National College of Ireland

Framework to assess cyber security maturity of smart buildings

MSc Internship
CyberSecurity

Siddhant
Student ID: x18203884

School of Computing
National College of Ireland

Supervisor: Mr Vikas Sahni

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Siddhant
Student ID:	x18203884
Programme:	CyberSecurity
Year:	2020
Module:	MSc Internship
Supervisor:	Mr Vikas Sahni
Submission Due Date:	07/09/2020
Project Title:	Framework to assess cyber security maturity of smart buildings
Word Count:	886
Page Count:	7

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard speci ed in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:	Siddhant
Date:	6th September 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator o ce must be placed into the assignment box located outside the o ce.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Framework to assess cyber security maturity of smart buildings

Siddhant
x18203884

1 Potential smart building attacks

Denial of service attack: Denial of service attack is used to shut down the targeted machine or a network by ooding the junk request on the server [1]. For example If in smart buildings air conditioning of data server room stops working than organization can face huge loss and can also lead to ddos attack, Or server face lot of requests at the same time than server will be busy on junk request and can not serve to the original users which can also impact the reputation of an organization by restricting user access to resources.

Table 1 shows a matrix for checking cyber maturity of smart buildings. It describes about impact areas of smart building's, possible breach incidents, cyber defence components, preventative aspects.

Table 1: Matrix for checking cyber maturity of a smart buildings

Impact areas	Cyber Breach incidents	Cyber defence components	Preventative aspects
Users	failure in Systems	Identity validation	Access to re system (False alarm to evacuate building)
Third party remote access	Nuisance techniques to life threatening damage	Security for end point devices	Access to security system (Unauthorized access)
Physical access to apps, networks and connected devices	Malicious softwares and virus infections	Network security	Access to communication network
Integration platforms	Attack by unauthorized outsider or fraud by sta	Data security	Access to utility-installed device
Communication gateway	Unintentional damage by third part access because there infrastructure got compromised	Multi layer security	Hijack BAS for ransomware

Improper access control: Improper access control can lead to very dangerous attack because if granting access is not proper than any person can access anything and which may lead to exposure of sensitive information.

Intrusion detection and prevention: Intrusion detection is a process of monitoring malicious signs inside the network for predicting the incidents [2]. Moreover intrusion prevention is used to stop the potential threats found by analyzing the network. So if intrusion detection and prevention system is compromised than anyone can hack into your smart buildings and can compromise your system and information.

Weak Encryption: If smart buildings are using weak encryption than anyone can do man in middle attack while transmitting data and can decrypt the information because encrypting technique is weak which will lead to exposure of sensitive information and can also damage the reputation of an organization.

2 Matrix for checking smartness of smart buildings

Here is a matrix which checks about smartness of smart building by checking what are the components present in that building and what is the impact of that component on smart buildings in terms of smartness as well as security. Moreover according to impact components is de ned in three part low, medium and high.

Table 2: Matrix for checking smartness of smart buildings

Smart components	Impact level on smartness	Security impact
Fire Detection devices	High (Fire detection deal with human life)	High (False alarm can evacuate whole building and attackers can attack in that speci c time)
CCTV	High (It can help in backtracking)	High (If CCTV is compromised than attacker can monitor all your activities and it will be di - cult to backtrack)
Access control	High (Only allow authentic persons)	High (Attacker can easily get into you infrastructure if access control gets compromised)
Command and control system	Medium (System transform actionable data into real time)	Medium (False public announcement can be made if system is compromised)
Lightning control systems	High (Helps to save energy)	Low (Impact is low because lightning can impact the work in night only and that for few minutes only)
Elevator	Low (Fast mode of travelling between di erent oors inside building)	Low

Smart components	Impact level on smartness	Security impact
Boiler	Low (Helps to increase the temperature of water)	Low
Databases	High(Helps to maintain the data of an organization in an systematic way)	High (Data is the main asset for every organization because it includes all the information about the organization)
Generator	High (Backup device for providing energy to an organization)	High (Organization can go under DDOS attack if energy supply cut down and generator also stops working)
Heating, Ventilation, Air conditioning (HVAC)	High (Helps in maintaining temperature of an organization)	High (If air conditioning of data server room stops working than organization can face huge loss and can also lead to ddos attack)
Network monitoring devices	High (Helps in monitoring di erent activities)	High (Looks for malicious activities in an organisation and beeps alarm if anything suspicious)

3 Smart buildings survey

Survey is lled by industry specialist who are currently working in smart building security in Ireland. In addition to this survey suggestions also gives real world avour to this thesis from industry specialist inputs.

So here are some graphs from a survey lled by industry specialists of smart buildings security.

