https://doi.org/10.48009/4_iis_2020_92-102

*Issues in Information Systems*
*Volume 21, Issue 4, pp. 92-102, 2020*

# A COMPARATIVE ANALYSIS OF BUSINESS AND NON-BUSINESS STUDENTS AWARENESS OF IOT DEVICES AND SECURITY PRACTICES: AN EXPLORATORY STUDY

***Queen E. Booker, Minnesota State University Mankato queen.booker@mnsu.edu***
***Carl M. Rebman Jr., University of San Diego, carlr@sandiego.edu***
***Hayden Wimmer, Georgia Southern University, hwimmer@georgiasouthern.edu***

## ABSTRACT

*The Internet of Things (IoT), through its interconnected devices, are designed to make our lives easier. Many students own and consistently use smart devices that are part of the IoT family. However, this ease of use comes with security issues such as lower encryption, authentication and identity management. This study examines student awareness of IoT devices and security practices for protecting oneself when using them. The study finds that students are largely unaware of devices that are considered part of IoT or what are the security best practices. The implication from the exploratory study is that educational opportunities should be added to the curriculum to ensure students across the University are aware of both technologies as they may someday be a consumer or developer of IoT technologies.*

**Keywords:** Internet of things, IoT devices, Security, Best Practices, Awareness

## INTRODUCTION

The term "Internet of Things" (IoT) (Atzori et al, 2010) refers to the network of dedicated physical objects ("things") that not only have the ability to communicate with other "things" through the Internet but also collect and exchange data. The IoT term was first brought up in 1999 by Kevin Ashton, who was the cofounder of the Auto-ID Labs at MIT (Razzaq et al, 2017). The internet of things (IoT) is a catch-all name for the growing number of electronics that aren't traditional computing devices, but are connected to the internet to send data, receive instructions or both (Fruhlinger, 2020). IoT encompass many different industries, healthcare, manufacturing, transportation, construction, and consumer electronics. Figure 1 illustrates the large scales uses of IoT( https://priceonomics.com/).

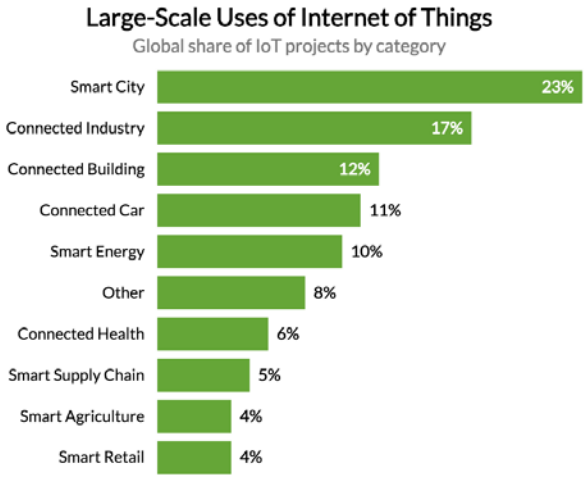


**Figure 1.** Large-Scale Uses of Internet of Things

IoT devices include wireless sensors, software, actuators, and can be embedded in to industrial equipment, environmental sensors, medical apparatus, and mobile phones (ARM, 2020). According to Statista, there were 22 Billion IoT devices in use in 2018 and that number is expected to increase to 50 billion in 2050 (Statista, 2020). According to Priceconomics.com annual revenue from IoT sales is forecast to hit $1.6 trillion by 2025 (from just $200 billion today and the amount of data produced by Internet of Things is expected to reach 4.4 zettabytes by 2020, from

just 0.1 zettabytes in 2013.The growth in the number of devices and the speed of that growth presents challenges to our security and freedoms as we battle to develop policies, standards, and governance that shape this development without stifling innovation (Maple, 2017).

