Association for Information Systems

AIS Electronic Library (AISeL)

SAIS 2020 Proceedings

Southern (SAIS)

Fall 9-11-2020

Assessing Cybersecurity Risks When Adopting Internet of Things (IOT) Devices

Julio Rivera
University of Alabama at Birmingham, jrivera@uab.edu

Paul Di Gangi
University of Alabama at Birmingham, pdigangi@uab.edu

Recommended Citation

Rivera, Julio and Di Gangi, Paul, "Assessing Cybersecurity Risks When Adopting Internet of Things (IOT) Devices" (2020). *SAIS 2020 Proceedings*. 15.
https://aisel.aisnet.org/sais2020/15

ASSESSING CYBERSECURITY RISKS WHEN ADOPTING INTERNET OF THINGS (IOT) DEVICES

Julio C. Rivera
University of Alabama at Birmingham
jrivera@uab.edu

Paul M. Di Gangi
University of Alabama at Birmingham
pdigangi@uab.edu

ABSTRACT

The Internet of Things (IoT) is a term covering a broad array of Internet-connected devices adopted by both business entities and consumers. Unfortunately, this connection to the Internet also exposes these devices to connections from other devices on the Internet. In the current cybersecurity environment, this means that IoT devices are susceptible to all manner of cybersecurity threats. Thus, the adoption of IoT devices brings with it exposure to an array of cybersecurity risks. This paper attempts to develop a framework to analyze the nature of cybersecurity threats and the resulting risks faced by entities adopting IoT devices.

KEYWORDS

Internet of Things, risk, adoption, cybersecurity

INTRODUCTION

The Internet of Things (IoT) is a term covering a broad array of devices "*that connect, communicate or transmit information with or between each other through the Internet*." (Report, 2015, p. 6). Such flexibility in its ability to share information is one of the primary drivers of IoT adopted by both business entities and consumers. Unfortunately, this connection to the Internet also exposes these devices to connections from other, unexpected and unauthorized, devices on the Internet. Furthermore, IoT devices may depend on a remote service infrastructure to deliver their functionality, potentially exposing users to threats compromising their privacy and data confidentiality. In the current cybersecurity environment, the adoption of IoT devices brings exposure to an array of cybersecurity threats.

This paper seeks to develop a framework that can analyze the nature of cybersecurity threats and the resulting risks faced by entities adopting IoT devices. The paper attempts to identify the categories of functional capabilities that IoT devices may deliver, and the cybersecurity threats these capabilities may bring with them. Understanding the nature of these capabilities can lead to identifying the cybersecurity risks to a given IoT device. In the next section, we first formulate a definition for IoT and then discuss the nature of risk inherent in such devices. We then develop a risk assessment framework for IoT devices and present a summary of this framework and its structure.

DEFINING INTERNET OF THINGS AND ITS STRUCTURE

The term "Internet of Things" was first introduced in the late 1990s (Bhandari, 2019), and although there is no one definition for the term; the Federal Trade Commission (FTC) (2015) report on Privacy & Security in a Connected World has defined it as "*devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.*" (p. 6) This definition covers a wide range of devices and supporting technologies used in commercial and consumer environments. IoT devices have a combination of features, including electronic components, software, sensors, and network connectivity, which may exchange data with servers, centralized systems, or other connected devices (Bertino, 2016).

A useful way of understanding IoT devices is via its architectural model describing device capabilities. To date, scholars have identified a three-layer model that provides a useful abstraction in analyzing IoT device capabilities and features (Burhan, Rehman, Khan, & Byung-Seo, 2018; Nord, Koohang, & Paliszkiewicz, 2019). Specifically, Nord et al. (2019) postulate an architectural model consisting of a sensing layer, a network layer, and an application layer. In this model, the sensing layer consists of an IoT device's environmental sensing and data collection capabilities; the network layer addresses an IoT device's network communication capabilities; and the application layer covers an IoT device's software delivered functionality, either on the device or through supporting software services.

Regarding sensing capabilities, IoT devices employ a wide range of sensors collecting such things as video, audio, positional, device status, and other environmental data (Burhan et al., 2018). From a network communication perspective, IoT devices use a broad array of technologies ranging from wired communication to wireless communication using anything from Wi-Fi to Bluetooth to cellular communication, and other wireless technologies (Burhan et al., 2018). Finally, at the application layer, the software processes and interprets sensor data, as well as commands the use of IoT device capabilities (Burhan et al., 2018). With software-driven command of device capabilities, this may include device capabilities as simple as turning on a switch, to a complex set of commands directing all aspects of the device (Adat & Gupta, 2017). Many devices offer combinations of these capabilities, resulting in a rich and complex mix of device capabilities.

