Implementing IoT Security Policy for Tata Steel

By Timur Ozkul #999072

Abstract

Table of Content

Introduction

Do you know that possibly the things around you can jeopardize your privacy, safety, security? Organizations and individuals around the world are witnessing a profound change in their relationship to technology. The World Economic Forum has described this transition, as the Fourth Industrial Revolution, as a convergence of the physical, digital and biological worlds with extensive consequences for the economy and even humankind. These developments pose new opportunities and obstacles for policymakers, as the mechanisms and structures of conventional governance need to be reconsidered in a changing environment. IoT is defined at a high level as a decentralized network of devices, applications and services that can sense, process, communicate and take action based on data inputs, including control of physical world elements [AKN20]. The IoT environment is diverse in its applications, and users. The IoT consists of objects (e.g., tags, sensors, and devices) that link to the cloud through a network, often, from which data can be gathered, exchanged, and analyzed to generate value [BJSL17].
Many investors have taken notice of the opportunities in IoT and huge sums of capital have flooded the market. Whilst growth offers many opportunities, IoT is not yet mature or secure. This introduces a huge range of problems by adding millions of new computers, hardware endpoints, billions of lines of code, along with more infrastructure to support the load. Different industry reports show cybersecurity is the number one issue today for industrial IoT users.
As we increasingly rely on intelligent, interconnected devices in our lives, billions of "things" can endanger personal privacy and risk public security intrusion and interference.
Most of the security and privacy problems of IoT such as unauthorised access and weak or absent encryption schemes come from two main reasons, and also at the same time are the motivational factors for this project. IoT artifacts have limited computing power, memory and bandwidth capabilities. Due to these limitations, the direct implementation of conventional protection mechanisms in IoT objects without modifications appears to be very hard. Of this reason a new race of lightweight IoT security techniques and protocols have been and are being developed. The second factor is the lack of comprehensive generally recognized IoT protection and privacy policies and the correct mitigation techniques [ANCK19].
The Security Policies are the various measures and controls that get implemented for an effective information security management system [HE02]. Davis and Olson have defined security policy as "to establish limits of acceptable behavior, decision confines, and standards." in [KMMB09], p. 494. Security policies are one of the weaker links in the security chain. The greatest threats often come from within the organization themselves. By those uninformed employees with no malicious intent. Hence one of the favored tactics of cybercriminals is social engineering. In 2017, according to Kaspersky, 46% of cybersecurity incidents were due to careless uniformed staff. However, only 52% of businesses believe they are at risk from within, according to the same study [HU19]. One of the major aspects of protecting these IoT devices are the security policies. The third motivation for this dissertation subject comes from the implementation of an effective security policy that can have a tremendous effect on the security of an organization.

The overarching theme of this specification report is to create a plan for the dissertation topic on implementing IoT security policies for an organization called Tata Steel. Tata Steel is an Indian multinational steel-making company who have chosen to give more emphasis on their security of IoT devices. Hence, have collaborated with Swansea University to come up with solutions and one aspect of that is to establish security policies for their IoT devices. This specification report will entail background research on the areas of IoT, IoT security, IoT classifications, IoT security analysis, security policy, security policies for IoT. Description of the dissertation project, which includes the problem Tata Steel is trying to solve and what the final product will look like. Finally, the project plan, which will include a Gannt chart to demonstrate a time line and a risk analysis to calculate the risks associated with the project.

Background research

The Internet of things (IoT)

-- Note to self: reference IoT book and look for 4th industrial revolution papers

Although for a few years the term 'fourth industrial revolution' has been used, there are many meanings. Moving on from the third industrial revolution, also known as the digital revolution, the fourth industrial revolution offers new possibilities for technology and connected devices to be used in industry and society. In this digital revolution, certain emerging areas include IoT, robotics, machine training, artificial intelligence (AI), nano-technical engineering, quantum computing, and biotechnology. "Almost every aspect of business will be profoundly changed by digitization and the IoT. Efficiency will increase, quality will improve, innovation will accelerate, costs will drop. Companies late to adopt the fourth industrial revolution, digital enterprise or IoT techniques will be left in the dust by competitors that got it a bit sooner," according to Chuck Byers, CTO of OpenFog Consortium. The impact coincides with the sheer amount of IoT devices, its said that by 2030 we will be communicating with 125 billion of those devices [Ea19]
There is no interpretation of IoT widely agreed upon, partially because the term IoT does not simply reflect a new technological architecture but a conceptual idea that describes how we communicate with the physical world. IoT is defined at a high level as a decentralized network of devices, applications and services that can sense, process, communicate and take action based on data inputs, including control of physical world elements [AKN20].
The IoT environment is diverse in its applications, and users. The IoT consists of objects (e.g., tags, sensors, and devices) that link to the cloud through a network, often, from which data can be gathered, exchanged, and analyzed to generate value. Examples of items include appliances (from refrigerators to toasters), personal hygiene products (such as hair brushes3 and toothbrushes4), medical devices, cars, smart phones, smart highways, smart electrical meters and machinery, to name a few. These connected devices produce data which is shared and analyzed. IoT consists of consumers, companies, organizations, and other end-users who communicate with or depend on the stuff, data, networks, and services. The complicated nature of IoT is the reason why it is also unofficially coined as the Internet of Everything.