According to the United States' National Initiative for Cybersecurity Careers and Studies (NICCS), these physical objects fall into one of three categories (NICCS, 2020):

1. Things that collect and send information (e.g., GPS sensors collect and send data on your location)
2. Things that receive and act on information (e.g., remotely unlocking your car)
3. Things that do both (e.g., vehicle sensors tracking positioning on the road, and alerting the driver when the vehicle strays outside of its lane)

IoT devices are more commonly known as "smart" devices and range in complexity. In the higher education environment, students use smart assistants like Siri and Alexa to assist with homework as well as other day to day activities, Internet connected doorbells and smart devices such as phones and watches that track homework due dates, meetings and other events deemed critical to their college success. These connected devices provide ease and convenience to life. This constant connection does have a downside. Unsecure networks can leave IoT devices vulnerable to cyber-attacks and provide cybercriminals access to sensitive information. However, there are practices that people can engage that can reduce those vulnerabilities. The NICCS (2020) provides a list of five such practices which are:

1. Change your device's factory security settings from the default password. This is one of the most important steps to take in the protection of IoT devices. Create a unique, complex password for each IoT device.
2. Update your devices with security patches. Even the simple act of regularly rebooting devices helps protect them, as malware is often stored in the temporary memory of a device and is removed upon reboot.
3. When connecting IoT devices to a network, consider connecting them to an isolated network that does not connect to computers storing valuable data.
4. Use a firewall to monitor the network traffic between the Internet connection and the IoT device. A firewall can detect unusual or suspicious behavior and prevent hackers from accessing devices on the same network.
5. Decide if there is a need to enable Internet connectivity on all devices. Just because a device has the capability to connect and interface with a network does not necessarily mean it should.

The number of IoT enabled devices increased the need to speed in transmission of messages or information and has led to the development of less secure Internet protocols. One such example is MQTT, which is a protocol for machine-to-machine and Internet of Things deployments but does not use encryption when communicating. Another challenge is that different IoT application fields have different industry standards which makes it difficult to adopt integrated security frameworks (Macedo et al, 2019).

As the number of connected "things" grow, students will not only become consumers of more of these devices, but they will also be engaged in the development of said devices. For example, engineering students will design smart cities, smart cars, and more smart consumer devices. Businesses will capitalize on data from smart health devices, smart watches etc., and a myriad of many applications that can improve life quality in society. Figure 2 illustrates the ownership rate of connected in the US in 2017 (http://statistia.com).

All these applications will lead to an increased amount of data that can be obtained from things, which will help with decision making processes. (Macedo, et al, 2019) The benefits that come from the data collected is shared with the responsibility of protecting data access and keeping the information secure from tampering or theft. If anything on a system is compromised, businesses can suffer financial loss as well as cause harm to the consumer. Thus, knowing best practices and the vulnerabilities in existing IoT technologies are important for all students who may engage in future technological developments and implementations. Knowledge of consumer-based IoT security best practices may also help enable awareness when making decisions about security used in development of or improvement of IoT devices. Knowing and following best practices can help drive improvements in device security and selections of protocol

