*Issues in Information Systems*
*Volume 17, Issue IV, pp. 21-28, 2016*

# SECURING THE INTERNET OF THINGS: A REVIEW

***Matthew Ahlmeyer, Bentley University, ahlmeye_matt@bentley.edu***
***Alina M. Chircu, Bentley University, achircu@bentley.edu***

## ABSTRACT

*The Internet of Things (IoT), the next evolution in Internet technology, is predicted to add tens of billions of devices to the Internet in the next few years. IoT will enable businesses to use these devices to collect data about their customers, products and internal operations, and use the data for improving existing processes and creating innovative products and services. Among the associated risks and challenges that must be addressed, IoT security is at the top of this list. In this paper, we analyze the recent academic and practitioner literature on IoT security. Overall, we find that although experts agree IoT security is extremely important, businesses in the IoT space, developers, users and regulatory agencies are slow in implementing IoT security measures. Our analysis identifies three major gaps: a lack of security in current IoT implementations, a lack of detailed, specific IoT guidelines in current IT security standards, and a lack of IoT laws and regulation at the country and international level. To address these gaps, we propose an IoT security framework that highlights key security requirements in five areas: IoT security levels, IoT security activities, IoT security value chain, IoT security standards, and IoT security education.*

**Keywords:** Information Technology (IT), Internet of Things (IoT) Security, Security Framework

## INTRODUCTION

The Internet of Things has arrived and is the next evolution – and disruption - in Internet technology (Dijkman et al., 2015; Ebersold & Glass, 2015). The Internet of Things (IoT) is defined as "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" (Rouse, 2014). IoT utilizes technologies such as radio-frequency identification (RFID) and sensors to connect "things" in the environment to the Internet. In this context, a thing can be, for example, somebody's heart monitor, a fitness tracker, an appliance, an industrial machine, or a car – all of which can collect data about their performance or location, save it and process it locally or on a server, and create alerts based on pre-defined rules – such as a car alerting the user when the tire pressure is too low. Current projections state that the number of such IoT devices by 2020 will be over 26 billion (Lee & Lee, 2015).

However, with any opportunity there are also risks and challenges that must be addressed, and IoT security is at the top of this list (Ebersold & Glass, 2015; Folk et al., 2015; French & Shim, 2016; Hodgson 2015; Weinberg et al., 2015). Information technology (IT) security is already a major concern that businesses should be focused on – in fact, experts suggest that IT security considerations should be just as important as business considerations when making business decisions (Buecker et al., 2010). As businesses start implementing IoT devices to improve their internal processes and connect with their customers, IoT security becomes paramount (Accenture, 2015). However, while experts identify a significant need for IoT security, businesses in the IoT space, developers working for these companies, and users of their IoT solutions are either failing to implement security measures, or are not very concerned with the security issues (Weinberg et al., 2015). This paper analyzes the recent academic and practitioner literature on IoT with the goals of identifying current developments, highlighting major IoT security gaps, and proposing a framework for addressing the gaps.

**IOT: TECHNICAL AND BUSINESS CONSIDERATIONS**

IoT is capable of bringing businesses to new, innovative levels never before experienced (Ebersold & Glass, 2015; Weinberg et al., 2015). This is as a result of the development of devices and sensors using RFID—such as wearables and other automation products. IoT has the ability to collect data on virtually anyone and anything and can be implemented almost anywhere (Hodgson, 2015). The ability to collect data on current and potential customers has led some businesses to fully adopt the IoT business models (Dijkman et al., 2015). This is increasing their value as businesses and leading to increased financial returns (Hodgson, 2015). These financial returns are a result of businesses better understanding their customers. Similarly, the average person is also fully invested in the IoT revolution. It is now commonplace to see someone who owns an IoT device whether they know they are using it or not. For example, smart watches and Nest Thermostats are part of IoT as they are devices that connect to the internet to transmit signals and data over networks enabling the user to learn more about their habits and become closer with their environment. This is an appealing option to the user as they can live a healthier lifestyle through a wearable that tracks their daily movement or save money through the thermostat that adjusts the temperature in their home when they leave for work each day. The IoT revolution is only just beginning and that the potential to expand into new areas will continue to occur.

