

**Deakin University**

**CSRI TRIBE**

Project Scope

**Project Sponsor - Mr. Damien Manuel**

**Project Team - SQUAD 1**

**Sowmya Viswanathan, 218600737**

**Angela Bhagath,218580537**

**Sultan Ali Khan, 217663965**

**Qutayba Usman Burki,217618954**

**Mridul Vajpayee, 217331547**

**Adeosun Peter Damilola, 218392095**

**Ali Saeed, 214003103**

**Sohail Mohammed 218664659**

**Aswathi Ashok Kumar, 218359105**

**Simran Sharma , 217575992**

**Talha Saleem,**

**Ayesha Nishadhi Withanage 217658481**

**Lasantha Jayatilaka 218216182**

Document Version 1.0

# Document Revision History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Version** | **Editor** | **Reason** | **Supervisor Signature** | **Client Signature** |
| 06-04-2019 | 1.0 | ANGELA BHAGATH | Defining Project Scope |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Motivation / Problem Description

We are living in an era where the technology is advancing on a rapid pace which is making the small businesses prone to cyber threats. In order to tackle these threats, the phenomena of cyber security are going to play a vital role to reduce these threats in cyber context. The preservation of data or information has to follow the principles of confidentiality, integrity and availability. Confidentiality means to protect the sensitive information which otherwise can undermine the security, in some cases the profitability, reputation, of any company while the integrity is simply to protect the information form unauthorized and unwanted access and modification. The availability, in some cases directly link to organization’s reputation, means to make data, services and information availability at all times for their intended personnel’s.

Any organization needs thorough research and assessments of their cyber security capabilities and effectiveness of their cyber environment since changes in technology are rapid and continuous, so organization must undertake adequate measures to improve its cyber environment and keep it up to date. The cyberattacks on an organization whether its nature is security breach, information loss and on organizational prosperity could rest in financial loss, reputational damage, decrease performance and productivity.

The goal of this project, undertaken, is to conduct a research which will assess the different controllers, provided by the NIST Cyber Security Framework from which the entire functionality of cyber security setup is based. The studies in cyber security area still in early stages, the concepts, ideas and mechanisms are still not fully evolved. Gradually more studies are taking place. We will be working on different areas of cyber security frame work which include identity, protect, detect, respond and recover.

Our main goal is to collect and gather as much as information from all the resources that are available to us from which we will build our own framework or try to update the current version of the framework. The component of identity will cover all the core norms of business environment and asset management. Protect plays the roles of protecting all the core aspects within the organization which includes identity management and access control. Detect is positioned to perform continuous monitoring. Response is associated to all the planning which includes coming up with strategies to mitigate all the threats. Recover is used as recovery mechanism to get all the lost data and to prevent further damage.

# Context

The Information Technology (IT) industry has advanced incredibly throughout the last 50 years. Constant, exponential development in preparing power and memory limit has made IT equipment quicker as well as minor, lighter, less expensive, and simpler to utilize. The IT industry has likewise progressively joined with the business into a consolidated division generally called Information and Communications Technology (ICT). In the course of recent years, specialists and policymakers have communicated mounting qualms about shielding ICT frameworks from *cyberattacks*—intentional endeavours by unauthorised persons to get to ICT frameworks, generally with the objective of theft, disturbance, or other unlawful activities. Various specialists expect the number and severity of cyberattacks to rise in the coming years. Battling this is a multi-disciplinary issue that traverses hardware and software through to policy and people – every last bit of it went for both averting cybercrimes happening in any case, or limiting its effect when it does. This is the action of ***cybersecurity.***

For more than two decades we have been hearing: "Cyberwar is coming!" Researchers acquainted with the Realist hypothesis of International Relations were amazed by the possibility of Cyber War developed close by the internet conceptualisation and then the acknowledgment. History and philosophy demonstrate that scientific advancements don't change human instinct enough to exterminate fierce clash. While the potential for utilizing the cyberspace in a disagreement is self-evident, the current winning properties of the internet make major ideas of assault, barrier, and at last war insufficient. However, even experienced IT experts very frequently confound demonstrations of digital errors and secret activities with digital attacks. Neglecting to conceptualize what cyberwar is and, significantly, what it isn't, skews discernment and results in flawed policymaking. Numerous organizations and establishments worldwide delay their cloud evolution. The primary purpose behind their inaction is security concerns. People will in general trust that just putting away information on their on-prem servers can shield from cybersecurity breaches. The other incredible challenge for the cloud cybersecurity is the Internet of Things or the IoT. The idea of the interconnected system of devices trading data implies that noxious access to a solitary unprotected point implies a potential security breach to the entire system. This is the reason cybersecurity is steadily announced as a huge threat for the organizations and the largest region of potential improvement. No protection is perfect, so not a single group of measures can ensure 100% safety of any business.