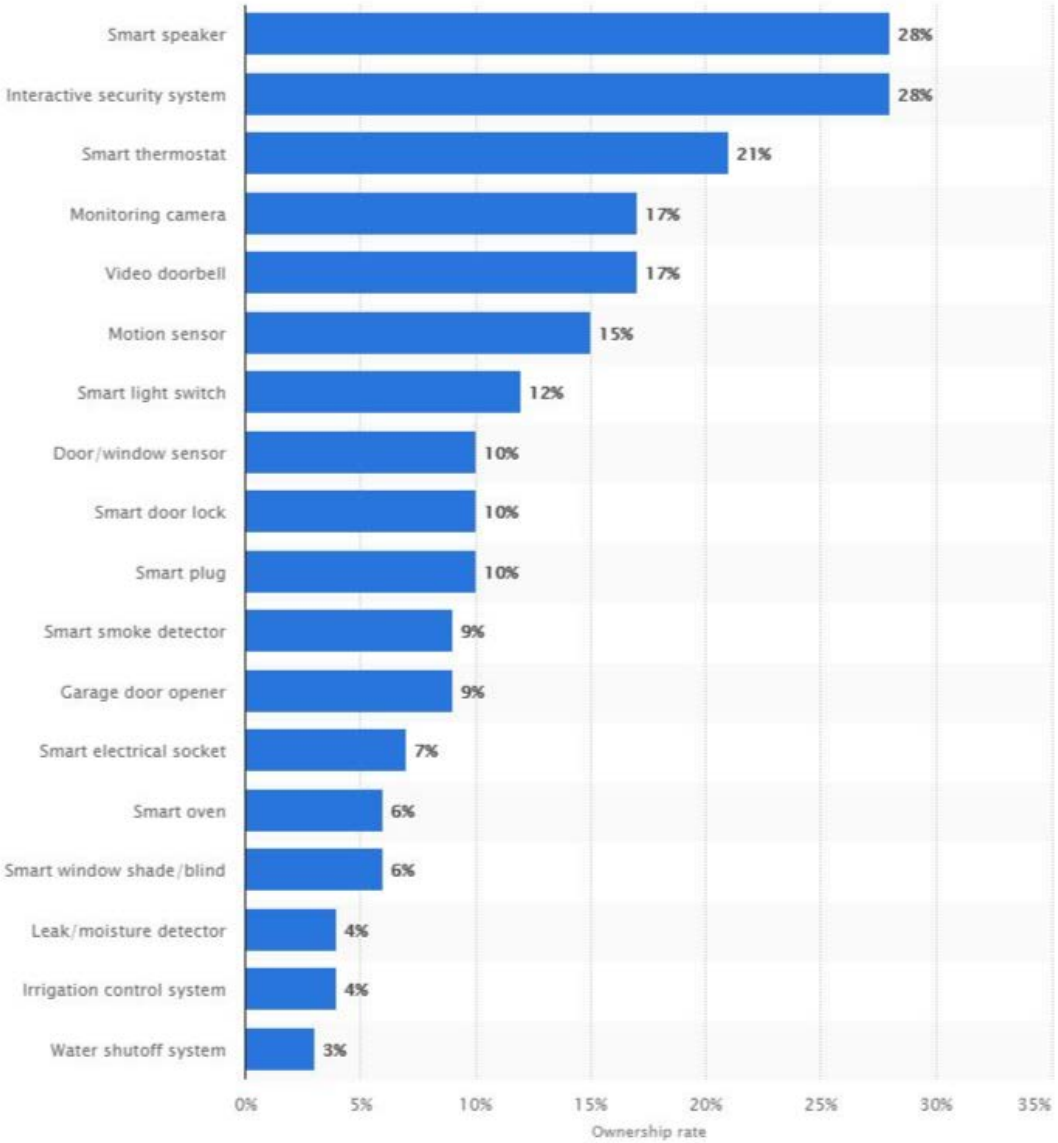


**Figure 2**. Ownership Rate of Connected Devices

This study explores student awareness of IoT technologies and use of IoT best practices and compared awareness between business students and non-business students.

This study contributes to the field by providing a process to assess the knowledge students possess regarding IoT technologies and security practices. It also provides insight into how a broader student base can benefit from understanding IoT technology development. The paper continues with the following sections: a brief literature review of IoT and security issues, methodology, results, discussion of findings, limitations, conclusions, and references.

## LITERATURE REVIEW

According to Macedo et al (2019), the IoT, is an ecosystem composed of the merging of heterogeneous network technologies. As such the IoT inherits the same security problems from the networks it uses to achieve its communication goals. These include the traditional wired networks, wireless networks, mobile networks, and sensor

networks. But it also incorporates new issues derived from its very specific characteristics such as sensor devices and other lightweight devices that do not provide a high degree of information protection and security.

Since almost any physical object can be designed or redesigned to become part of the IoT, there is a large increase in the attack surface. Weight scales, mattresses, home utilities, smart-TVs and other day-to-day objects that were not designed with security issues in mind, by being networked are now posing vulnerabilities to be exploited by malicious users because it is quite difficult to manage identities considering the number of possibilities of devices!