In order to make IoT live up to its potential, there is a need to understand and further develop the technical side of IoT. Recent research identifies five technologies that enable successful IoT-based products: RFID, wireless sensor networks, middleware, cloud computing, and IoT application software. RFID allows for the automatic identification and data capture using radio waves, a tag, and a reader (Lee & Lee, 2015). RFID has evolved to capture more than just traditional barcode data when scanned and tags no longer have to be manually scanned by an individual to be logged. In passive RFID applications, a strategically placed reader can pick up the frequency from a tag placed on a product – from a package that needs tracking during transportation to a car that can be identified remotely (Lee & Lee, 2015). Active RFID tags that have their own batter supply and can instigate communication with a reader at any time can also be used in IoT applications, typically on devices that are tracking temperature, movement or chemical composition levels. Next, wireless sensor networks (WSN) consist of spatially distributed autonomous sensor-equipped devices to monitor physical or environmental conditions and can cooperate with RIFD systems (Lee & Lee, 2015). Recent advancements in WSN have made low-power miniature devices affordable (Lee and Lee, 2015). Middleware is a software layer interposed between software applications to make it easier for software applications to communicate with one another (Lee & Lee, 2015). This communication is key to IoT as without middleware the IoT device would only be able to collect data but the computer or database on the back-end would not be able to interpret what was being collected. Thus, middleware is essential as it transmit the data collected into readable forms. The fourth factor, cloud computing, is the ability to have access to a shared pool of resources on-demand (Lee & Lee, 2015). With the massive amounts of data that IoT collects cloud computing has enabled applications with the ability to store the data virtually and then access it at any moment. Finally, a myriad of IoT applications and interfaces have been developed as a result of IoT. This has enabled device-to-device and human-to-device communication (Lee & Lee, 2015).

Our review of the literature identifies an inherent conflict in the IoT space: as new technology is developed, the goal of companies is to get the product developed and to market as soon as possible, in spite of some inherent risks that the new technology may bring about. With respect to IoT, security and privacy are major concerns (Hodgson, 2015), but they are often forgotten or minimized (Weinberg et al, 2015). Instead of ensuring that these devices are secure and safe before implementation, convenience often is more important to both the developers and sometimes users. Put differently, the goal of getting the product to market, installed, and implemented to begin profiting or collecting data is more important than the security and privacy of those who utilize the new technology (Weinberg et al., 2015). Additionally, the security frameworks that are currently in place have yet to adapt and adequately cover IoT related issues as a survey of IT security professionals found that 70% thought current frameworks were ill prepared to handle the IoT revolution (Lee & Lee, 2015). Thus, while the IT audit and cybersecurity jobs are in high demand, they may not be able to effectively oversee IoT devices. Similarly, the regulatory aspect of IoT is also in its infancy stages. Any regulation—especially on an international level—is difficult to achieve due to the rapid progression of the technology and varying views on such technology (Weber, 2015). Laws prohibit the collection of personally identifiable data, however, this is a grey area in IoT as while the data may be personal it may not always be able to be tied back to a specific individual. This hazy area has caused the regulation to lag behind technology and resulted

in industries manufacturing these devices to self-regulate (Weber, 2015). However, as previously stated, convenience is often the predominant factor. Thus, security issues are often overlooked as they would inhibit the product from entering the market. We look at the literature addressing these tradeoffs in more depth in the next section.

## UNDERSTANDING IOT SECURITY CHALLENGES

The definition of IoT security is similar to that of mobile security which includes the protection of personal and business information that is stored, collected, and transmitted from devices connected to the internet (Weber, 2015). This involves the protection from malware threats and unauthorized access to the device (Weber, 2015). Three major themes are present in the practitioner and academic papers investigated for our IoT security analysis. *First*, there are "call to action" papers which point out that security is an issue and those developing or utilizing IoT devices should pay careful attention to security. *Second*, there are technical papers which analyze IoT security threats and offer concrete solutions as to how to solve the security issue plaguing IoT. *Third*, there are legal frameworks papers that look at the security and privacy regulations and laws and their application to IoT.