There'll be tremendous benefits for customers. The IoT transforms people's way of life. From equipment and services that make life more convenient (for example, applications that change temperatures or pre-heat ovens) to life-save devices (for example wireless infusion pumps and asthma management kits), consumer IoT devices allow "virtually all devices to connect to the Internet" [BJSL17].
Intelligent systems can manage the collection of ‘things’ that form an IoT ecosystem, which can autonomously connect to things to monitor and control them. In addition, these smart systems can gather data from a thing or group of things and process the data and gain valuable knowledge to make intelligent decisions [En17].
The data obtained from millions of IoT devices is so huge that it makes segregating and collecting valuable information from them difficult. To organize these unstructured data to form a coherent chunk of information, artificial intelligence (AI) based algorithms are used to eradicate useless data and optimize every business. Intertwined IoT-AI partnerships can help companies progress to the next level. IoT-AI applications allow businesses to avoid unplanned downtime, increase operational performance, spawn new products and services and improve risk management. AI is a natural complement to IoT implementations, allowing a competitive advantage. - Note to self: need to put fake reference
DHL leverages the innovative IoT solutions along with artificial intelligence creating a transport model that reduces drivers' tiredness and lets drivers spend less time on the road and provide a better balance between work and life. “By 2028, DHL aims to build 10,000 IoT-enabled truck transportation vehicles. It says AIoT has reduced 50% of their transit time with 90% reliability of real-time tracking” [Re20].
It is clear that these IoT technologies and services offer a tremendous benefit to human life, but they come with a significant cost to the protection of individual privacy and security.
This is because the IoT inherits most of the issues of the Internet related to location awareness, security, service quality and is most likely amplified considering they are directly link with physical objects [ANCK19]

The Security of IoT

The IoT incorporates vast amounts of new products that are distributed or installed within or inside an enterprise. Data obtained from these devices can then be analyzed and implemented. In certain situations, the systems deployed may perform other tasks. This research will require the establishment of previously unseen connections that can affect the privacy of individuals or groups of people. In certain cases, people may not even realize they are being watched or documented given the ability to embed virtually any platform in next-generation microchips. In all cases, it is necessary to ensure the security of each component of an IoT system so that malicious actors can not take unauthorized advantage of the power of the IoT.
The generation and processing of data is so important to the IoT that the security of data during its life cycle must be taken into account. It is difficult to handle information at this level as data moves through multiple institutional boundaries and with different policies and intentions. Individuals would undoubtedly have different privacy priorities than companies, which in effect

have different objectives than government or other organisations. Data are often processed or stored on edge computers that have extremely limited capacity and are vulnerable to advanced attacks. An edge system is any hardware that manages data flow between two networks [SGE15].

Despite the numerous technical and physical components of an IoT ecosystem, IoT should be thought of as a system of systems. This complexity poses challenges in keeping the IoT secure and can be the cause of organization IT systems being targeted through other other IT systems. The following are the challenges faced with the development of secure IoT ecosystems:

(a) Large attack surface: IoT-related threats and risks are complex and rapidly changing. Given its effect on the safety, protection and privacy of its people (data collection and processing may be opaque to users as IoT is focused heavily on data collection, sharing and processing from numerous sources including sensitive information), the threat landscape of IoT is extremely broad.
(b) Limited device resources: The implementation of traditional IoT security practices will require substantial reengineering due to technological constraints. Most of the IoT devices are limited in resources and advanced security measures can not therefore be used effectively.
(c) Complex ecosystem: Security concerns are compounded because IoT should not be regarded as an isolated set of devices, but rather as a complex, diverse and widespread ecosystem with aspects such as people, apps, communication and interfaces.
(d) Fragmentation of standards and regulations: Further complicating related issues are the fragmented and sluggish implementation of standards and legislation to direct the implementation of IoT security measures and good practices, along with the continuing increase in new technologies.
(e) Widespread deployment: In addition to IoT's commercial applications, recent developments have seen Vital Infrastructures (CIs) shift into smart infrastructure using IoT in addition to conventional infrastructure.
(f) Security integration: This is a very difficult activity because the views and expectations of all stakeholders can be conflicting. For instance, various IoT devices and systems can be based on various authentication solutions that are integrated and interoperable.
(g) Safety aspects: This is very important because of the existence of actuators that influence the physical environment. Safety threats can come from security threats.
(h) Low cost: The large adoption of IoT and its advanced applications in various critical fields suggests the potential for substantial cost savings by the use of features such as data flows, automated monitoring and integration. Conversely, the low cost, typically associated with IoT devices and systems, also has security implications. Manufacturers can be likely to restrict safety features to ensure low cost and product protection can not be covered against other forms of IoT attacks.
(i) Lack of expertise: It is a relatively new area, and so people with the necessary skills and experience in IoT cybersecurity are missing.
(j) Security updates: It is exceedingly difficult to apply security changes to IoT, as the unique features of the user interfaces available to users do not permit conventional

updating processes. Securing such mechanisms is a daunting task in itself, particularly with regard to over-the-air updates.

(k) Insecure programming: Since the burden of quick delivery for IoT devices is higher than in other fields, it puts limits on the efforts available to improve protection and privacy by design. For this reason, and often because of budget issues, IoT companies usually concentrate more on functionality and usability than on security.

(l) Unclear liabilities: The absence of a consistent assignment of liabilities could lead to ambiguities and conflicts in a security incident, in particular in view of the broad and complex IoT supply chain. Therefore, it remains unclear how to handle safety if one element was shared by multiple parties. Liability compliance is another big concern [En17].

The myriad of security challenges faced with IoT has created “fertile ground” for cyber attacks. In October 2016, the world had seen the largest and most disruptive distributed denial of service (DDoS) attacks through the use of botnets on IoT devices. The Mirai malware had targeted a domain registration services provider, Dyn (which support major Internet platforms and services such as PayPal, Twitter, VISA, etc.). The way Mirai attacked the IoT devices is that it firstly scanned the internet for IoT devices that ran ARC processors. This ARC processor ran on a stripped-down version of the Linux operating system. Mirai infected devices that have not updated their default username and password [GMGE18].

According to Forbes in 2019, F-Secure security researchers have cautioned strongly that cyber attacks on IoT systems are now accelerating at a pace unparalleled. The attacks in 2019 calculated a triple rise in assault traffic to over 2.9 billion events compared to 2018. The organization uses honeypots – world wide decoy servers disguised as daily operational hardware to draw regular attacks – and this is the first time the honeypots “has ever hit the billion mark”. The researchers have attributed this rise in attacks to the growth in IoT devices worldwide. We have seen many warnings about the vulnerability of these devices to attack in recent months. This is due to a simple lack of protections in old firmware or architectures, and also a lack of housekeeping infosec. IT departments are still not even aware of all of these devices on their networks, making it nearly difficult to fix security problems [Do19].

IOT classifications

Cyber security starts with the identification and decomposition of property assets. The term IoT is quite broad. The degree of protection required against unauthorized data access, modification or the availability depends on the IoT device. A "IoT classification scheme" identifies a range of IoT levels, and is essential to their security. Classifying IoT according to the scheme means defining and applying the correct degree of security. The classification of data would also help in ensuring compliance with legislation.

The IoT Security Foundation has a very comprehensive classification which uses the CIA triad to help categorise the devices.The CIA triad Is a general guide for measuring information security. The CIA triad is composed of three concepts that are designed to guide policies for

information security within an organization. Firstly, confidentiality which is the protection of information from unauthorized access. Secondly, Integrity which is information is kept accurate and consistent unless authorized changes are made. Finally, availability which is that the information is available when and where it is rightly needed. These three concepts are rated per device on the level impact it could have on an organization. Where the standards of integrity, availability, and confidentiality are described as follows:

- Integrity
    - Basic - Devices are immune to low-level sources of threat with very little capabilities and priority.
    - Medium - Devices are resistant to medium-level threats that have very little, focussed capability.
    - High - Devices that tolerate significant levels of sources of threat.
- Availability
    - Basic - Devices the lack of availability of which will cause slight disruption.
    - Medium - Devices whose lack of availability has limited impact on a person or organization.
    - High - Devices the lack of availability of which would have a major impact on an person or an organization or affect several people.
- Confidentiality
    - Basic - Devices that processes public information.
    - Medium - Sensitive information processing devices, like Personally Identifiable Information, whose breach would have minimal effect on a person or organization.
    - High - Sensitive information processing devices, including confidential personal data, whose failure would have a major effect on an individual or organization [SCF18].