Many studies have been presented that consider the security aspects of IoT devices. For example, Zhao and Ge examined (2013) security problems in IoT considering their characteristics concerning the application layer, network layer and perception layer . Khan et al (2018) examined current challenges on IoT security and presented solutions based on block-chain technology. Sfar et al. (2018) presented a roadmap of security in the IoT through a systemic and cognitive approach. Sicari et al (2015) identified concerns with IoT security among factors such as access control, and privacy, and focused on proposals that address security solutions and security middleware applied to mobile devices. Kouicem et al (2018) reviewed commercially available IoT frameworks and identified the security features and flaws of the different frameworks.

There were no recent studies examining student knowledge about IoT technology and security were found at the beginning of the study but there are many studies that examined students Internet or digital literacy. For example, Detlor et al (2011) potential salient factors of internet literacy and student demographics, and how that literacy could affect students achieving learning outcomes. Case and King (2017) found that students in general were unaware about Internet safety best practices, and college students were often victims of purchasing fraud. They recommended increasing education of students about the dangers of online activity. Case and King (2018) also studied the ethical behavior of students in the online environment and found students in the online environment often engage in unethical behavior online and such behavior could have implications for security and privacy concerns.

## METHODOLOGY

The study incorporated data gathering at a single mid-sized, Midwest, regional, comprehensive university. This study was performed during the 2018, 2019 and 2020 academic years. Data was collected in a sophomore level introductory business course that is required for all business students and for students in a wide range of undergraduate majors including but not limited to construction management, aviation, public management, entertainment management, engineering, information technology, arts management, ethnic studies, law enforcement and others as part of a course module on innovation and technology. Data was collected as part of a pre-quiz (“What do you already know?”) for the module. Students were allowed only one attempt but could see the correct answers after submission of the quiz. The twelve questions included in each quiz are shown in Table 1 and were based on information provided on the NICCS website and from other peer reviewed literature: Pre-Module Assessment Questions.

**Table 1.** Pre-Module Assessment Questions (questions are randomized)

| Question # | Question | Possible Answers |
|---|---|---|
| 1 | From the list below, choose the devices that can be considered an IoT device: | smart tv, a smart phone, a smart watch, a smart speaker such as Alexa, smart car, credit card, smart mattress, genetically modified foods, sneakers, lamps |
| 2 | Federal agencies can only access public user data, that is, data that is available to the public. | True/False |
| 3 | Information gathered by a smart device is not shared with anyone and is used exclusively to improve service from the company. | True/False |
| 4 | HTTP is a the most common standard protocol used to send data from an IoT enabled device to the company that collects the data. | True/False |
| 5 | MQTT is a protocol for machine-to-machine and Internet of Things deployments but it does not use encryption when communicating. | True/False |
| 6 | Hackers can gain access to common technological devices such as computers, laptops, tablets, and cell phones. | True/False |
| 7 | Hackers can gain access to technological devices such as a smart thermostat, baby monitor, outdoor security cameras, and/or TV. | True/False |
| 8 | An important step to take in the protection of IoT devices is to change the device's factory security settings from the default password. | True/False |
| 9 | Passwords for any device connected to the Internet should be unique and complex. | True/False |
| 10 | It is important to use a firewall to monitor the network traffic between the Internet connection and an IoT device. | True/False |
| 11 | It is important that the consumer connect an IoT device to the Internet so that it can operate. | True/False |
| 12 | It is safe to connect smart device (e.g., phone, watch) to open wi-fi connections whenever possible. | True/False |

The questions were included in random order with 18 out of 30 other module related questions. The demographic data for students regarding major is part of the data provided to faculty in the course enrollment worksheet. The data from the exercises and course enrollment worksheet were merged to create the dataset. After aggregating the data, t-tests were run to compare the business/non-business major responses in the comprehensive dataset. The question responses were coded as either correct (1) or incorrect (0). T-tests are a typical statistical process used to determine whether there is a statistically significant difference between the means in two unrelated groups. The two unrelated groups in this study are business versus non-business students. Questions 1, 3, 5, and 7 were used to measure IoT knowledge. Questions 8, 9, 10, 11 and 12 were used to measure awareness of IoT security best practices. Questions 2, 4 and 6 were used as baseline questions to ensure integrity of responses.