In recent years cyber threats have grown exponentially in both quantity and volume (Hodgson, 2015). Security breaches and cyber heists are happening all around us and the authors of these papers do not expect that to change. This can and should be frightening to both companies and users. There are significant emerging security issues in IoT applications, networks, and devices/equipment, which could have major impacts on many industries and products (Accenture, 2015). Due to the unprecedented connectivity level in IoT, the potential vulnerabilities are also unprecedented (Folk et al., 2015), as every device is susceptible to being hacked and have its data compromised (Schneier, 2014). Hewlett Packard performed a study in 2014 that revealed 70% of IoT devices contain serious vulnerabilities (Lee & Lee, 2015). This was confirmed by Veracode who tested a handful of devices as part of their IoT security research and found that all but one was vulnerable in multiple categories (Veracode, 2015). It is anticipated that 20% of security budgets will be designated solely to IoT by 2020 (Ranger, 2020).

A common phrase among practitioners is that security needs to be the DNA or the foundation of IoT (Folk et al., 2015). Companies involved in the IoT space can integrate security at the core of their value proposition by setting up a team of business executives and security specialists, integrating security best practice with IoT product development, educating customers and front-line staff in security best practice, and addressing privacy concerns with transparent policies (Turner, 2015). Four key areas for IoT security development need to be addressed: protecting communications, protecting devices, managing devices, and understanding your system (Symantec, 2016).

Looking at the IoT security from a more technical lens, the issues can be analyzed by utilizing pre-existing IT security frameworks, and expanding them to include IoT. For example, IBM has developed a well-known security framework that addressed the missing elements in existing security standards, such as the COBIT and ISO/IEC standards. COBIT (Control Objectives for Information and related Technology) was first developed in 1996 as an audit standard by ISACA, an organization previously known as the Information Systems Audit and Control Association that today serves many IT governance professionals. COBIT has gone through several iterations and upgrades to incorporate control, management and IT governance elements. Today, in its 5$^{th}$ iteration, it is a comprehensive standard for the governance of enterprise IT solutions (Wal et al., 2012). COBIT looks at business information that every enterprise needs to support business decisions through criteria including effectiveness, confidentiality, integrity, compliance, and others (IBM, 2010). In addition, IBM analyzed standards issued by the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC) (IBM, 2010). The ISO/IEC 27002:2005 standard is comprehensive in covering security issues and establishing complex control requirements. After looking at COBIT and ISO/IEC, which both address the "how" of security through best practices and control objectives, IBM developed their own security framework describing the missing element – the "what." The IBM security framework ensures that every IT security domain is properly addressed. All these frameworks, however, are yet to incorporate IoT security recommendations. As a result, approximately three-fourths of security professionals feel as though the current security standards insufficiently address IoT specific concerns (Lee & Lee, 2015).

Other more technical approaches take aim at what security procedures and techniques should be implemented when developing these devices. First, a secure boot must be performed each time the device is turned on or activated. This is most likely done through proper cryptography methods. Next, proper authentication is essential through the use of strong passwords (at minimum) or better yet the use of X.509, an encryption authenticator, or Kerberos, another method of properly verifying the user (IBM, 2015). Once the device and the user have been authenticated, secure communication must occur by the transmission of the data through secure encryption channels (SSH or SSL) (IBM, 2015). When done right, encryption can be extremely secure, however, there are many older forms of encryption that are less secure but popular to implement because of their simplicity. Lastly, protection against cyber-attacks and intrusion detection mechanisms must also be done through the use of firewalls that limit communication to only known, trusted hosts (IBM, 2015). Additionally, embedding a device designed to detect and report invalid login attempts and other malicious activities (IBM, 2015). Last, but not least, the U.S. Federal Trade Commission (FTC) notes that only basic, static security approaches cannot adequately secure an IoT device. It recommends that all devices be designed with continuous security procedures updates in mind, as security problems and solutions are always evolving (FTC, 2015).