The aggregation of the three are then given a class which illustrates the possible impact the device can have if it gets jeopardized. The followinng demonstrate identifies the classes categorization its impact [SCF18].

- Class 0: where compromise is likely to result in no discernible effect on an person or entity with the data produced or the degree of control offered.
- Class 1: where a compromise with the generated data or the degree of control offered is likely to have very minimal effect on an entity or organization.
- Class 2: in addition to Class 1, the system is designed to withstand accessibility attacks that would have a major effect on an person or entity, or effect on several individuals.
- Class 3: The system is designed to protect sensitive data like confidential data, in addition to Class 2.

➢ Class 4: in addition to Class 3, where the data created or control level given, or if there is a security breach, can affect critical infrastructure or cause personal injury [SCF18].

For each compliance class, the levels of integrity, availability and confidentiality are shown in the Figure 1 below.

Compliance Class	Security Objective		
	Integrity	Availability	Confidentiality
Class 0	Basic	Basic	Basic
Class 1	Medium	Medium	Basic
Class 2	Medium	High	Medium
Class 3	Medium	High	High
Class 4	High	High	High

Figure 1 - Compliance Class Security Objectives [SCF18]

As a high level example, a device that simply sends data reading such as vibration levels of a machine has a compliance class of low. The response to a false or bad reading in this case might be that someone from the organization goes to the machine to check out. As opposed, a device that sends temperature readings to another so it can self regulate would have a compliance class of high. The response to a false or bad reading in this case might affect critical infrastructure or cause personal injury.

In conjunction with the compliance class, the use of application rating is used. The safety criteria can vary depending on the context in which a given product is being used. Usually, products and services are planned for primary application use, the type of market, and the operating environment. However, their users can, deliberately or inadvertently, use the products and services in various application environments. The security can not be sufficient when used outside of the intended context. This contradicts the principle of best practice because the expected use case affects the correct safety mechanisms. The different application categories are as follows: consumer (domestic), Enterprise, industrial, medical, automotive, public agency, critical national infrastructure [SCF18].

IoT Risk Analysis

A security evaluation is a procedure of evaluating how effectively an organization (e.g., information system, server, network, procedure, computer, etc.) conforms to the security requirements defined. Safety specifications are defined around the three basic safety properties (i.e., confidentiality, integrity, and availability) using resources such as security policies, security plans, standards, baselines, etc. The evaluation purpose is to determine whether security targets are being achieved, and to help identify the steps to be introduced to achieve those

goals. In every case, like every other security process, the evaluation process should not be a one-time process and should be used in any phase of the lifecycle of the evaluated entity. Organisations, in general, face threats. Such risks have the ability to adversely impact many facets of the company. The degree of these effects depends on several factors, not only on the threat itself but also on the impact and likelihood of these threats. Risk assessment is the process in which the analysis is carried out. Risk assessment is a crucial part of the overall and wider cycle called risk management and helps the company to routinely and reproducibly identify, quantify and prioritize the risk present. Risk management is a systematic and full process where the ultimate aim is to control all risks found through the process of risk assessment [Ol19].

There are two types of risk management used, qualitative and quantitative risk evaluation. Quantitative risk evaluation uses monetary numbers to measure risk. It uses statistical calculations to give you the amount of potential loss of a given risk depending on the asset valuation of the risk level and the probability of subsequent losses.
Qualitative risk assessment focuses on assessing risk based on probabilities and impacts and uses an evaluation scale to define risk as: low, medium, high.

Of the several methodologies available for risk analysis we have chosen to use OWASP.
The first step is to identify a security risk that must be measured. The tester will collect information about the threat, the nature of the attack, the vulnerability involved and the impact on the organization of an effective exploit. Generally, it is better to choose the worst case option on the side of caution, which leads to the higher overall risk.

The second step is the factor of likelihood. The initial step is to assess the "likelihood" once a risk is identified and to figure out how significant it is. At the highest point, this is a rough estimate of the probability that an attacker will find and exploit this specific vulnerability.
The third step is making effective estimations on variables. When looking at the effect of a successful attack, two kinds of impacts are necessary to know. The first is the 'technical impact' on the application, its data and its functions. The other is the "business effect" of the application on the financial and client.
The fourth step is to determine the severity of the risk. In this step, the likelihood and the impact are calculated, then compiled to determine the overall magnitude of this risk.
If the risks has been identified, a priority list of what to repair will be issued. In general, the most important risks will first be set. It simply does not improve the risk profile in general to address less critical risks, even if they are simple or affordable

