**The commercial impact of cyber risk on the**

**Internet of Things (IoT)**

 Text

Description automatically generated

TEAM PROJECT

NAMES: PRAVEEN KUMAR MADDINENI (11601302),

VIJAY RAJ PATHANI (11609155)

INFO 5737

INSTRUCTOR: NAYANA PAMPAPURA MADALI

 

|  |  |  |
| --- | --- | --- |
| **Contents** | |  |
| **1** | Introduction | 3 |
| **2** | Background | 4 |
| **3** | Scope | 5 |
| **4** | The main objectives of this proposal are | 5 |
| **5** | A Concept Map of your final project | 5-6 |
| **6** | The Milestones of the Intervention | 7-8 |
| **7** | Case Studies | 9-10 |
| **8** | Types of Cyber-security threats the intervention seeks to monitor, stop, mitigate, or prevent | 11 |
| **9** | Utilization of surveillance in Industries | 11 |
| **10** | Surveillance in organizations | 11 |
| **11** | Prevention in platforms | 11 |
| **12** | Prevention in Organizations | 12 |
| **13** | Mitigation in platforms | 13 |
| **14** | Mitigation in Industries | 14 |
| **15** | Adoption of the Implementation of the Intervention and Target Audience | 14 |
| **16** | Benefits, Opportunities, Cost, and Risks | 15 |
| **17** | Benefits | 15 |
| **18** | Risks | 15 |
| **19** | Opportunity | 16 |
| **20** | Cost | 16 |
| **21** | Impacts or Practical Implications | 17 |
| **22** | Before | 17 |
| **23** | After | 17 |
| **24** | The commercial impact of cyber risk on the Internet of Things project proposal | 18 |
| **25** | Emerging Trends | 18 |
| **26** | Project Lessons Learned | 19 |
| **27** | Contribution | 20 |
| **28** | References | 20 |

**Introduction**

Cyber-security is the practice of protecting information systems from intrusions, attacks, or exploitation. The term "cyber-security" is often used to refer to protecting computer networks from malicious software and online threats. Cyber-security has become a hot topic in the digital world, and it is no surprise that it has come to the Internet of Things. The Internet of Things (IoT) refers to a network of physical devices that can interact with each other over the internet. These devices may be computers, phones, tablets, cameras, wearable technology, and distinct types of sensors (Jang-Jaccard & Nepal, 2014). For example, an IoT system could be connected to a bike's brakes so that if it detects that the brakes are applied, it can start tracking the rider's speed and distance traveled.

There are several ways in which IoT devices could become targets for cyber-attacks. First, they could be vulnerable to hacking attacks because they are connected to networks or the internet. Second, they could be susceptible to malware attacks if they have software vulnerabilities that allow attackers to take control of them. Third, they could be used as tools for espionage because they may have access to sensitive information about customers or employees. Fourth, they may contain personal information about users or data on their databases which can be exposed by hackers who gain access to these systems via their Internet Protocol addresses (IPs) (Farrell, 2015).

Cyber-security is a growing concern for businesses and individuals. The number of cyber-attacks has risen dramatically over the past few years, with no sign of slowing down. This makes it important for companies to understand how to prevent attacks in the first place and how to respond if they get attacked (Miller, 2022). In addition, cyber security interventions should be taken seriously because they present an opportunity for attackers to steal sensitive information from companies' networks, databases, and consumers who use IoT devices with little or no security measures against cyber security.

**Background**

IoT has introduced new challenges, such as cyber-terrorism and cyber warfare, which have increased the need for better security controls. The use of IoT has increased in recent years. According to a report by International Data Corporation (IDC), there were over 50 billion connected devices by 2020. This number is expected to increase further with the availability of more affordable devices that can be used worldwide. However, this growth poses a threat because it makes businesses vulnerable to cyber-attacks that can result in data loss or unauthorized access to sensitive information like financial data or intellectual property (IP). In addition to being vulnerable to external threats like malware attacks from hackers who may steal personal information about customers or employees, businesses also face internal threats like data breaches resulting from human error, such as configured incorrectly systems or weak passwords (Farrell, 2015).