At present, IoT security is implemented mostly through a self-regulation process – with some companies choosing strong security features, and others skimping or lagging behind on security requirements, which can result in harm and potential misuse of the device (Symantec, 2016). However, there are emerging questions regarding the role governments should play in these complex issues. Several authors make calls for better understanding the legal and regulatory issues around IoT. Data protection and privacy laws related to specific types of data interfere with IoT on a daily basis. In the European Union (EU) the EU Data Protection Directive is influencing the processing of personal data (Weber, 2015). Similarly, in the United States there are regulations—such as the Health Insurance Portability and Accountability Act (HIPAA)—that have an effect on data collection techniques (Weber, 2015). The areas of conflict lie that the raw data collected by IoT devices are not necessarily personal as a specific individual is not identified, yet through a combination of analytical and detective methods an individual may be able to be identified (Weber, 2015). As IoT devices continue to be installed and collect data automatically, the risk of non-compliance with these personal and data protection laws only amplifies. However, the legal ramifications have not yet become clear. There is a lack of international laws and regulation surrounding IoT resulting in self-regulation among the developing companies as the regulatory agenda has not entered the IoT sphere (Weber, 2015).

To foster developments in this area, the EU has been funding several cross-country projects focus on developing a trustworthy IoT environment to protect the security and privacy of European citizens by analyzing the IoT governance, privacy, security, and ethical issues (IERC, 2015; Vermesan et al., 2015). In the US, there are calls for action that devices and the networks that connect them need to be more secure – and that the government should set higher standards for IoT device security (Risen, 2016). To this end, the FTC is currently working with the technology industry to develop privacy and security safeguards without stifling innovation (Risen, 2016).

## TOWARDS AN INTEGRATED IOT SECURITY FRAMEWORK

Our review of academic and practitioner literature indicates that clear, independent, and comprehensive IoT security guidelines are sorely needed. Next, we propose a solution to this problem by discussing five key elements we believe will be required in order to build an integrated IoT security framework: security levels, security activities, security value chain, security standards, and security education.

**IoT Security Levels.** We propose that IoT security needs to be part of the design at the physical hardware, network, and application levels. *First*, the IoT device itself needs to be designed using security principles. This covers the sensors that capture data, the data storage mechanism, and the micro-controller or actuator capable of controlling the device behavior, processing data and establishing a network connection. A key challenge at this level is the fact that IoT devices have important limitations as compared to other computer-based devices – such as limited storage capacity and, if available, processing capacity, lack of battery for passive devices or limitations to "always on" processing for active, battery-powered devices. There is also a variety of IoT device configurations, and as a result there is large variation in capabilities these IoT devices have for secure operation (Ardiri, 2014; Cisco, 2016; Xu et al., 2014). Thus, security needs to be considered at the device design phase, and be embedded in the hardware (Xu et al., 2014). *Second*, the connections between the device and the network need to use secure technologies. The

connections can take many forms – directly from the device to the Internet, from the device to a gateway, or peer-to-peer among devices (IBM, 2015). The key challenges for securing the network connections again stem from the device limitations mentioned above, which make it difficult to use the well-established secure network protocols available for traditional computer connections. Therefore, new protocols developed especially for IoT device communication are required (Ardiri, 2014; Xu et al., 2014). *Third*, the software applications used to manage the IoT device need to incorporate security features that are appropriate for the device limitations described above but strong enough for ensuring the security of the software. Several such features are described in the next paragraphs.