In addition to an IoT device's native hardware capabilities, there is the added dimension of how the device uses its capabilities and what it communicates to the outside world. Given that IoT devices connect to the Internet, they send and receive data as part of their operation. Many IoT devices rely on the data they send and receive to augment their native capabilities. Typically they use services provided by the device vendors or other third-party service providers, who in turn, use the data to deliver additional functionality or services (Cvitić, Vujić, & Husnjak, 2015). How to handle this data and who is the recipient and owner of such data adds to the complex nature of IoT devices and their adoption. Thus, IoT represents a complex technical architecture with implications for how information is received, transmitted, and processed. Such a device carries with it the potential to compromise the confidentiality, integrity, and availability of an organization or home user's security and privacy.

INTERNET OF THINGS RISK ASSESSMENT

IoT devices operate in environments that combine sensing, communications, and processing capabilities. Each of those areas exposes users to risk (Cvitić et al., 2015). Those risks range from the theft of data to the takeover and malicious control and actuation of IoT devices (Fagan, Megas, Scarfone, & Smith, 2019). Even though this broad range of risks exists, it is useful to think of risks as falling into two broad categories. One category is that of risks to data security, while another is the risk to the control of the IoT device itself (Fagan et al., 2019).

Data security risks range from the theft of data from an IoT device or its sensors to the theft of data collected by a third-party service augmenting IoT device functionality. In addition to the direct threat to data security, there is also the indirect threat of inferring valuable information from any data collected. Direct threats to data security are relatively easy to understand since the data will be of value to the party acquiring it. For example, gaining access to Personally Identifiable Information (PII) is recognized as something valuable to those engaging in identity theft (Report, 2015).

Indirect threats to data security, however, are a more subtle but no less threatening breach of data security. These threats arise from the collection of enough data to infer information that may be of value to a malicious third-party. For example, collecting data on something as innocuous as turning lights on or off may lead to the creation of a profile showing a dwelling's occupancy patterns. In such a case, the individual data points themselves are not of value, but when aggregated, they can be used to infer behavior patterns (Report, 2015). Thus the risk assessment process should not neglect this aspect.

Risks to the control of IoT devices are no less threatening than data security risks. IoT devices are a combination of computing hardware, sensing capabilities, and controlling software. Each of those areas poses an attack vector for a malicious third-party seeking to control the device. Generally, vulnerabilities in these areas are the results of flaws in the device's operating software or the firmware embedded in the device hardware. The exploitation of these attack avenues can allow malicious third-party control of an IoT device and depend on the device's capabilities to engage in a wide variety of malicious behavior. Apart from using a device to surveil or generate attacks on other Internet attached devices, there is the real possibility of actuating an IoT device's embedded capabilities to manipulate it or attached devices (Report, 2015).

A PROPOSED RISK ASSESSMENT FRAMEWORK FOR INTERNET OF THINGS DEVICES

The purpose of proposing a risk assessment framework is to give IoT technology adopters a frame of reference when gauging their cybersecurity risk exposure. For security professionals, this is the first step in deciding how to mitigate risk, and ultimately deciding what level of risk to accept. As such, a framework should be a guide on what items should be assessed, and allow the technology adopting entity to make decisions on how to handle their risk exposure. The nature of IoT devices with their wide range of capabilities and applications requires that we develop a framework with a sufficient level of abstraction applicable to all IoT devices.

