unique IoT device vulnerabilities as well as some information system vulnerabilities that do not apply to the IoT device.

In this sense, there are two classes when comparing vulnerabilities and predisposing conditions between the IoT device and information system: they can be the *same* or *different*. *Same* means the sets are identical such that the IoT device brings no new vulnerabilities or predisposing conditions but has all the same vulnerabilities and predisposing conditions as previously considered in the system's risk assessment. *Different* sets can be one of several categories:

[19] Committee on National Security Systems Instructions

[20] Distributed Denial of Service

1. No previously identified vulnerabilities and predisposing conditions apply, only new vulnerabilities and predisposing conditions (may) apply.

2. Some, but not all previously considered vulnerabilities and predisposing conditions apply, and new vulnerabilities and predisposing conditions apply.

3. Some, but not all previously considered vulnerabilities and predisposing conditions apply, but no new vulnerabilities and predisposing conditions apply.

4. All previously considered vulnerabilities and predisposing conditions still apply, and new vulnerabilities and predisposing conditions apply.

3.2.3 Effects on Likelihood(s) of Occurrence of Threats

How does the IoT device affect likelihood(s) of occurrence determinations as part of a risk assessment? Risk impact is dependent on two components: likelihood of occurrence and magnitude of impact. As per CNSSI No. 4009, likelihood of occurrence "is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)." [CNSSI] Determination of likelihood as part of a risk assessment is therefore based on identified threat sources and events as well as vulnerabilities and pre-disposing conditions. Threat sources, events, and vulnerabilities identified for the IoT device must be used in the assessment of likelihood. Likelihood of occurrence can often be expressed in a relative way (e.g., low, medium, or high likelihood of occurrence). As part of a risk assessment, the effect of an IoT device on likelihood of occurrence can be expressed as being *greater*, *lower*, or *equal* to the likelihood of occurrence without the IoT device. For example, an IoT device being connected to a system may create new possible connections (e.g., cellular data connections) that may increase the likelihood of a remote actor being able to exploit a vulnerability. In this case, the system with the IoT device can be said to have *greater* likelihood of occurrence compared to the system without the IoT device. Conversely, an IoT device with limited direct network connectivity (e.g., the IoT device can only communicate with the network through a hub/gateway) may reduce the comparative likelihood that a remote actor can exploit a vulnerability, resulting in a *lower* likelihood of occurrence *for that device*. In some instances of threats and vulnerabilities, the designation of a lower likelihood of occurrence may apply only to the IoT device, not the larger system. This is an important distinction. The system may still face the same overall level of likelihood of occurrence for a threat based on many factors, even if the likelihood of occurrence for the proposed IoT device is lower[21].

[21] A risk assessment must be performed at the system level, which will help identify security controls appropriate for that system. This publication discusses how an IoT device to be included as part of a larger system can be considered, which can impact those security controls, but does not solely dictate which controls are appropriate for the system, which must take into account all elements of the system, connections to other and supporting systems, etc. For example, a system may be comprised of laptops, smartphones, routers and other IT equipment that facilitates the use of cloud services and other external resources. These parts of the system will require a number of security controls to protect the system and its operation. As an IoT device is added to this system, it may operate and function in ways no other system element does, which could change which security controls apply. If the IoT device doesn't store any data, it may not need to meet some data at rest requirements needed on other system elements. The IoT device will still connect to the rest of the system, though, and may need to support other security controls such as protection of data in transit.

3.2.4 Effects on Magnitude(s) of Impact of Threats

How does the IoT device affect magnitude(s) of impact considered as part of a risk assessment? In addition to likelihood of occurrence, a risk assessment will consider the magnitude of impact. Magnitude of impact is defined in CNSSI No. 4009 as the level of harm "that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability." [CNSSI] The introduction of IoT devices into an information system can expand the harm to include human safety, environmental, and other impacts. IoT devices may introduce *greater*, *lower*, or *equal* magnitude of impact compared to the rest of the system. For example, an IoT device that is safety- and/or mission-critical may create *greater* magnitude of impact if compromised. A constrained IoT device (e.g., with limited storage, memory, or processing power), may contribute *lower* magnitude of impact relative to other elements in the system.