Security Policy

The Security Policies are the various measures and controls that get implemented for an effective information security management system [HE02]. Policies are considered the bedrock of an information security management system. Hone and Eloff have states in [KMMB09],

p.402: "undoubtedly, the singularly most important of these controls is the information security policy". From the perspective of the management, it aims to provide direction and support for information security in conjunction with the relevant laws, regulations, and organization requirements. Davis and Olson have defined security policy as "to establish limits of acceptable behavior, decision confines, and standards." in [KMMB09], p. 494. In terms of employee perspective, the security policy is a guideline on what the correct and expected behavior is [HE02]. As with most societies, employees tend to be quite clueless in regards to what secure behavior constitutes. These policies aim to inform on how to mitigate against future threats and the consequences it may have on them and the business if they fail to do so. To give a general idea of what a security policy looks like, we have illustrated a high-level overview of such statements in Figure 2.

ISP focus areas	Sub-areas
Password management	Locking workstation Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department's level of responsibility
Internet use	Installing unauthorised software Accessing dubious websites Inappropriate use of the Internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS
Mobile computing	Sending sensitive information via mobile networks Checking work email via free networks
Information handling	Disposing of sensitive documents Inserting DVDs and USB devices Leaving sensitive material unsecured

Figure 2 - High-level overview of Information security principles of a security policy, from [HE02]

Since the majority of people never receive any cybersecurity training, they seemingly are oblivious when it comes to this genre. Hence one of the greatest threats often comes from within the organization themselves. By those uninformed employees with no malicious intent. Hence one of the favored tactics of cybercriminals is social engineering. In 2017, according to Kaspersky, 46% of cybersecurity incidents were due to careless uniformed staff. However, only 52% of businesses believe they are at risk from within, according to the same study [HU19]. It is not only the average employees who are clueless but also the senior level staff who lead these companies. It becomes evident that the lack of security awareness is one of the weaker links in the security chain, and it becomes that much more important to implement an effective security policy [Bi04].

Figure xxxxxx illustrated security policies that are applicable for IoT devices. The first column indicated the reference number for the policy whenever they need to be recalled the reference number is used. The second column is the policy statement; this is the requirement that needs to be fulfilled. The third column is the compliance class that is used to correspond the right policy to the right IoT devices. Last column is the category applicability meaning the use of the

application environment. This could mean for instance any of the following consumer (domestic), Enterprise, industrial, medical, automotive, public agency, critical national infrastructure. As mentioned in the IoT categorization section.

Req. No	Requirement	Compliance Class	Category Applicability	
2.3.10.1	The product/service stores the minimum amount of personal information from users.	1 and above	M	TBD in future release
2.3.11.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	1 and above	M	TBD in future release
2.3.6.4	The product does not accept the use of null or blank passwords.	1 and above	M	TBD in future release

Figure - [XXXXXX]

Regulation and standards

One unfortunate characteristic of IoT's current state is the lack of standardization in all facets of IoT. This can be seen by analyzing the broad variety of communication protocols, messaging busses, processors and even operating systems which can be fused to provide IoT functionality together. Organizations today are unable to buy bundled IoT systems readily that suit their particular uses cases and as such have to strive to build their own systems. This complexity foreshadows weaknesses and misconfigurations within every IoT device. Current IoT standards security requirements can also assist adopters in evaluating the aforementioned threats and risks associated with IoT deployment [CSA]. We have identified 53 different guidelines related to IoT from the following organization but not limited to, IoT Security Foundation, European Union Agency for Network and Information Security (ENISA), Industrial Internet Consortium (IIC), GSMA, Open Web Application Security Project (OWASP), IoT Security Initiative, Online Trust Alliance (OTA), Cloud Security Alliance (CSA), US National Institute of Standards and Technology (NIST), IEEE.

We highlight the latest state of the art relating to IoT Security Standards, current data security frameworks and IoT stakeholders involved. The discussion is limited to IoT data at rest.
The Broadband Internet Technical Advisory Group recommends a set of IoT data security and privacy recommendations for data at rest, such as reducing data storage, encrypting data storage, extracting confidential data, and maintaining data availability. The IoT does not,

however, provide an in-depth collection of guidelines for IoT data at rest, nor does it define the countermeasures needed to enforce its guidelines. In fact, threats and attacks against IoT data at rest remain unchecked.