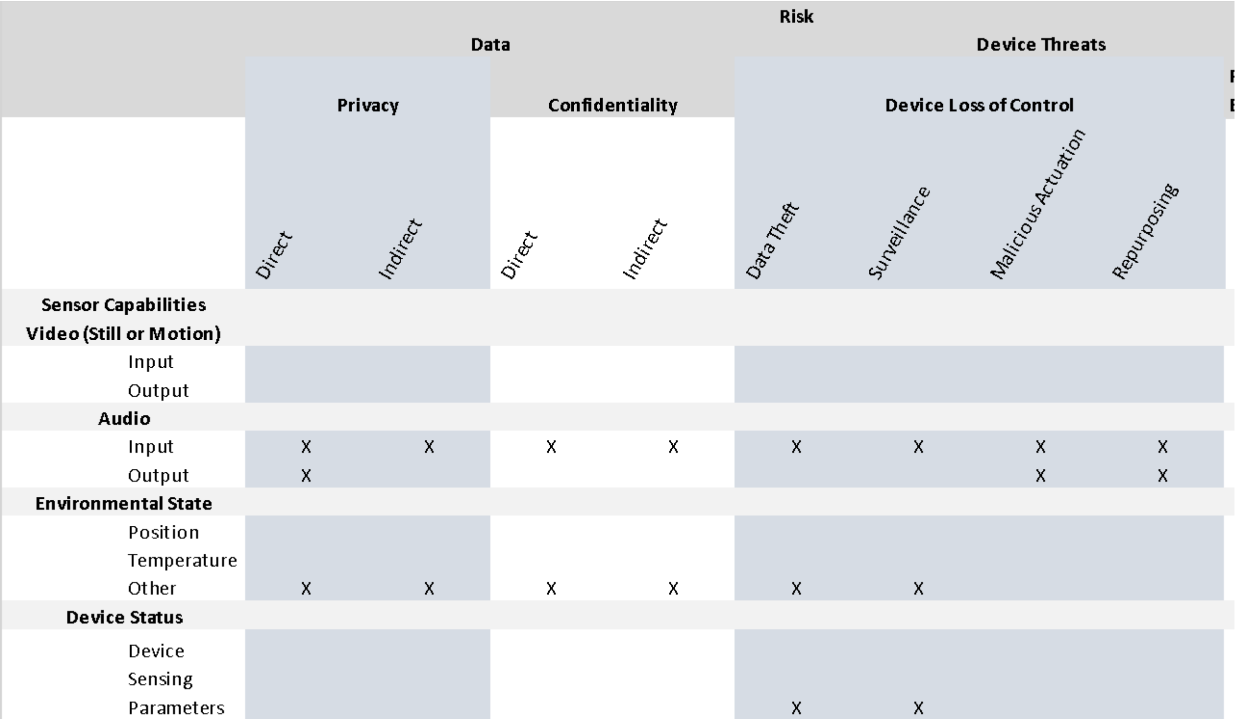
As mentioned in the previous discussion, a useful abstraction when examining IoT device capabilities is the three-layer architectural model postulated by Nord et al. (2019). This model identifies three categories of IoT device capabilities: 1) a sensing layer, 2) a network layer, and 3) an application layer. The previous discussion also identifies two areas of risk inherent in all IoT devices; risks to data security, and risks to control of IoT devices (Report, 2015). Therefore, it is useful to examine each architectural layer from the perspective of both risks to data security and risks to IoT device control.

In the following tables, we capture the types of risks associated with the sensing, network, and application layers in IoT devices in two categories – data risks and device threats. Within the data risks, we have direct and indirect risks to both privacy and confidentiality. Direct data risks are those that occur from loss of privacy or confidentiality from the compromise of specific data elements; for example, data considered to be PII. Indirect data risks would be those resulting from the collection of data that infers compromising information about the targeted entity, such as collecting data about behaviors or events that can lead to inferring a pattern of behavior.

In the realm of device threats, we have the risk of loss of device control, as well as the risk of device function blocking. Loss of device control can lead to data theft, where data collected by the device or its services may be collected for use by a malicious third-party. Related to this risk is the compromise of device control, allowing a third-party to surveil an entity through the use of device sensors and capabilities. A third-party gaining device control might also use the device's capabilities to actuate a device's sensing or manipulation capabilities, including device capabilities that might command other devices. Repurposing a device might lead to using that device for purposes other than those for which it was intended, such as generating attacks on other devices or computing platforms. Finally, the risk of device function blocking exists when a device is prevented it from fulfilling its intended function(s) via malicious attacks, such as might result from a denial of service attack.

The risks enumerated above illustrate broad categories of risk and ensure that the risk assessment process evaluates risk exposure in each category. IoT devices are subject to multiple cybersecurity risks, and in fact, there is overlap in the risk categories identified. However, when these risks are evaluated using the sensing, network, and application architectural layers, the nature of the risk at each layer may take on a different character.

In Table 1, we see how the risk categories are applied at the sensing layer. This layer comprises the sensing capabilities that an IoT device may have, illustrating the types of data that such a device may collect. Some of these capabilities are bidirectional, such as devices that combine both input and output capabilities, as might be seen in two-way video devices or voice-controlled personal assistants. Beyond that, there is a wide range of devices that are capable of sensing such things as temperature and other environmental data or delivering data on a device's current status. Furthermore, some of these also allow for the manipulation of the device's state or of other devices that it controls.