3.2.5 Determine Updated Risk Assessment

With an understanding of the threat sources and vulnerabilities introduced by the IoT device, as well as the resulting likelihood of occurrence and magnitude of impact, organizations can perform an updated risk assessment of the information system using information available about the proposed IoT device. Figure 6 shows how information about an IoT device will flow into the updated risk assessment of the system in which the IoT device is integrated. The resulting updated risk assessment may require the organization to allocate new security controls to the information system to effectively manage the anticipated risk. The organization may identify certain security controls that apply to the IoT device, or that must be provided by the IoT device specifically. Ultimately, it is important for organizations to identify all security controls required to reduce information system risk to an acceptable level. Section 3.3 will focus on using the identified security controls to determine the technical and non-technical capabilities needed from the IoT device and/or other system elements.

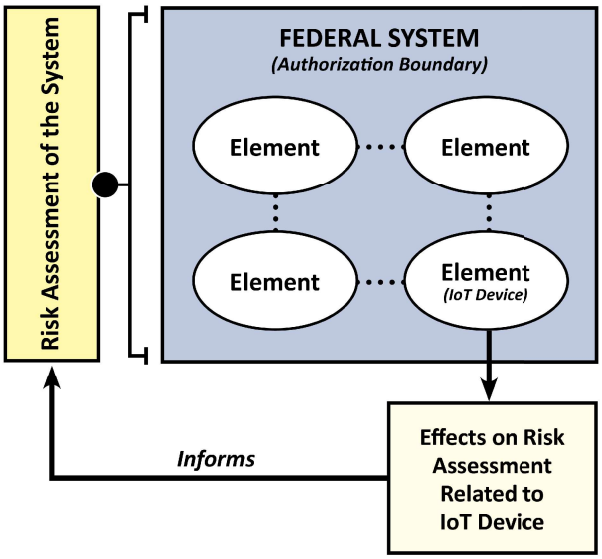

Figure 6: Effects on Risk Assessment due to IoT Device Informs the Risk Assessment of the Entire System.

3.3 Identifying Device Cybersecurity Requirements

Device cybersecurity requirements should be based on the security capabilities and security requirements of the system and organization while also accounting for considerations like those highlighted in Section 3.1 and updates to the system risk assessment that may be necessary as discussed in Section 3.2. Figure 7 below illustrates this process and how it will draw on the considerations and guidance from the prior sections to inform the device cybersecurity requirements.

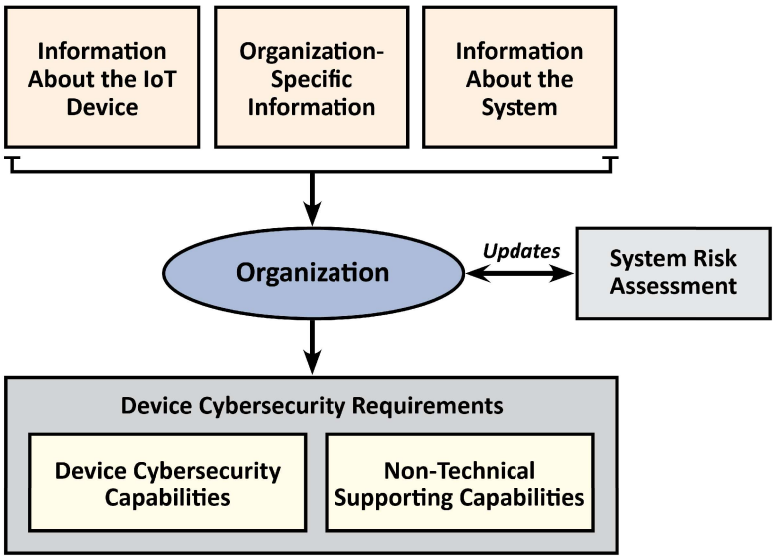

Figure 7: Organizations Can Gather Information to Update the System Risk Assessment and Determine Device Cybersecurity Requirements

Determining IoT device cybersecurity requirements may be challenging for some use cases. To assist organizations in selecting IoT device cybersecurity requirements, this section presents several NIST publications and resources. When the full set of security controls for the system has been identified, organizations can translate those controls into device cybersecurity capabilities and non-technical supporting capabilities. Since IoT device cybersecurity requirements are in support of security controls allocated to information systems, organizations can identify the device cybersecurity requirements needed to support the security controls allocated to the information system(s) to which the IoT device will be connected. Information security and systems administration personnel should collaborate to identify security controls that require support from system elements (e.g., IoT devices).