The main hypothesis was that there would be no significant difference in the knowledge about IoT technologies and security best practices between business and non-business students. Specifically:

***H1: There is no significant difference between knowledge of IoT technologies between business and non-business students.***

Because of the newness of IoT as part of curriculums, we expect students to have similar levels of knowledge about IoT technology. Given the current general understanding about IoT we expect that the overall knowledge about IoT technology to be low overall and in both groups of students.

***H2: There is no significant difference between awareness of IoT security best practices between business and non-business students.***

Because of the newness of IoT as part of curriculums, we expect students to have similar levels of knowledge about IoT security best practices. Given the current general understanding about IoT we expect that the overall knowledge about IoT security best practices to be low overall and in both groups of students.

## RESULTS

The objective of this study was to explore student awareness of IoT technologies and security best practices. The data was collected during six semesters. The number of respondents by major is shown in Table 2. Respondents by Semester. 902 students out of a total of 1,023 completed the assessment. Of the students not completing the assessment, 91 were business majors and the rest were nonbusiness majors.

**Table 2.** Respondents by Semester

| Semester | Number of Students Completing Assessment | Business | Non-Business |
|---|---|---|---|
| Fall 2017 | 158 | 104 | 54 |
| Spring 2018 | 135 | 91 | 44 |
| Fall 2018 | 150 | 115 | 35 |
| Spring 2019 | 145 | 118 | 27 |
| Fall 2019 | 143 | 101 | 42 |
| Spring 2020 | 171 | 120 | 51 |
| **Total** | **902** | **649** | **253** |

Although diversity demographics are not used in the study, they are provided to give context of the diversity of the students involved in the class. Because of the small number of diverse students, the information is not broken down by semester. Gender information is provided in Table 3, ethnicity information is provided in Table 4, and specific major for the respondents is shown in Table 5. Though a table is not provided, it should be noted that most business majors take the course in their sophomore year as it is required for admission to the major but non-business majors take the course as juniors or seniors as it is not a pre-requisite to completing the major.

**Table 3.** Gender Information

| Gender | Number of Students |
|---|---|
| Male | 489 |
| Female | 518 |
| Non-Binary | 16 |
| **Total** | **1023** |

**Table 4.** Ethnicity Information

| Ethnicity | Number of Students |
|---|---|
| International | 87 |
| Black/African American | 78 |
| Hispanic/Latino | 60 |
| Indigenous | 4 |
| Pacific Islander | 4 |
| White | 780 |
| No response | 10 |
| **Total** | **1023** |

**Table 5.** Detailed Major Information

| Major | Type | Number of Students |
|---|---|---|
| Finance | Business | 137 |
| Accounting | Business | 118 |
| Marketing | Business | 165 |
| International Business | Business | 22 |
| Management | Business | 207 |
| Aviation | Non-Business | 90 |
| Engineering | Non-Business | 63 |
| Information Technology | Non-Business | 54 |
| Public Management | Non-Business | 7 |
| Construction Management | Non-Business | 34 |
| Other | Non-Business | 5 |
| **Total** | | **902** |

Table 6 shows the correct responses by question number for business and non-business majors. It also shows the percent of students who selected the correct answers. The percent is based on the total population of that group, e.g., for Q1, the percent of students answering correctly for Business majors is based on 150/649, where 649 is the number of business majors completing the pre-assessment.