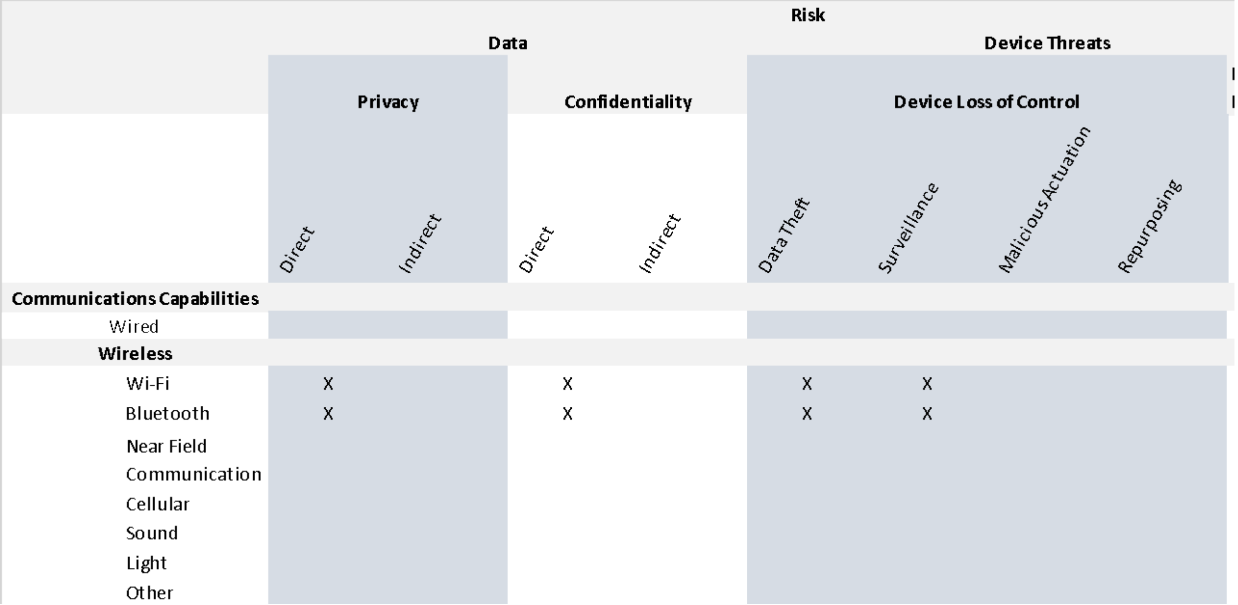
	Risk							
	Data				Device Threats			
	Privacy		Confidentiality		Device Loss of Control			
	Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Repurposing
Sensor Capabilities								
Video (Still or Motion)								
Input								
Output								
Audio								
Input	X	X	X	X	X	X	X	X
Output	X						X	X
Environmental State								
Position								
Temperature								
Other	X	X	X	X	X	X		
Device Status								
Device Sensing Parameters					X	X		

Table 1. Sensing Layer (Amazon Echo Dot Example)

A simple example of such a device might be an Amazon Echo Dot, a popular consumer device that serves as an intelligent digital assistant, is used as an exemple for illustrative purposes. This device allows a user to communicate via voice and has an internal speaker that provides audio responses. The device connects to a network through its Wi-Fi connection (as well as through Bluetooth, if enabled). Functionality for the device is managed via its onboard software and its communication with a third-party service provider (i.e., Amazon). The Echo device software also has an extensible framework for adding additional features, as well as allowing it to interface and possibly control other devices. Control of other devices depends on a software interface providing access to the other device's third party services.

At the sensing layer, we can identify risks to data due to the Echo's combination of input and output audio capabilities. In this regard, those capabilities can be used to collect data directly or generate audio output, as well as indirectly to sense patterns of behavior related to audio input. Data on the device's state or the state of other devices it controls may obtained from the Echo device. Both of these situations can lead to the data theft or the use of the device for surveillance. Finally, there is the possibility of a denial of service attack on such a device, both by flooding its network interface, as well as preventing the device from responding to voice commands by generating enough audio interference to prevent it from detecting voice commands.

Table 2 applies the risk categories to an IoT device's network layer. Regardless of the nature of an IoT device, in order to function, it must communicate with a network. Communication may be through wired or wireless means. While there are risks such as man in the middle attacks, that are shared by both wired and wireless communication, the realm of wireless communication has many more opportunities for malicious exploitation. Due to the many potential wireless communication protocols, an IoT device may communicate through, each with its peculiar vulnerabilities, it is essential to evaluate the risks a device is subject to in each risk category.