Cyber-security interventions are an essential part of a business's risk management process. Cyber-security interventions cover a wide range of activities that help to protect and defend a company's assets from cyber threats. Cyber-security interventions include: performing threat analysis and risk assessment, implementing incident response plans, conducting penetration testing, which is a process where security professionals test the security of an organization's systems by trying to break into them, training employees on how to recognize and report suspicious activity on their devices, intending to prevent breaches before they happen (Miller, 2022) and developing policies and procedures for sharing information about cyber threats between members of the organization.

**Scope**

The scope of the cyber-security intervention is to ensure that the Internet of Things (IoT) will be secured and protected. The main task of this intervention is to safeguard and secure all devices connected to the internet. This includes industrial, consumer, and medical devices. This project aims to create an IoT solution to ensure these devices are safe from cyber-attacks.

**The main objectives of this proposal are:**

* To identify specific threats that could affect the security of our IoT project and propose solutions.
* Developing a plan for implementing our tool will not cause any damage to our project but will improve it to make it more secure.

**A Concept Map of your final project:**

**Diagram

Description automatically generated**

**Figure-1**

In the above CMAP has been clearly says about the Security Engineering. In this concept map (Figure 1), it has been mainly focused on the Security Architecture. I have connected the solution different cyber-security concepts that we learned about during this project. I have also included a brief description of what each component of the concept map entails and how it relates to one another.

The first component is "cyber risk assessment." This component refers to the process by which organizations assess their risk of being hacked or having sensitive information stolen. The second component is "cyber defense." This component refers to the process by which an organization protects itself from hackers and other bad actors. The third component is "cyber forensics." This component refers to collecting evidence after an attack has occurred, so that an investigation can be conducted into who was responsible for carrying out such an attack. The fourth component is "cyber threat intelligence," which refers to collecting information about potential threats before they become reality so that we can be prepared for them when they do occur (Farrell, 2015). Finally, the fifth component is "cyber incident response," which refers to how long it takes for an organization to recover once it has been hacked or victimized by a threat actor after it has been made aware of such an incident occurring within its walls via some form of communication channel, such as email, text messages, or phone calls. Security Architecture deals with cryptographic systems, principles, and design organization. Cryptographic systems can send messages that only the intended receiver can read, and they consist of a key, ciphertext, and encryption. It also includes principles such as design and architectural principles. It also includes vulnerabilities such as those in web-based, mobile, or embedded systems that we should be aware of to protect against them.

**The Milestones of the Intervention:**

Cybersecurity has evolved into what it is today: an integral part of every company's business model today. It has evolved from simple identity and access management to a comprehensive approach to the security of an organization's information assets (Paul, 2017). This evolution has been driven by several factors, including an increase in the number of devices connected to the internet, the emergence of new opportunities for attackers to exploit, and an increasing focus on mitigating risk within organizations.

The evolution of cyber security intervention is a major milestone in the evolution of the Internet of Things. The most significant developments in this area are the introduction of modern technology and devices, the increase in the number of connected devices, and the growth of data storage on these devices.

The internet has become a crucial part of our lives, and it can be accessed at any time by anyone. This makes it easy for the criminals to access sensitive data and commit crimes. The evolution of cyber security has been a major milestone in the history of internet and computing. The major milestone is the creation of the internet, which was created in 1969. The next major milestone was when computers were connected to the internet and became a part of everyday life. This was accomplished by 1991 when the World Wide Web was created. The next major milestone occurred in 1996 when companies started using email as part of their business structure instead of letters or phone calls. This allowed them to communicate with customers much more efficiently and effectively than before. Hackers started targeting computer systems by sending out emails with malicious links to their recipients (Nepal, 2014). This caused many computers across the world to crash, which results in a rise in cyber incidents.

As we entered the 21st century, there was a shift in how we thought about cybersecurity interventions. Instead of focusing on protecting our physical assets like buildings or cars, we began thinking more about protecting our digital assets like computers and mobile devices (Bryant & Pfeiffer). By this point in history, most information had been digitized and we could no longer afford to ignore cyber security threats because so much of our lives were being affected by them (Davies). In 2000, viruses were introduced into the market. These viruses could infect the hard drives on computers and cause them to crash or even destroy them completely if not detected quickly enough by security experts or antivirus programs on infected machines. In 2002, worms were created that spread through networks using email as their primary means of attack. These worms could cause widespread damage to networks that were not protected by firewalls or antivirus software (NIST). In 2004, spam frauds began targeting customers who used online banking services and other online services such as social media platforms like Facebook and Twitter; these frauds tricked people into revealing personal information (Miller, 2022).