The Open Web Application Protection (OWASP) suggests different IoT security and privacy guidelines at rest, such as minimizing data storage, minimizing data retention, maintaining allowed access and physical access preclusion. The OWASP also notes IoT stakeholders such as suppliers, developers and consumers who may use their guidelines to secure IoT data at rest. Nevertheless, the OWASP did not consider the required countermeasures to enforce its recommendations, nor did it distinguish potential attacks and threats against IoT data at rest.
The European Union Agency for Cybersecurity (ENISA) suggests several IoT data at rest security and privacy guidelines, such as reducing data retention, encrypting data storage, identifying recovery methods, informing clients and ensuring proper data destruction. The ENISA, however, does not consider the IoT stakeholders that may use its guidelines, nor does it define suitable solutions for implementing its guidelines. The ENISA does however uncover attacks and threats against IoT data at rest.
The IoTA organization proposes a list of security and privacy guidelines for IoT data at rest, including data storage encryption, user information, and deletion of confidential data. IoTA neither separates the implementing techniques needed to fulfill its guidelines, in addition to, for whom these guidelines are for. Attacks and risks to IoT data at rest are left unidentified.
The IoT Security Foundation (IoTSF) proposes a set of guidelines for IoT data at rest security and privacy , such as using distributed data storage, identifying recovery methods, ensuring proper data destruction, and searching for encrypted details. However, the IoTSF does not recognize effective countermeasures to enforce its guidelines, neither does it differentiate IoT data at rest attacks and threats.

IoT security and privacy concerns are exacerbated by the absence of effective standards, regulation and lax governance. Nonetheless, some measures have been suggested at national level for instance, the General Data Protection Regulation (GDPR), Industrial Internet Consortium (ICC), IoT Security Foundation (IoTSF).

The European Union (EU) voted in December 2016 to use the GDPR as a replacement for the obsolete Data Protection Directive (DPD) introduced in 1996. The DPD's main goal was to protect the personal information of individuals within the EU from abuse and to allow individuals within the EU to have greater control over their personal data. The aim of the GDPR is to replace the DPD as a regulation and it will cover the entire EU as unified legislation. The GDPR also made six significant improvements relative to the DPD (e.g., in terms of identifying personal data, human rights, data controllers and processors and global impact).
Not all IoT applications deal with personal information — for example, applications related to the Industrial Internet of Things (IIoT). One example is a digital healthcare revolution due to the exponential growth of wearable and integrated medical devices that offer continuous monitoring of the health. Healthcare data is also extremely vulnerable, and draws the attention of attackers. Therefore, health data must be protected within the framework of the GDPR. Many essential IoT

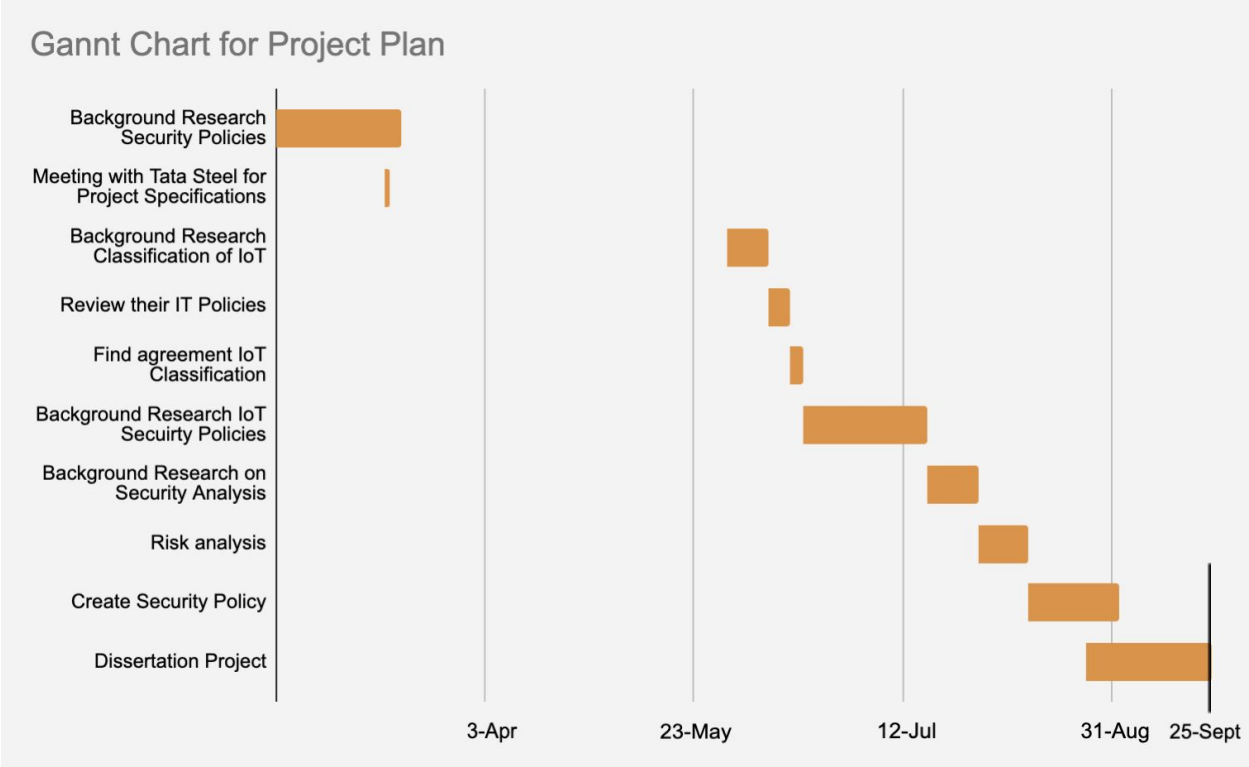
applications dealing with personal data such as smart metering and smart home applications do have to be protected within the framework of the GDPR.
The ICC is an organization that was set up in 2014 to increase interconnected devices development. This organization's key purpose is to create a partnership between businesses, universities, and governments to collaborate on the creation of testbeds for real-world systems. It has also been directly interested in promoting the specifications of IoT standards. To this end, the ICC introduced a security architecture originally designed for the IoT in 2016. The key objective of this security architecture is to ensure universal recognition by the industry on how to build safe IoT systems.
IoTSF is a non-profit organization that since 2015 has expanded the IoT industry. This development involves creating protocols, workshops, and seminars on security and privacy. The IoTSF has also discussed the problems in the market and, above all, it has worked with a cooperative effort to fill the difference with other IoT firms. The IoTSF introduced an IoT system as a checklist that IoT producers should use to improve compliance with the IoTSF specification. This style of collaboration aims to exchange experience, skills, and best practices.