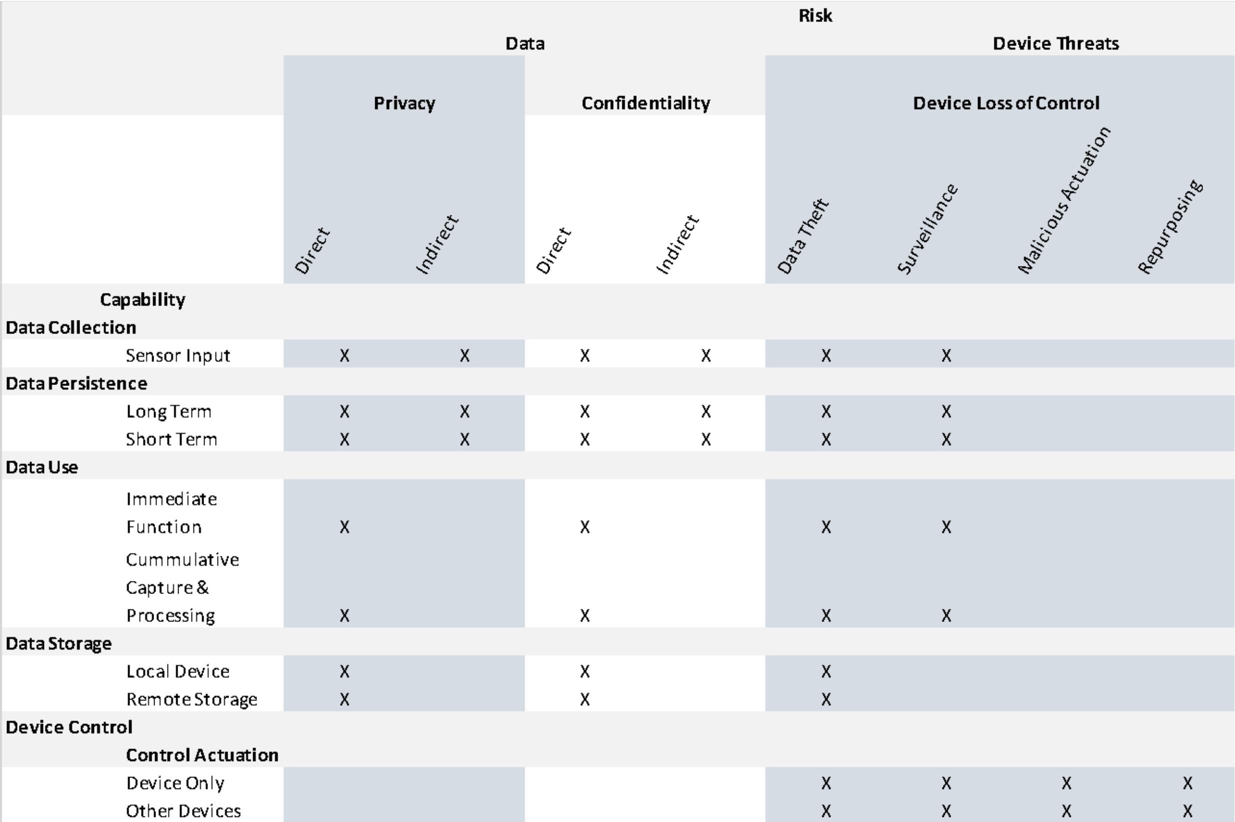
	Risk							
	Data				Device Threats			
	Privacy		Confidentiality		Device Loss of Control			
	Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Repurposing
Communications Capabilities								
Wired								
Wireless								
Wi-Fi	X		X		X	X		
Bluetooth	X		X		X	X		
Near Field Communication								
Cellular								
Sound								
Light								
Other								

Table 2. Network Layer (Amazon Echo Dot Example)

Examining an Echo Dot at the network layer perspective reveals that the Echo uses two wireless interfaces. Both of these interfaces are subject to the known cybersecurity threats associated with those communications methods. Since communication utilizes radio transmission, radio signals can be intercepted and captured, leading to risks regarding any data transmitted. Finally, a denial of service attack can be deployed against such a device's network layer, by flooding the network with radio frequency interference.

Lastly, the application layer ties together the sensing and network capabilities to give an IoT device its functional capabilities. This layer may include application software on the device, as well as services provided by a third-party. This combination presents a challenge when evaluating risk, as particularly when evaluating the risks from third-party services, there may be little transparency. IoT devices contain a software layer that acts as an operating system and supports hardware and networking functionality, as well as the software that provides device functionality. Each of these areas of potential vulnerability must be evaluated based on their associated risk.