**Table 6.** Correct Answers by Major (Business/Non-Business)

| Question | Correct | Business-Correct | Non-Business-Correct | Percent of students answering correctly | |
|---|---|---|---|---|---|
| | | | | Business | Non-Business |
| Q1 | 329 | 150 | 179 | 23% | 71% |
| Q2 | 254 | 154 | 100 | 24% | 40% |
| Q3 | 356 | 316 | 40 | 49% | 16% |
| Q4 | 568 | 389 | 179 | 60% | 71% |
| Q5 | 137 | 36 | 101 | 6% | 40% |
| Q6 | 902 | 649 | 253 | 100% | 100% |
| Q7 | 345 | 185 | 160 | 29% | 63% |
| Q8 | 312 | 102 | 210 | 16% | 83% |
| Q9 | 154 | 126 | 28 | 19% | 11% |
| Q10 | 113 | 36 | 77 | 6% | 30% |
| Q11 | 251 | 92 | 159 | 14% | 63% |
| Q12 | 96 | 59 | 37 | 9% | 15% |

Recall that Questions 1, 3, 5, and 7 were used to measure IoT knowledge; and Questions 8, 9, 10, 11 and 12 were used to measure awareness of IoT security best practices. Questions 2, 4 and 6 were used as baseline questions to ensure integrity of responses. More than 50% of the business majors selected the correct answer for question 4 (60%) and that was the only question where most business majors selected the correct answer. For the non-business majors, more than 50% of the respondents selected the correct answers for questions 1, 3, 7, 8, and 11. This suggests that the non-business majors were fairly accurate in identifying IoT technologies and were not as accurate in identifying IoT best practices.

T-tests were conducted to compare the two groups and the results are shown in Table 7. As shown in the table, there are significant differences between the two groups with respect to their knowledge about IoT technologies and security best practices. That the non-business majors had more awareness of the IoT technologies may be influenced by the types of majors (e.g., engineering, information technology).

Although there are significant differences in their knowledge bases, the results indicate that neither group has a good understanding of IoT technologies or the security best practices. Recall the hypotheses:

***H0: There is no significant difference in the knowledge about IoT technologies and security best practices between business and non-business students. Specifically:***

***H1: There is no significant difference between knowledge of IoT technologies between business and non-business students.***

***H2: There is no significant difference between awareness of IoT security best practices between business and non-business students.***

Based on the t-test results, we reject the hypothesis and sub-hypotheses.

**Table 7.** T-test results.

| Question Number | Business/Non-Business Variances | t-Stat | t Critical two tailed | P(T<=t) two tailed |
|---|---|---|---|---|
| 1 | 0.18/0.21 | (14.39) | 1.97 | 0.00 |
| 2 | 0.18/0.24 | (4.51) | 1.97 | 0.00 |
| 3 | 0.25/0.13 | 10.88 | 1.96 | 0.00 |
| 4 | 0.24/0.21 | (3.13) | 1.96 | 0.00 |
| 5 | 0.24/0.24 | 5.46 | 1.97 | 0.00 |
| 6 | 0.0/0.0 | NA | NA | NA |
| 7 | 0.20/0.23 | (9.88) | 1.97 | 0.00 |
| 8 | 0.13/0.14 | (24.34) | 1.97 | 0.00 |
| 9 | 0.15.0.09 | 3.32 | 1.96 | 0.00 |
| 10 | 0.05/0.21 | (8.20) | 1.97 | 0.00 |
| 11 | 0.12/0.23 | (14.58) | 1.97 | 0.00 |
| 12 | 0.08/0.13 | (2.22) | 1.97 | 0.03 |

## LIMITATIONS AND FUTURE RESEARCH

This exploratory study compared knowledge about IoT technology and security best practices at one institution. In this study we provide the questions we used to measure student knowledge before introducing it in the course. The pre-assessment revealed that neither business nor non-business majors had a good understanding of IoT technologies or security best practices. However, this was one university and one course. Additional data needs to be collected at more schools and in different classes. Also, the questions used were based on information provided on the NICCS website and from other information systems textbooks and security literature. These questions need to be tested for validity before being used in a wider study.