**IoT Security Activities.** We further propose that IoT security needs to incorporate several essential activities: identification, authentication, authorization, and monitoring. *First*, IoT devices require secure identifiers – such as serial numbers – that can be traced back to the device manufacturer and uniquely identify devices. This concept is widely used for access control for people and applications in existing security frameworks (IBM, 2010), and should be extended to IoT devices as well. Identifiers can be linked to permissions schemes that define how the device is allowed to interact with its environment, and these permissions can be changed dynamically – either by users or if the device is compromised during a security breach. Determining the appropriate identification scheme and secure ways of assigning identifiers to devices is essential for establishing a secure IoT environment. *Second*, secure authentication mechanisms are required to establish a connection between the IoT device and the network (Cisco, 2016), as defined in the IoT Security Levels element above. *Third*, authorization mechanisms (Cisco, 2016) need to be implemented so that the device allowed behavior during actual use can be determined based on the identity of a device and its associated permissions. *Fourth*, monitoring activities need to take place to identify unusual patterns in the data provided by the IoT devices and identify potential security breaches (Cisco, 2016; IBM, 2015).

**IoT Security Value Chains.** We also propose that IoT security needs to permeate the entire value chain for the IoT solution. The value chain, a term originally coined by Michael Porter of the Harvard Business School, is now widely understood as the set of activities required to design, source, manufacture, deliver, use, and support a product. As mentioned above, the design of the IoT solution – including its hardware architecture, network connection protocols and software applications – needs to consider security as an important design requirement. The sourcing of materials and knowledge - physical components of the hardware devices and developer resources for software programming – needs to take place through a trusted supply chain (IBM, 2015; IoTSF, 2016). The manufacturing of the physical devices needs to include secure assignment and registration of appropriate identifiers for each device, while the development of the network communication mechanisms and of the software applications needs to include functionality to support the IoT Security Activities (as described in the previous paragraph). The delivery of the solution to the end user(s) needs to be done in a secure environment. Testing for both hardware and software security features (IBM, 2015) is also a key element of the manufacturing and delivery stages. The usage phase needs to allow, among others, for security breach monitoring, data analysis (for identifying abnormal patterns), and subcomponent isolation (in case of confirmed security breaches) (Cisco, 2016; IBM, 2015). Last, but not least, the support phase needs to implement secure mechanisms for the maintenance (IBM, 2015), return, replacement, recycling or re-manufacturing of the IoT solution or any of its components (hardware or software). The ultimate goal is to established a supply chain of trust (IoTSF, 2016) or trusted ecosystem (IBM, 2015) that can allow IoT solution providers to identify trusted partners and provide trusted solutions to others.

**IoT Security Standards.** An important element of the IoT security environment is the establishment of standards that companies can apply for their IoT solutions. *First*, even if the number of different IoT hardware configurations is exploding, standards for hardware interfaces and for secure IoT network communication can be established to ensure interoperability. *Second*, standards for securing the micro-controller part of the application can be developed building on industrial control knowledge from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), the International Society of Automation (ISA), and others (Kovacs, 2016). *Third*, standards for IT governance need to be updated to include specific IoT recommendations. For example, the COBIT standard (Wal et al., 2012) should incorporate principles specific to the use of IoT devices in and by enterprises – including principles for the governance of the hardware, network and software components of the IoT solutions for all COBIT processes ("Evaluate, Direct and Monitor," "Align, Plan and Organize," "Build, Acquire and Implement," "Deliver, Service and Support," and "Monitor, Evaluate and Assess") (Wal et al., 2012). As the readers may notice, there are parallels between the security value chain activities we discussed earlier and the COBIT processes, and we see opportunities for developing an integrated framework that combines these two perspective and applies them

specifically to IoT. Last, but not least, we recommend more transparency, communication and collaboration between emerging IoT security standards-making bodies. Organizations such as the IoT Security Foundation (IoTSF) and the Industrial Internet Consortium (IIC) are currently working on their own IoT security frameworks (IIC, 2016; IoTSF, 2016). However, we believe that sharing information and joining efforts will create the required critical mass to ensure sufficient comprehensiveness and wide adoption of the emerging standards.