Example of Device Cybersecurity Requirements Supporting Security Controls

An organization might want to acquire an IoT device such as a *smart speaker* to use in the office environment. The smart speaker will need to connect to the system (e.g., internal network) so that organization management can access the speaker from other parts of the environment of operation and play audio over the speaker. These remote connections will require proper authentication and authorization. To support the authentication and authorization controls, the smart speaker may require device cybersecurity capabilities such as the ability to deny remote connections; the ability to authenticate and/or authorize entities attempting to make remote connections; and the ability to terminate connections within organizational policy. Other device cybersecurity capabilities may apply, but these are presented as example capabilities. Additionally, the allocated security controls may require the organization to configure the smart speaker to authenticate and authorize users within organizational policy, which could require non-technical supporting capabilities from manufacturers. These non-technical supporting capabilities could include obtaining documentation from the manufacturer about how the IoT device can be configured to support organizational authentication and authorization policy.

3.3.1 Identifying Requirements using SP 800-213A

Organizations may leverage SP 800-213A of this publication, The IoT Device Cybersecurity Requirement Catalog [800-213A]. This catalog contains device cybersecurity requirements organized by technical (i.e., device cybersecurity capabilities) and non-technical (i.e., non-technical supporting capabilities). The device cybersecurity requirements in the catalog are derived from security controls in SP 800-53 Rev. 5 and therefore may be helpful in supporting security controls in low, moderate, and high impact information systems.[22] SP 800-213A can be a valuable resource for organizations when identifying applicable IoT device cybersecurity requirements.

Organizations can use the mappings (i.e., between SP 800-53 Rev. 5 security controls and device cybersecurity requirements) included in SP 800-213A to identify appropriate device cybersecurity requirements. The mappings show, for each identified SP 800-53 Rev. 5 security control, the corresponding device cybersecurity capabilities and non-technical supporting capabilities needed to support the security control. Using the mapping, the organization will be able to develop a comprehensive list of device cybersecurity capabilities and non-technical supporting capabilities. This list of device cybersecurity capabilities and non-technical supporting capabilities may need to be tailored—just like an organization tailors the SP 800-53 Rev. 5 security controls. Some device cybersecurity capabilities and non-technical supporting capabilities identified through the mapping may not be applicable to the use case. For example, a required SP 800-53 Rev. 5 security control might map to the capability "Ability to create an

[22] The device cybersecurity requirements (i.e., device cybersecurity capabilities and non-technical supporting capabilities) included in the SP 800-213A catalog were based on the IoT core baselines, but adapted the content of those high-level sets of capabilities into more thorough articulations. This adaptation was guided by the SP 800-53 security controls, with the more specific and additional content (relative to the IoT core baselines) developed to support the statements in applicable SP 800-53 security controls and enhancements. Additional information is included in SP 800-213A.

organizationally-defined system use notification message or banner to be displayed on the IoT device." For many IoT devices and/or use cases, this capability is not applicable; organizations might choose to scope this identified capability out of the needed capabilities. Other identified device cybersecurity capabilities and non-technical supporting capabilities might be best provided by a different system element (e.g., gateway, IoT Platform, cloud service provider) instead of by the IoT device. If an organization is planning to acquire a constrained IoT device (i.e., the device has limited internal memory, storage, and/or processing power), the organization may need to carefully consider those capabilities that can be provided by the IoT device and those capabilities that will need to be provided by other system elements. Organizations should also carefully consider the key device cybersecurity requirements for an IoT device that *must* be present on the device for it to be integrated into the system.

3.3.2 Identifying Requirements using Other Resources

In addition to device cybersecurity capabilities and non-technical supporting capabilities identified using the mapping described in Section 3.3.1, organizations may determine that additional capabilities are needed from IoT devices and/or system elements in order to support security controls and reduce risk to acceptable levels. The NISTIR 8259 series of documents, CSF, RMF, and other activities and resources can help organizations identify additional needed capabilities.