Although the study itself is limited in terms of population and validity, it should begin a conversation about where and how much about IoT should be in the college curriculum. With IoT technologies being embedded in everything from mattresses to monitors, and with protocols like MQTT have less security than HTTP, students should be aware of IoT, its implications for their individual lives as well as for products they develop. As with current IoT technologies future developers are likely to favor protocols with better speed with an expectation that the end user will employ the proper technologies to keep themselves safe. In addition to further validating this instrument with other respondents, additional studies need to be made about intent to engage in security best practices with relation to IoT.

## CONCLUSION

The purpose of this exploratory study was to compare knowledge about IoT technologies and IoT security best practices between business and non-business major. The principles of management course was selected as the data collection course because it (1) includes a module on information technology, (2) is required for several technology based majors as well as all college of business majors, and (3) includes a submodule on innovation and disruptive technologies which lends well to a discussion about IoT. Although the t-tests found significant differences between the responses for business and non-business majors, the overall results indicate that neither group is particularly competent with regards to understanding IoT technologies or the security practices. The implication of this result, particularly the part about understanding the various protocols, is that as members of product development teams, they could potentially opt for less secure protocols such as MQTT in favor of speed while increasing vulnerabilities in

future products. Further, they themselves may create vulnerabilities in the workplace by their inadequate use of IoT security practices through lack of knowledge.

Although the module for this class discusses the security best practices and how many products are becoming IoT, later assessments in the course did not show a significant change in correct answers to the questions presented in this study. Do students feel that IoT technologies are more secure than they really are? Is the curriculum not effective in improving the awareness? Should there be more emphasis on IoT in the introductory IT course required for all business majors? These are questions for future studies. As IoT becomes more pervasive, it is important that students understand IoT both as consumers and as product developers.

## REFERENCES

ARM, definition of Internet of Things https://www.arm.com/glossary/iot-devices accessed 9 June 2020

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Case, C. J., & King, D. L. (2017). A LONGITUDINAL ANALYSIS OF UNDERGRADUATE STUDENTS'INTERNET SECURITY PERCEPTIONS AND PURCHASING BEHAVIOR. *Journal of Business and Behavioral Sciences*, *29*(1), 57.

Case, C. J., & King, D. L. (2018). Ethical Attitudes and Behavior of Undergraduate Business Students: Trends and the Role of the Electronic Resources Policy. *Journal of Business and Behavioral Sciences*, *30*(2), 75-88.

Detlor, B., Julien, H., Willson, R., Serenko, A., & Lavallee, M. (2011). Learning outcomes of information literacy instruction at business schools. *Journal of the American society for information science and technology*, *62*(3), 572-585. https://doi-org.ezproxy.mnsu.edu/10.1002/asi.21474

Furhlinger, J. (2020) https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.

Macedo, E. L., de Oliveira, E. A., Silva, F. H., Mello, R. R., França, F. M., Delicato, F. C., ... & de Moraes, L. F. (2019). On the security aspects of Internet of Things: A systematic literature review. *Journal of Communications and Networks*, *21*(5), 444-457.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155-184.

NICCS, Securing the Internet of Things (https://niccs.us-cert.gov/featured-stories/securing-internet-things-0) accessed 5 31 2020

Ng, C. K., Wu, C. H., Yung, K. L., Ip, W. H., & Cheung, T. (2018). A semantic similarity analysis of Internet of Things. *Enterprise Information Systems*, *12*(7), 820-855.

Priceonomics (2020) https://priceonomics.com/the-iot-data-explosion-how-big-is-the-iot-data/ Accessed 9 June 2020

Psannis, K. E., Xinogalos, S., & Sifaleras, A. (2014). Convergence of Internet of things and mobile cloud computing. *Systems Science & Control Engineering: An Open Access Journal*, *2*(1), 476-483.

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(6), 383-388.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146-164.

Statistia.(2020) https://www.statista.com/statistics/802690/worldwide-connected- devices-by-access-technology/#:~:text=By%20the%20end%20of%202018,in%20use%20around%20the%20world accessed 11 June 2020

Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security* (pp. 663-667). IEEE.