Table 3 summarizes the application layer risks. This layer addresses device functionality in terms of both data collection and device control. From a data perspective, how data is collected, used, and stored are areas that need to be assessed for risk. As mentioned earlier, the data an IoT device collects or works with, may not be just stored on the device, but may also be handled and stored by third-party services. Complicating this picture further is how an IoT device is controlled, or in turn, controls other devices. Each of these areas needs to be evaluated for cybersecurity risks to get an accurate picture of the risk exposure in adopting a given IoT device.



		Risk							
		Data				Device Threats			
		Privacy		Confidentiality		Device Loss of Control			
		Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Repurposing
Capability									
Data Collection									
	Sensor Input	X	X	X	X	X	X		
Data Persistence									
	Long Term	X	X	X	X	X	X		
	Short Term	X	X	X	X	X	X		
Data Use									
	Immediate Function	X		X		X	X		
	Cummulative Capture & Processing	X		X		X	X		
Data Storage									
	Local Device	X		X		X			
	Remote Storage	X		X		X			
Device Control									
	Control Actuation								
	Device Only					X	X	X	X
	Other Devices					X	X	X	X

Table 3. Application Layer (Amazon Echo Dot Example)

The application layer reveals a wealth of cybersecurity risks. The software that controls the device may be susceptible to exploitation, opening to a range of risks spanning data theft to malicious control and repurposing of such a device. Complicating the picture further is the susceptibility of third-party services to malicious exploitation that can result in data theft or compromise, as well as the possibility of malicious device actuation or repurposing. Adding to this is the potential for the functionality of the device to blocked either through local control or through the third party services a device may use.

In the Amazon Echo Dot example, a device user would be able to use the proposed framework to evaluate their risk exposure from adopting the device. The risks identified show a certain degree of overlap based on the architectural layer analyzed. That overlap is a result of the different facets of a device's capabilities highlighted by each architectural layer. So while one layer may emphasize the sensing aspect of a device, another layer emphasizes the software control of those sensing mechanisms. Ultimately, looking at the aggregate results provides a comprehensive view of the cybersecurity risks associated with the adoption of an IoT device.

CONCLUSION

This paper presents a framework for evaluating cybersecurity risk exposure when adopting IoT devices. It is by no means an exhaustive treatment of the risks associated with device adoption, but it does provide a systematic approach to evaluating risk. The three-layer architectural model provides a useful abstraction of an IoT device's capabilities, facilitating the evaluation of risks in the data and device threat categories. Proceeding through a risk analysis at each architectural layer yields a comprehensive view of IoT cybersecurity risks.

The decision to adopt an IoT device is a balance between a device's perceived benefits to the user, versus the inherent cybersecurity risks in adopting such a device. In making such a decision, the user needs to weigh potential risks, the likelihood of realizing those risks, and the perceived benefits of the device. The proposed framework addresses the potential risk question. The framework does not address the issue of the likelihood that a particular risk is realized; that exercise is something the user will have to engage in based on the proposed device's use and environment. Furthermore, if the decision is made to adopt an IoT device, the user will also have to decide what steps to take to mitigate or accept any risks that are identified as likely to be realized. Those decisions, though, rely on developing a comprehensive picture of the of the cybersecurity risk exposure inherent in adopting a given IoT device.

REFERENCES

1. Adat, V., & Gupta, B. B. (2017). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems, 67*(3), 423-441. doi:10.1007/s11235-017-0345-9
2. Bertino, E. (2016). *Data Security and Privacy in the IoT.* Paper presented at the EDBT.
3. Bhandari, G. (2019). Internet of Things (IOT) Market Report. *Macrosource Media*. Retrieved from https://www.macrosourcemedia.com
4. Burhan, M., Rehman, R. A., Khan, B., & Byung-Seo, K. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors (14248220), 18*(9), 2796. doi:10.3390/s18092796
5. Cvitić, I., Vujić, M., & Husnjak, S. (2015). Classification of security risks in the IoT environment. *Annals of DAAAM & Proceedings, 26*(1), 0731-0740. doi:10.2507/26th.daaam.proceedings.102
6. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2019). *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*. National Institute of Standards and Technology Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf
7. Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications, 133*, 97-108. doi:10.1016/j.eswa.2019.05.014
8. Report, F. S. (2015). *Internet of Things Privacy & Security in a Connected World*. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-Internet-things-privacy/150127iotrpt.pdf