**IoT Security Education.** We believe that the successful implementation of our previous security recommendations in the IoT security areas discussed above (solution levels, activities, value chains, and standards) depends heavily on educating professionals who are currently working or will work in the IoT space about security requirements. In the Information Systems community, there is already a recognition from students, recruiters and faculty members that security is one of the most important elements of foundations information systems courses (McCoy et al., 2015). However, according to an analysis of popular textbooks, security is not presented as a functional requirement during systems analysis and design training (Salisbury et al., 2015). If developers are not aware that they have to design for security, they expose the information systems they develop and the associated data to significant security risks that are harder to mitigate after development has ended. As we discussed in the IoT Security Levels element of our framework, designing for security is a best practice at all IoT solution levels – not just the application, but the hardware and network levels as well. Thus, we recommend that educational programs in all areas relevant to IoT, such as information systems, computer science, electrical engineering, industrial engineering, and automation and control, among others, should include broad coverage of IoT security topics in general and in-depth coverage from each area's perspective. In addition, current curriculum standards need to be updated to incorporate IoT security.

## CONCLUSIONS AND FURTHER RESEARCH

Current research has taken one of several major approaches when addressing the IoT security issue. The first route is stating that IoT has unlimited potential, but also has several residual risks - one of which is security. These authors simply state that IoT security is an issue and state reasons why including identity theft, data breaches, and hackings. The end of these articles is typically a call to action that states developers need to consider security when developing new products or that information technology professionals will be required to address upcoming security concerns. However, these articles typically offer no solutions or ways in which security can be improved. Another angle typically explored focuses on technical solutions to IoT security. Due to the fact that these papers are more specialized in nature, the managers and users concerned with IoT security may have difficulty in understanding how to actually apply the solutions in their environment. Last, but not least, there is an emerging regulatory angle that looks at how and why governments should develop IoT security standards. Our analysis suggests that there are three major gaps in each one of these areas: a lack of security in current IoT implementations, a lack of detailed, specific IoT guidelines in current IT security standards, and a lack of IoT laws and regulation at the country and international level. Overall, we find that although experts agree IoT security is extremely important, businesses in the IoT space, developers working for these companies, users of their IoT solutions, and regulatory agencies are slow in implementing IoT security measures. To address these gaps, we propose an IoT security framework that highlights key security requirements in five areas: security levels, security activities, security value chain, security standards, and security education.

Future academic research can advance our understanding of the gaps identified in this paper, of the technical, economic, and adoption barriers for IoT security practices, and the challenges of developing and adopting security standards. We are currently exploring some of these issues in ongoing research. Researchers can also study how to explicitly incorporate security considerations into business model frameworks for IoT (Dijkman et al, 2015). From a practical perspective, businesses focused on the IoT market and their employees need to understand the extent of the IoT security risks and the possible solutions, and to start implementing these solutions and test their effectiveness. Ultimately, we believe that joint action on the part of the IoT solution providers, businesses using IoT devices, consulting companies, regulators, and educational institutions will be needed to place security at the forefront of the IoT conversation and develop concrete security solutions for IoT.

**ACKNOWLEDGEMENTS**

Matthew Ahlmeyer's research was supported in part by a UTC Honors Research Fellowship.

**REFERENCES**

Accenture (2015). Security call to action. Available: https://www.accenture.com/t20160122T014933__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents22/Accenture-Security-Call-to-Action-IOT.pdf#zoom=50.

Ardiri, A. (2014). Is it possible to secure micro-controllers used within IoT? *Evothings*. Available: https://evothings.com/is-it-possible-to-secure-micro-controllers-used-within-iot/.

Cisco (2016). Securing the Internet of Things: A proposed framework. Available: http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

Dijkman, R. M., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management, 25*(6), 672-78.

Ebersold, K., & Glass, R. (2015). The impact of disruptive technology: the Internet of Things. *Issues in Information Systems, 16*(IV), 194-201.

FTC (2015). Careful connections. Available: https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

Folk, C., Hurley, D. C., Kaplow, W. K., & Payne, J. F. X. (2015). The security implications of the Internet of Things. *AFCEA International Cyber Committee*. Available: http://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf.