In 2022, it is expected that the Internet of Things (IoT) is pervasive in every room of your house. It is possible to get anything you want delivered by an autonomous device that can be controlled via voice commands or via a smartphone app. As we enter this new era of technology with the advent of IoT applications and devices, we need to start thinking about how these modern technologies will impact our cyber security programs. What are the best practices for managing and securing these devices? How can we address potential threats?

As we look toward 2022, it is important to remember that cyber security has evolved significantly since 1996 and it is poised to continue evolving as modern technologies emerge. The evolution of cyber security intervention has been marked by two significant turning points (1996 and 2022). The first was the development of a new paradigm for cyber security: the Internet of Things. This new way of thinking about cyber security intervention has changed how we think about each individual device as a potential attack vector. It has also created new challenges for companies who want to protect their data and systems from outside threats.

The second milestone was the growth in threat actors' ability to use technology for malicious purposes. The first generation of threat actors were hackers who used technology as a tool--they did not understand it themselves or know how to use it maliciously. The second generation are hackers who know exactly what they are doing and have taken advantage of technological advances to create sophisticated tools that allow them to do more damage than ever before.

**Case Studies:**

According to a report by the Center for Strategic and International Studies, cyber-security is a complex problem that requires a unified effort from all levels of government and business. It is not just about protecting individual computers from hackers; it is also about protecting data from being stolen or corrupted and controlling access to critical systems. Therefore, we are seeing more companies sharing information about employee behavior and other sensitive information related to their employees' cyber security needs rather than keeping such information for themselves (Jang-Jaccard & Nepal, 2014). For example, suppose one company has been compromised by hackers before and lost essential data. In that case, another company can be more vigilant in protecting its systems by learning firsthand what happened to the first company.

In addition, the federal government has recently stepped up its efforts to tackle cyber risk in IT projects by requiring that companies disclose any vulnerabilities they find in their systems before they start working on them. These new regulations were implemented after it was discovered that some companies had failed to disclose these vulnerabilities when they were asked about them during an audit conducted by an auditor hired by the Department of Energy (DOE) (Paul, 2017). Therefore, cyber-security intervention is at individual-level, organizational level, and system levels.

Individual level: This is where you will find our users and how they use the internet. The more they use the Internet of Things, the more likely they will be vulnerable to cyber-attacks. For example, many devices are connected to the internet in a home environment, such as smart thermostats, cameras, or smart locks (Jang-Jaccard & Nepal, 2014). These devices have a lot of personal information stored on them, which hackers could use to steal from users, for example, by recording their conversations or stealing their credit card information.

Organizational level: This is where companies play an essential role in protecting against cyber-attacks by providing security solutions that can protect your business from any attack, including email hacks and data breaches (Farrell, 2015). Offering solutions to these types of attacks by providing effective countermeasures against hackers who try to penetrate their network by using various techniques, Malware frauds and spams, for example, can steal sensitive information from users' computers, such as usernames and passwords, making it easy for hackers to gain access to systems within their company network without being detected by management. And system level: When talking about system-level cyber security

**The types of Cyber-security threats the intervention seeks to monitor, stop, mitigate, or prevent.**

Cyber-security intervention seeks to monitor, stop, mitigate, and prevent cyber-security threats that can take down systems and applications. The types of cyber-security threats we monitor include but are not limited to malicious software (malware), vulnerabilities in system or application software, unauthorized access to data or information stored on the system, and attacks on network infrastructure. As part of this intervention, we also seek to mitigate risks caused by human error.

The intervention seeks to monitor, stop, mitigate, or prevent cyber-security threats by utilizing the following.

**Surveillance:** The intervention monitors and tracks cyber threats in real-time through automated systems.

**Prevention**: The intervention seeks to stop cyber threats before they happen by implementing preventive measures such as blocking or filtering malicious traffic (Miller, 2022).

**Mitigation:** The intervention aims to manage cyber-threats after they have occurred by implementing detective controls that can detect suspicious behavior and act on it before it becomes a full-fledged threat**.**

**Utilization of surveillance in Industries**

The commercial impact of cyber risk on the Internet of Things proposal is that it can be used to monitor, stop, mitigate, or prevent cyber security. The proposed solution will allow companies to use surveillance technology to monitor their networks and identify potential threats. This will enable them to act before a breach occurs to avoid costly damages and losses. The benefits of surveillance are many. For example, it allows industry to see what is happening to their systems and in the environment around them. This gives them an opportunity to respond quickly in case something goes wrong or needs fixing.