The major factors contributing to this problem is mentioned below

* 1. failure to cover cyber security basics
  2. No idea on what generates corporate cyber security risks
  3. Lack of a cyber-security policy
  4. Confusing compliance with cyber security
  5. The human factor – the weakest link of everything
  6. Bringing your own device policy (BYOD) and the cloud
  7. Funding, talent and resources constraints
  8. No information security training
  9. Lack of a recovery plan and Constantly evolving risks.

Hence, using security controls as a key metrics we need to accurately represent the cyber security capability and maturity of an organisation for which we use NIST Cyber Security Framework Version 1.1 in this project. In this project we will be assessing each area of the framework such Identify, Protect, Detect, Respond and Recover. Each area contains more security controls which we will be exploring and will find the best key metrics that will promote an organisation’s maturity in terms of cyber security.

# Value Proposition ( Simran & Talha)

The Benefits of using this solution is that it gives an opportunity so that organisations can identify the areas where we can implement the new areas. This profiles help in making stronger communications. Implementation plan and framework when paired together help the organization to enable cost-effective prioritization and communication of activities which help in improvement.The component Implementation tier of the framework assists the organization by telling on how an organization views the cyber security risk management.

# Core Idea/User Stories/ Requirements(Peter & Pavs13)

**Core Ideas:**

**Methods in accessing current/implemented frame work process:**

* Developing techniques to describe the level of sophistication and rigor an organization employs in applying its cybersecurity practices. Access current implantation tires in the organisation and also determine the appropriate tires to implement.

* Creating and developing training modules to ensure staff are being trained on best practice and how to apply.

* Improving frameworks and functions by identifying and comparing security controls in each framework and their sub categories.

* Integrating of frameworks in Supply chain risk management.

* Carrying out web surveys in the to identify loop holes in implementation of frame works.

**USER STORIES /Requirements:**

**Asset management:** Proper inventory of systems, devices, applications, external information systems, software platforms, definition of cybersecurity roles and responsibilities, mapping organizational communications and data flows.

**Business environment :** Roles must be identified in critical infrastructure and supply chain; clear resilient requirements and mission statement , dependencies on other services must be identified.

**Risk assessment:** Threats and variability must be identified and properly communicated, evaluated and responses are prioritized/identified.

**Risk management strategy Processes**: identification of risk tolerance and proper consideration of critical infrastructure role.

**Access control:** credentials and identities are properly managed for authorised users and devices by managing permissions, remote accesses and network integrity.

**Awareness and training:** Third party, Privileged and executive users should be trained on information and physical roles and awareness.

**Data security Data-at-rest protection/**[**data-in-transit protection**](https://www.ssh.com/products/tectia-ssh/)**: management a**nd destruction of formal asset. Protections against data leaks proper integrity check.

**Maintenance:** Swiftly maintenance and monitoring and control over remote maintenance.

**Protective technology Log collection and analytics**; controlled access to removable media and controlled access to assets.

# Target Deliverables (Lasantha and Ayesha)

## Target Deliverables

This project involves following target areas to be addressed and their dependencies to achieve the excellence in forming security controls in an organisation. As the importance of the security controls are stated in the above areas, this section will elaborate the target deliverables of this project.

### Identify

Primary objective of this area is, identifying and assessing product and services in an organisation in following areas to mitigate the vulnerabilities due to malicious functionality or poor development practices. According to NIST Cybersecurity Framework, current practices to improve controls in following areas must be identified.

* Asset Management
* Business Environment
* Governance
* Risk Assessment
* Risk Management Strategy
* Supply Chain Risk Management

Above areas of an organisation must be identified and respective details must be verified and validated.

### Protect

In this area, identifying the best practiced policies and technologies to support the security controls are the goals. They must be improved according to the following areas.

* Identity Management and Access Control
* Awareness and Training
* Data Security
* Information Protection Processes and Procedures
* Maintenance
* Protective Technology

This stage is extremely important when identifying the parameters to improve security controls.

### Detect

Detection of threats or attack events and how the detection related procedures benefit to improve security controls is the key objective of this area. Detection procedure includes following processes.

* Anomalies and Events
* Security Continues Monitoring
* Detection Process

Above areas must be taken into consideration when improving security controls of and organisational system.

### Respond

Respond to an attack also plays a critical part during an attack. Measures and counter measure when responding to an attack is the area discussed in this section and how it benefits to improve security controls. Responding to an attack comprises following sup sections.