Description of the project

Tata Steel, an Indian multinational steel-making company had chosen recently to give more emphasis on their security of IoT devices. They have collaborated with Swansea University to come up with solutions and one aspect of that is to establish security policies for their IoT devices in the Port Talbot, Wales Factory. The majority of their devices are Industrial IoT but they have requested to direct the security policies towards IoT. As they are purchasing more IoT devices they are not running any type of check of whether the purchased devices are safe or not. They have an ecosystem of all types of IoT devices and hence their objective is to safeguard themselves against possible attacks. One aspect of their main objective is to establish an IoT security policy. At the end of this project, they will receive documents with security policies for IoT for their context. The risk analysis is a by-product of creating the security policy but could be appended to in the end. The dissertation report itself will have several sections. The literature review section will be the basis for a theoretical framework in which the definition and analysis of the main research theories, principles, and models will be done. This will entail IoT, IoT security, IoT classification, IoT risk analysis, and lastly IoT security policies. The methodology section will describe how research that is conducted, so the overall approach, methods of collecting data, details of where, when, and with whom the research took place, tools and materials used, any obstacles faced in conducting the research and how it was overcome, and finally evaluation of your methods. Next would be the result of my research, which would include tables, graphs, and charts. The discussion is the analysis and implications of the results in relation to the topic. That will the general structure of what will be written in the dissertation report.

Project plan

Gantt chart



Background Research on Security Policies

For the computer science project research methods module in Swansea University, we were assigned to do a report on a related subject to that of our dissertation project. The report I wrote was on ‘how to implement an effective security policy’. The background research made gave insight on what a security policy is, its importance, and how to implement security policy effectively.

Tata Steel Meeting for Project Specifications

This was the first meeting Tata Steel had with Swansea University to discuss their main issues and how we are going to tackle the issues. During the meeting, a presentation was given on the report written on ‘how to implement an effective security policy’ and an introduction of the person who will be working on a security policy project. In addition, the specification and scope of the project were described.

Background Research Classification of IoT Devices

Classifying IoT according to the scheme means defining and applying the correct degree of security. This background research will allow us to find the right classification approach as there are several of them. Currently the proposed one from IoT Security Foundation seems to be the most comprehensive one and best suited for this project.

Find Agreement on which IoT Classification Type to Use

After doing a comprehensive background research on IoT classification we will have to contact Tata Steel, to see if they are in agreement with the chosen classification type. After understanding their reasoning for not wanting to go with that specific classification type, try to provide alternatives.

Review their IT Policies

Currently Tata Steel does not have IoT policies but they do have an IT policy. The IT policy that they have in place is already received and needs to be analysed. The analysis will be a starting point for structuring the IoT policy. In addition, it will give a template for the format for us to follow.