**Surveillance in organizations**

Surveillance allows an organization to understand how well they are doing at securing their systems. That way they know what areas need improvement and where there's room for improvement because there is now more visibility into what is happening within the network than ever before with traditional methods like logging in, among other examples (Jang-Jaccard & Nepal, 2014).

**Prevention in platforms**

A cyber security intervention in platforms can be defined as a system that monitors, stops, mitigates, or prevents cyber security attacks by utilizing prevention. There are many ways to achieve this goal. One of the most popular ways is through encryption technology. Encryption is used to protect data from being read and can be used to prevent unauthorized access to information (Miller, 2022). When this happens, it prevents hackers from stealing information like passwords or credit card numbers.

**Prevention in organizations**

The Internet of Things is a technology that connects everyday objects to the internet, allowing them to communicate with each other and with computers. This can introduce new vulnerabilities into the network, which could lead to cyber-attacks and data loss (Brown, 2019). The recent Equifax data breach and WannaCry ransom ware attack have highlighted how critical it is for organizations to have a comprehensive approach to cyber-security.

The first step in prevention is visibility, ensuring that all parts of your organization are aware of current threats and what needs to be done to prevent or mitigate them. This includes regular training on cyber security best practices as well as collecting data about potential vulnerabilities in your systems so you can assess whether they pose an immediate threat or not when compared against other organizations facing similar threats (e.g., those that have been targeted by ransomware attacks).

Prevention techniques include securing all devices on an enterprise network by installing antivirus software on each device and having a policy that requires employees to change their passwords every 90 days. Cybersecurity interventions are used by organizations such as banks, insurance companies, government agencies, retail stores, and other companies that deal with sensitive information such as credit card numbers and bank account numbers (Miller, 2022). Organizations should prevent cyber-security threats because prevention can help prevent future attacks by preventing hackers from gaining access to devices when they first become available on the marketplace or when users first begin using them.

**Mitigation in platforms**

To mitigate cyber-attacks on the IoT, companies should consider implementing security measures such as: a comprehensive threat detection platform that monitors all traffic entering and exiting an organization's network, a layered approach to security based on security levels and authentication methods employed by different apps/services running on a device, and a comprehensive patch management program that keeps software up to date with all security patches available (Jang-Jaccard & Nepal, 2014).

**Mitigation in Industries**

Cyber-security hazards mitigation works in industries such as healthcare and banking by ensuring that information is protected and that the right people can access it. In healthcare, this means ensuring that only authorized personnel have access to patient data. In banking, this means ensuring that only authorized personnel have access to customer information. In both industries, cyber-security risk mitigation includes encryption, authentication, and data loss prevention. These can all be used to prevent unauthorized access to sensitive data.

**Adoption of the Implementation of the Intervention and Target Audience**

The impact of cyber security on the Internet of Things is not only an issue that concerns the system owners, but also the service providers. The service providers will have to deal with the security issues related to their products or services whenever they are deployed in real-world situations (Brown, 2019). As a result, they may have to spend time and resources in developing and testing innovative solutions to improve their products' security.

It should be noted that many conferences and workshops are devoted to disseminating information about cyber security on the Internet of Things field, especially when protecting critical infrastructure systems. These workshops will be held at various events such as conferences and industry “meetings,” and through online content creation (webinars) on such issues as: what does it mean to be secure? How do you know when you are secure? How can I implement security measures within my product? And how can I make sure my customers are protected?

 Every year, several workshops are held to exchange information and ideas on cyber security matters related to the Internet of Things. Information on cyber security on the Internet of Things can be found in different conferences like CYBIO, it is a community for information security professionals, academics, and students. CYBIO is a forum for anyone with an interest in information security. It is a platform for researchers, professionals, and students to build their professional network and collaborate on research (Luke, 2021). This forum is the first and largest dedicated community of information security professionals, academics, and students in Israel.

**Benefits, Opportunities, Cost, and Risks**

**Benefits**

Cyber-security is important on the Internet of Things (IoT) project proposal. It can be used to detect and prevent cyber-attacks, which are becoming more common as devices become connected and people use them for more sophisticated tasks. This is especially important for IoT devices, which have traditionally been used for convenience rather than security.