* Response Planning
* Communication
* Analysis
* Mitigation
* Improvements

Above measures must be taken in to consideration when responding to an attack. We need to identify how they can benefit in improving the security controls in an organisation.

### Recover

Recovery phases is essentially important when overcoming a cyber-attack. Recovery measure must be emphasised as it plays one of the most critical areas. Following sub sections must be taken into consideration while facing into a recovery stage.

* Recovery Planning
* Improvements
* Communications

Following measures must be taken into consideration with respect to all the above-mentioned areas (Identify, Protect, Detect, Respond, Recover). Improving Security Controls will be greatly influenced by the following mentions.

* Identifying Technologies
  + Identifying existing technologies and their problemed areas
  + New technologies with their benefits and limitations
* Policies
  + Loopholes in existing policies
  + How existing policies can be improved
  + New policies and their benefits and limitations
* Practices
  + Identifying current IT Practices and their problemed areas and loopholes
  + How existing practices can be amended to improve
  + New practices and their benefits and limitations

Above mentioned three areas must be emphasised while improving the security controls and there will be certain limitations and dependencies when applying the improvements of security controls.

# Roadmap (Aswathi,Sohail,Saeed)

In order to work our product successful, we will divide functionality into sprints as given below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Name** | **Goal** | **Features** |
| 4 april to 12 april | Sprint 1 | Research, access and determine key metrics based on controls, NIST Frame work,  Platform Selection  Designing and developing tools.  Control identification | Scope document that has been agreed by all parties.  Technology selection, |
| 13 april to 25 april | Sprint 2 | Development and product environment setup, GIT version controlling and setting up project on local machines, security controllers testing for organization maturity. (Tier 4) | Basic project setup, development environment setup  Git version controlling, linkages and association between controllers for result |
| 28 april to 09 may | Sprint 3 | Cyber security capability testing,  Building business communication, mitigation challanges | Documentation of testing, |
| 12 may to 25 may | Sprint 4 | Demo  Controls rating, testing, | Report with recommendations for business, and controls tested and verified, |

## Execution Strategy

* Firstly, gather the information to find out the problems and vulnerabilities of the system and present them for consideration
* Next, Identify the potential tools and controls to solve these problems using the NIST framework and cybersecurity controls
* Develop the strategic controls and their integration with the system
* Testing of the controls and checking for the solution of threats associated with them
* Integration of all the system controls to be tested and presented as a single unit
* Provide a continuous research and update report and get feedback time to time for further development

## Sprint 1

**Goals:**

The goal of Sprint 1 is to choose a specific areas(Identify, Protect, Detect, Respond, Recover), of NIST framework, by the members, research on the same and identify suitable controls for each area that can be then tested upon the organization to check its capability and maturity.

**Target deliverables:**

A detailed report describing the workflow, to be specific, the approach in identifying and selecting the area of work, discovering the associated controls, their evaluation, testing, and implementation to improvise the cyber security capability and maturity of the organization.

## Sprint 2

## Work in Progress

**Goals** - To be discussed

The goal of Sprint 1 is to deliver the end to end infrastructure so we can start collaboratively planning the interfaces to enable integration efforts to commence on (client name)’s side. These can be decomposed to:

* Get an end to end solution working
* Collaboratively create an output data format / schema (in collaboration with client)
* Prepare a suitable environment within a docker container to encapsulate and execute the transformation process

**Target deliverables -** To be discussed

* A docker container encapsulating the transformation engine
* An invocation script that accepts the input folder, output folder and invocation parameters
* A deployment document that describes how to install and use the solution

## Sprint 3 - Work in Progress

**Goals -** To be discussed

The goal of Sprint 3 is to build upon the Increment in Sprint 2, namely by adding:

* Error logging
* Input/Output Validation
* Transformation logic

**Target deliverables** - To be discussed

* A docker container encapsulating the transformation engine
* An invocation script that accepts the input folder, output folder and invocation parameters
* A deployment document that describes how to install and use the solution
* List of errors and associated meaning
* Sample dataset to validate the transformation engine reported results

## Sprint 4 - Work in Progress

**Goals** - To be discussed

The goal of Sprint 3 is to…

* bang
* pow
* smash

**Final deliverables** - To be discussed

* thing 1
* thing 2
* thing 3
* thing n

# Limitations, Constraints and Considerations :

The limitations, constraints and considerations of the project are as follows:

* The team needs to work on identify the vulnerabilities and determine the threats.
* This project will focus on cyber-security techniques that need to have solid outlines of communication and conventions in place, responsiveness, acquaintance, and getting everyone to work collectively.
* The team will adapt to working in Linux environment.