French, A. M., & Shim, J. P. (2016). The digital revolution: Internet of Things, 5G, and beyond. *Communications of the Association for Information Systems, 38*(1). Available : http://aisel.aisnet.org/cais/vol38/iss1/40.

Hodgson, K. (2015). The Internet of [Security] Things. *SDM Magazine*. Available: http://www.sdmmag.com/articles/91564-the-internet-of-security-things.

IBM (2010). Introducing the IBM security framework and IBM security blueprint to realize business-driven security. Available: www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf.

IBM (2015). IBM point of view: Internet of Things security. Available: http://public.dhe.ibm.com/common/ssi/ecm/ra/en/raw14382usen/RAW14382USEN.PDF.

IERC (2015). IoT Governance, Privacy and Security Issues. *European Research Cluster on the Internet of Things*. Available: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

IIC (2016). The Industrial Internet Consortium's approach to securing industrial Internet systems. Available: http://www.iiconsortium.org/pdf/IIC_Approach_to_Securing_Industrial_Internet_Systems.pdf.

IoTSF (2016). Press release: Internet of Things Security Foundation drives plan for the supply chain of trust. Available: https://iotsecurityfoundation.org/press-release-internet-of-things-security-foundation-drives-plan-for-the-supply-chain-of-trust/.

Kovacs, E. (2016). IT, OT collaboration key to securing industrial networks. *SecurityWeek.com*. Available: http://www.securityweek.com/collaboration-between-it-ot-teams-key-securing-industrial-networks.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-40.

McCoy, S., Everard, A., & Jones, B. M. (2015). Foundations of information systems course content: A comparison of assigned value by faculty, recruiters, and students. *Communications of the Association for Information Systems, 36*(1). Available: http://aisel.aisnet.org/cais/vol36/iss1/35.

Ranger, S. (2016). Internet of Things: Finding a way out of the security nightmare. *ZDNet*. Available: http://www.zdnet.com/article/internet-of-things-finding-a-way-out-of-the-security-nightmare.

Risen, T. (2016). The privacy, security risks of the Internet of Things. *U.S. News & World Report*. Available: http://www.usnews.com/news/articles/2016-01-22/the-privacy-security-risks-of-the-internet-of-things.

Rouse, M. (2014). Internet of Things (IoT). *TechTarget*. Available: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

Salisbury, W., Ferratt, T. W., & Wynn, D. (2015). Issues and opinions: Assessing the emphasis on information security in the systems analysis and design course. *Communications of the Association for Information Systems, 36*(1). Available: http://aisel.aisnet.org/cais/vol36/iss1/18.

Schneier, B. (2014). The Internet of Things Is wildly insecure - and often unpatchable. *Wired.com*. Available: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

Symantec (2015). An Internet of Things reference architecture. Available: https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf.

Turner, M. (2015). How to secure the Internet of Things. *ComputerWeekly*. Available: http://www.computerweekly.com/opinion/How-to-secure-the-internet-of-things.

Veracode (2016). The Internet of Things: Security research study. Available: https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf.

Vermesan, O., Friess, P., Guillemin, P., Giaffreda, R., Grindvoll, H., Eisenhauer, M., Serrano, M., Moessner, K., Spirito, M., Blystad, L-C., Tragos. E. Z. (2015). Internet of Things beyond the hype: Research, innovation and deployment. *European Research Cluster on the Internet of Things*. Available: http://www.internet-of-things-research.eu/pdf/Internet%20of%20Things%20beyond%20the%20Hype%20-%20Chapter%203%20-%20SRIA%20-%20IERC%202015_Cluster_%20eBook_978-87-93237-98-8_P_Web.pdf.

Wal, K. V., Lainhart, J., & Tessin, P. (2012). A COBIT 5 overview. *ISACA Webinar Program*. Available: www.isaca.org/cobit/documents/a-cobit-5-overview.pdf.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627.

Weinberg, B. D., Milne, G. R., Andonova, Y. G. & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624.

Xu, T., Wendt, J. B., & Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose CA USA, 417 – 423.