The benefits of implementing cyber-security include increased security for IoT devices and data, reduced risk of cyber-attacks on IoT systems, better ability to identify threats within the network environment, it can keep hackers from accessing sensitive data stored on the IoT devices. Additionally, it helps companies prevent unauthorized access to their systems or networks by limiting what users can do with their devices and reducing downtime due to device failures by providing redundancy or resiliency mechanisms. Companies also benefit from reduced costs associated with monitoring devices remotely and by eliminating or reducing the need for human error during device setup and maintenance.

**Risks**

As the Internet of Things project continues to grow, so does the risk that the devices we use on a regular basis could become compromised by online criminals. This is a significant concern for many people, as it can lead to loss of personal information, financial fraud, identity theft, and damage to property (Hossain Faruk et al., 2022). By implementing a cyber-security intervention, we can help protect our customers from these risks and ensure they can continue using their IoT devices without worry.

The risks associated with implementing cyber-security measures include hackers will find vulnerabilities in the system before it is implemented and take advantage of them prior to any security measures being put in place; the device could be used by an unauthorized party to access other devices or systems (Hossain Faruk et al., 2022). And the network infrastructure could be compromised, resulting in interruptions in service for everyone on the network.

**Opportunity**

The Internet of Things project will provide cyber security to the world market by offering a secure, secure, and a reliable platform that can be easily integrated into existing systems and infrastructure. This will allow businesses to better protect their data from cyber-attacks and cyber criminals who may want to steal it. By using this platform, businesses will be able to use an open-source solution that they can customize according to their needs (Hossain Faruk et al., 2022). This means that they will be able to control the entire process from start to finish, allowing them to focus on their core business rather than worrying about security issues.

This approach would also encourage more people to join up with companies as they would have access to all the necessary tools needed for them to work properly within their environment without any hassles or complications whatsoever! The opportunity to increase efficiency by providing additional functionality that could result in greater productivity, profitability, or customer satisfaction and the opportunity to increase security by protecting critical infrastructure from cyber attacks

**Cost**

Cyber-security is a major issue on the Internet of Things project proposal. The cost of cyber-security intervention can range from $1 to $20 billion (about $62 per person in the US (United States)) per year, depending on what one is trying to protect against. Cost of cyber-security intervention is a significant factor in the success of the Internet of Things project. A successful cyber-security plan will require an investment in both human resources and technology that can be used to protect the project's intellectual property (Hossain Faruk et al., 2022). The cost of hiring security personnel, purchasing security software, and managing the security process is just one part of this equation; if these measures are not successful, then it may be impossible for a company to rely on its Internet of Things products in a meaningful way.

**Impacts or Practical Implications**

The following is a summary of the major findings regarding the effects/impacts before and after the implementation of the cyber-security intervention.

**Before:**

We found that there was a high rate of security breaches on the Internet of Things projects. The most common types of breaches were unauthorized access to data, denial of service attacks, social engineering attacks, viruses, worms, and Trojan horses. Before the intervention there were 36% of attacks with unauthorized access to data, 32% denial of service attacks, 16% social engineering attacks and 8% viruses, worms, and Trojan horses (Kiertzner, 2016).

**After:**

We found that there was a significant decrease in security breaches after implementing a cyber-security intervention. The most common types of breaches were unauthorized access to data, denial of service attacks, social engineering attacks, viruses and worms, and Trojan horses. After the implementation of the security measure only 10% of attacks were found to be unauthorized access to data. 25% were denial of service attacks, 18% social engineering attacks, 30% viruses/worms and 15% Trojan horses (Kiertzner, 2016).

**The commercial impact of cyber risk on the IOT project proposal:**

The two main findings of this study are: the commercial impact of cyber risk has been increasing over the last decade, and the effects of cyber risk on business operations have been more pronounced in the last few years, especially in terms of loss of revenue (Kiertzner, 2016).

**Future Trends**

Cyber-security is an emerging and future trend that will continue to be a major focus of the IoT project. As more devices are connected to the internet, the risks of cyber-attacks on these systems increase. A recent study found that the top three threats to the Internet of Things (IoT) were malicious code, human error, and natural disasters. In recent years, cyber-attacks have affected organizations ranging from small businesses to large corporations. In 2016 alone, hackers stole $1 billion (about $3 per person in the US) from global banks through online fraud. The Department of Homeland Security has also reported that cyber criminals make over $100 million per day from stealing credit card numbers used by consumers around the world (Luke, 2021).