Guidance that identifies applicable starting-points for device cybersecurity requirements may help some organizations overcome challenges they may encounter when determining appropriate device cybersecurity requirements for IoT devices. Organizations must hit a moving target in identifying device cybersecurity requirements to support a set of controls that may change based on the IoT device selected and its use case. Further compounding this challenge is the need for thorough understanding and consideration of a number of areas (e.g., technical knowledge about cybersecurity, knowledge of the operational side of the system/device, insight into organizational security controls), which may be spread among multiple personnel within an organization or fall outside their cybersecurity work role and related expertise. Small organizations, those geographically further from headquarters, and those with significant proportions of personnel without technological or cybersecurity work roles, among other factors may find these challenges are amplified.

NISTIR 8259A specifies the high-level device technical cybersecurity capabilities that generally achieve minimal securability for most customers. The IoT core baseline, as the IoT device cybersecurity capability core baseline from NISTIR 8259A is called, is meant to apply to all IoT use cases and customers, meaning it is phrased at a high level to meet many different needs. NISTIR 8259B presents a set of non-technical supporting capabilities—the IoT non-technical supporting capability core baseline—generally needed from manufacturers or entities to support common security controls. Like 8259A, the non-technical capabilities in 8259B are phrased at a high level to be broadly applicable to various use cases and customers.

The IoT core baselines presented in NISTIR 8259A and 8259B can be profiled for a specific customer, sector, or use case. The process of profiling tailors and/or extends the IoT core baselines and can be performed at any level of specificity, even to an individual customer (e.g., organization within the federal government).

One such profile of the IoT core baselines that is guided by the needs and goals of organizations is called the federal profile, which is included as Appendix A to SP 800-213A [800-213A]. The federal profile uses the SP 800-53 Rev. 5 controls catalog [800-53] as an input source of federal government security needs and goals to identify device cybersecurity capabilities and non-technical supporting capabilities. Since the federal profile targets minimal securability for all federal government use cases, it focuses on device cybersecurity requirements that support the low-impact baseline set of SP 800-53 Rev. 5 controls, which would be a sub-set of the device cybersecurity requirements in Sections 2 and 3 of SP 800-213A. This focus for the federal profile is based on the assumption that the low-impact baseline set of controls will be used as the minimum set of controls for systems either directly or as a sub-set of the full set of controls used (e.g., if the organization uses the moderate or high impact baseline or employs additional tailoring beyond the baseline). The federal profile is therefore recommended as a starting point for organizations to use to identify IoT device cybersecurity requirements when incorporating an IoT device into a low-impact system.

The federal profile, and other similar lists of capabilities that may be more applicable to the specific use case or deployment, can be helpful for organizations to reduce the challenges they may face in determining device cybersecurity requirements for IoT devices. However, the federal profile and other lists of device cybersecurity requirements may not be a perfect fit for a specific IoT device, organization, and/or system. The list of device cybersecurity capabilities and non-technical supporting capabilities in the federal profile may still need to be tailored as described in Section 3.3.1[23]. In particular, the use of the low-impact baseline may not be appropriate for all organizations and use cases (e.g., if the IoT device is to be integrated into a moderate- or high-impact information system). Tailoring of device cybersecurity requirements derived from profiles, including the federal profile, using any available information such as organization-specific considerations will help alleviate possibly costly issues when seeking approval for or integrating the IoT device (e.g., having to procure another IoT device when the IoT device purchased cannot be approved or connected to the system as intended). This underscores the importance of involving IT personnel to ensure an evaluation of features and functionality pertinent to being able to securely configure or integrate a device, prior to a purchase being made.

Using the guidance described in Section 3.3, organizations shall identify all applicable IoT device cybersecurity requirements, including *key* device cybersecurity requirements, ensuring that information system security controls are supported. If the IoT device and/or manufacturer do not provide all required device cybersecurity capabilities and non-technical supporting capabilities, organizations should follow established risk management strategies to plan for the IoT device's incorporation into the system. Section 4 discusses these risk mitigation options.

[23] Manufacturers may choose to incorporate the device cybersecurity requirements from the federal profile in their IoT devices, especially for IoT devices where federal agencies are an expected customer