Background Research on IoT Policies

Research papers on IoT policies are very few. The use of standards and regulation will be the main guideline. Most comprehensive documents on this subject were found from the organization of ENISA, IoT Security Foundation, and OWASP.

Background Research on Risk Analysis for IoT

There are several methodologies possible for this task. Through the background research we will find out what the most ideal risk analysis is for Tata Steel's context. Currently the OWASP methodology seems to be the most appropriate but further study needs to be done.

Risk Analysis

Currently we have chosen to apply Qualitative risk assessment where it focuses on assessing risk based on probabilities and impacts and uses an evaluation scale to define risk as: low, medium, high. The risk analysis methodology we currently have in mind is the OWASP utilizing the 5 step process. By analyzing the risk we will be better able to steer security policy in the right direction.

Create the Security Policy for Tata Steel

Based on all the research and finding that have been done, we will come up with the best possible security policy for IoT devices for Tata Steel's context. This will come in the same structure and layout as their existing policies but will have an extensive list of security policy statements. This list will be subdivided in accordance with their categories, as following:

business security processes and responsibility, device hardware and physical security, device application, device wired and wireless interfaces, authentication and authorisation, encryption and key management for hardware, and privacy.

Dissertation Project

This is done by drawing together theories, methods and methodologies and bringing them to bear on this topic and then writing up a report.

Risk Analysis

Conclusion

book

Bibliography

[AKN20] Benedikt Abendroth, Aaron Kleiner, Paul Nicholas. Cybersecurity Policy for the Internet of Things. Retrieved 17 April 2020, from https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-for-iot

[ANCK19] Hezam Akram Abdulghani, Niels Alexander Nijdam, Anastasija Collen, Dimitri Konstantas. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. 1:6 - 774, 2019. Doi: 10.3390/sym11060774

[Ba17] Baseline Security Recommendations for IoT. ENISA. 11(6) :774, 2017. doi: 10.2824/03228

[Bi04] Matt Bishop. Introduction to Computer Security. Addison-Wesley, Boston, 2004, ISBN 0-321-24744-2

[BJSL17] Megan L. Brown, Umair Javed, Kathleen Scott, Madi Lottenbach, John Lin. The IoT Revolution and our Digital Security. Retrieved 17 April 2020, from https://www.uschamber.com/IoT-security

[Do19] Zak Doffman. Cyberattacks On IOT Devices Surge 300% In 2019, Measured In Billions. Retrieved 1 April 2020, from https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/
[GMGE18] Tatikayala Sai Gopal, Mallesh Meerolla, Jyostna G, Reddy Lakshmi Eswari, E Magesh. Mitigating Mirai Malware Spreading in IoT Environment. IEEE. ISBN: 978-1-5386-5314-2. doi: 10.1109/ICACCI.2018.8554643
[Ha18] Nermin Hajdarbegovic. Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. Retrieved 17 April 2020, from https://www.toptal.com/it-developer/are-we-creating-an-insecure-internet-of-things
[HE02] Karin Hone, J.H.P Eloff. Information security policy - what do international information security standards say?. Computers & Security, 21:402 - 409, 2002. Doi: 10.1016/S0167-4048(02)00504-7
[Hu19] Kaspersky. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Retrieved 16 November 2019, from https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[In19] Internet Of Things To Connect 125 Billion Devices Worldwide By 2030. Retrieved 3 April 2020, from https://www.busiweek.com/internet-of-things-to-connect-125-billion-devices-worldwide-by-2030/
[KMMB09] Keneth J. Knapp, R. Franklin Morris, Jr., Thomas E. Marshall, Terry Anthony Byrd. Information security policy: An organization-level process model. Computers & Security, 28:493-508, 2009. https://doi.org/10.1016/j.cose.2009.07.001
[Ol19] Armando José Martins de Oliveira. IoT Security Assessment in an IoT Smart City Scenario. Retrieved 1 April 2020, from https://eg.uc.pt/bitstream/10316/87985/1/Dissertacao_AOliveira_final_3_9_2019.pdf
[SCF18] IoT Security Compliance Framework. Retrieved 16 November 2019, from https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf
[SGE15] Cloud Security Alliance. Security Guidance for Early Adopters of the Internet of Things. Retrieved 16 November 2019, from https://www.security-congres.nl/download/?id=17707114&download=1
[Re20] Research Report on Global Smart Food Logistics Industry 2020-2025. Retrieved 16 April 2020, from https://www.marketwatch.com/press-release/research-report-on-global-smart-food-logistics-industry-2020-2025-2020-04-13?mod=mw_quote_news