As more devices become connected to the internet, they will become more vulnerable to cyber-attacks. This means that a company's business could be negatively impacted if it does not take steps to protect its information systems against these attacks. An emerging trend is that to improve device security, companies are using more advanced hardware and software systems (Paul, 2016). This includes using biometric technology such as fingerprint scanning or facial recognition software so that they can ensure that only authorized users have access to certain parts of the system. Another emerging trend is that companies are taking their data security more seriously by encrypting all their data and storing in offline until needed instead of just storing it online where anyone could easily access it without permission from those involved with its creation or dissemination (like social media sites).

**Project Lessons Learned**

In the initial stages of the cyber-security intervention project proposal, we learned that cyber-security is extremely important to a project's success. The way that cyber security is conducted within a company is quite different from the way it is done in other forms of business. To ensure that an organization can maintain its security and privacy standards, they must be able to detect incidents as soon as possible, respond to them quickly and efficiently, and prevent future breaches. The lessons we have learned are:

1. Cyber-security planning is crucial for any IoT project

2. Effective cyber-security training will help your employees understand how to react in case of an attack

3. The tools you use need to be easy enough for your employees or contractors to use

The project team also believes that there are lessons learned from this proposal that can be applied to future efforts to improve cyber-security posture:

- Ensure that one has a clear understanding of their critical infrastructure before initiating an intervention plan.

- Identify all parties involved with the critical infrastructure and establish trust relationships between them.

- Develop policies and procedures for monitoring critical infrastructure.

- Develop an automated system for sharing information across various locations.

- Build relationships between entities responsible for managing distinct aspects of critical infrastructures.

**Contribution**

This research project was conducted by Vijay Raj and Praveen Kumar. The introduction, background, scope, and milestones were written by both members to ensure they had a common consensus when drafting this paper. Once the research basis was formulated, Vijay Raj focused on the case studies, while Praveen Kumar focused on benefits, opportunities, costs, risks, impacts or practical implications, and emerging trends. Finally, the lessons learned were shared by Vijay Raj and Praveen Kumar. Since each research section had different lessons from the other.

**References**

Brown. (2019). *Software Security Framework: Engineering Secure Products*. <https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/sas-software-security-framework-107607>

Suresh, H., Hunt, N., Johnson, A., Celi, L. A., Szolovits, P., & Ghassemi, M. (2017). *Clinical intervention prediction and understanding with deep neural networks*. PMLR. Retrieved December 7, 2022, from <https://proceedings.mlr.press/v68/suresh17a.html>

Hossain Faruk, M. J., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022). A review of quantum cybersecurity: Threats, risks and opportunities. *2022 1st International Conference on AI in Cybersecurity (ICAIC)*. <https://doi.org/10.1109/icaic53980.2022.9896970>

Kiertzner. (2016, August 3). *How will Brexit impact cybersecurity?* SAS Voices. <https://blogs.sas.com/content/sascom/2016/08/03/post-brexit-cyber-security/>

Miller. (2022). *Cybersecurity: Prevention and intervention*. Champlain College Saint-Lambert. <https://www.champlainsaintlambert.ca/cont-ed-program/cybersecurity-prevention-and-intervention/>

Suresh, H., Hunt, N., Johnson, A., Celi, L. A., Szolovits, P., & Ghassemi, M. (2017). *Clinical intervention prediction and understanding with deep neural networks*. PMLR. Retrieved December 10, 2022, from <https://proceedings.mlr.press/v68/suresh17a.html>

Farrell. (2015). *Will control or reliability propel IoT in utilities?* SAS Voices. <https://blogs.sas.com/content/sascom/2015/04/09/will-control-or-reliability-propel-iot-in-utilities/>

Jang-Jaccard, J., & Nepal, S. (2014). [A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*](https://www.sciencedirect.com/science/article/pii/S0022000014000178), *80*(5), 973–993.

Paul. (2017). *Predictive analytics: What it is and why it matters*. SAS. Retrieved December 9, 2022, from <https://www.sas.com/en_us/insights/analytics/predictive-analytics.html>

Luke. (2021). The Internet of Things*: Understanding the Adventure*. <https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/ebooks/en/iot-understanding-adventure-110792.pdf>