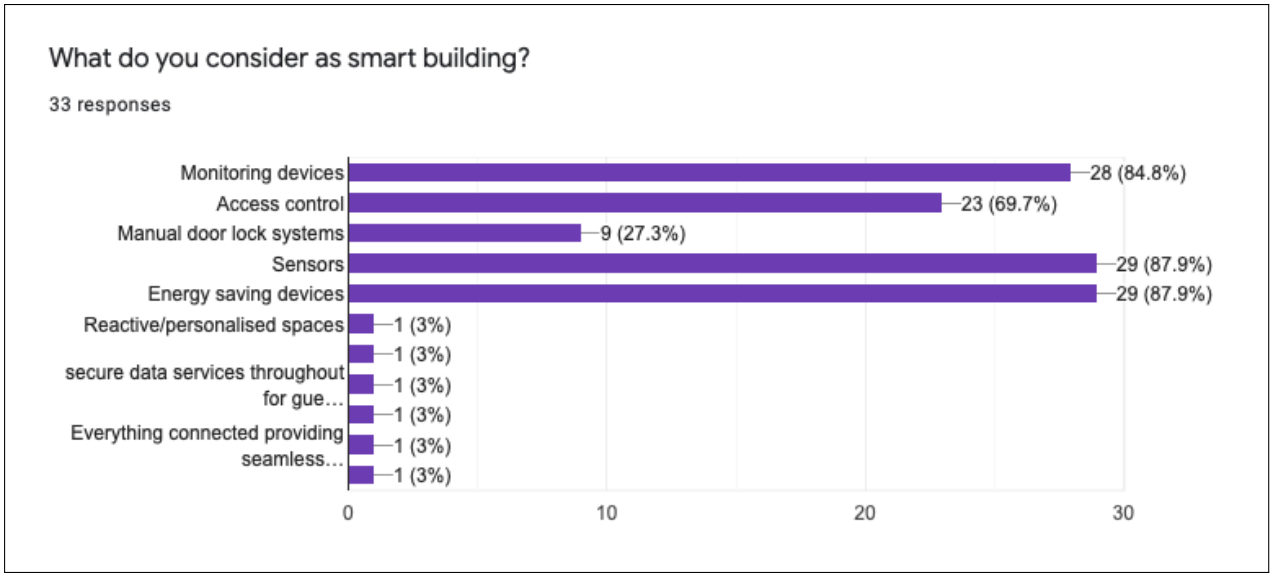

Figure 1: Smart buildings considerations survey

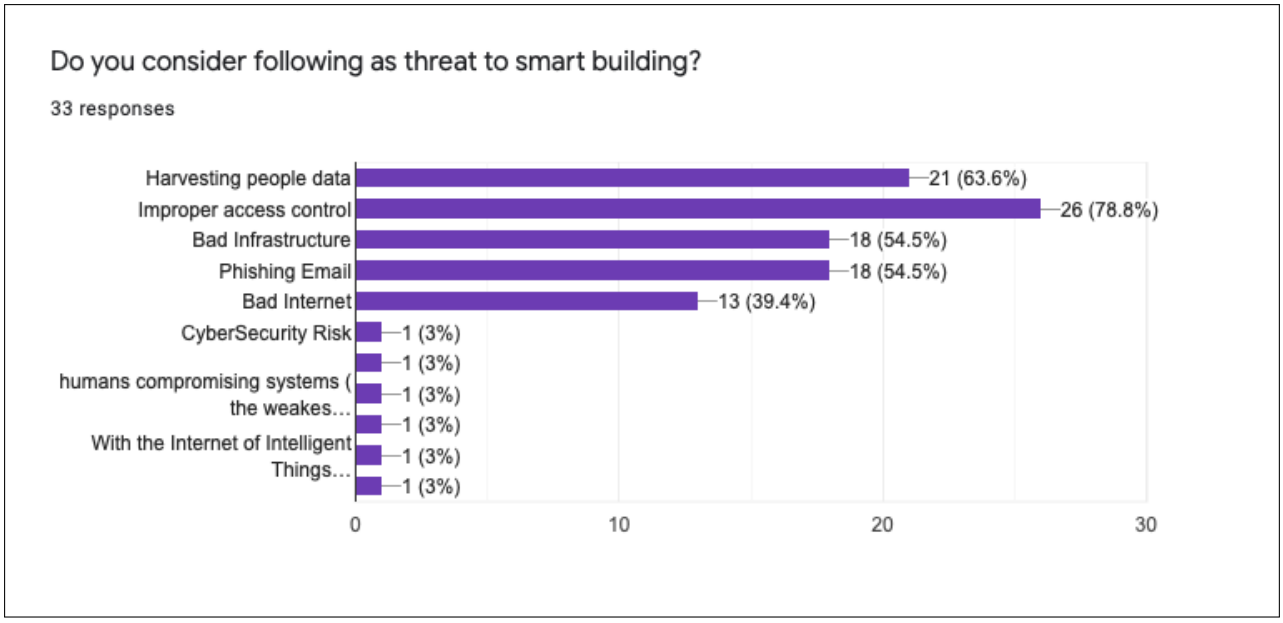

Figure 2: Smart buildings threats survey

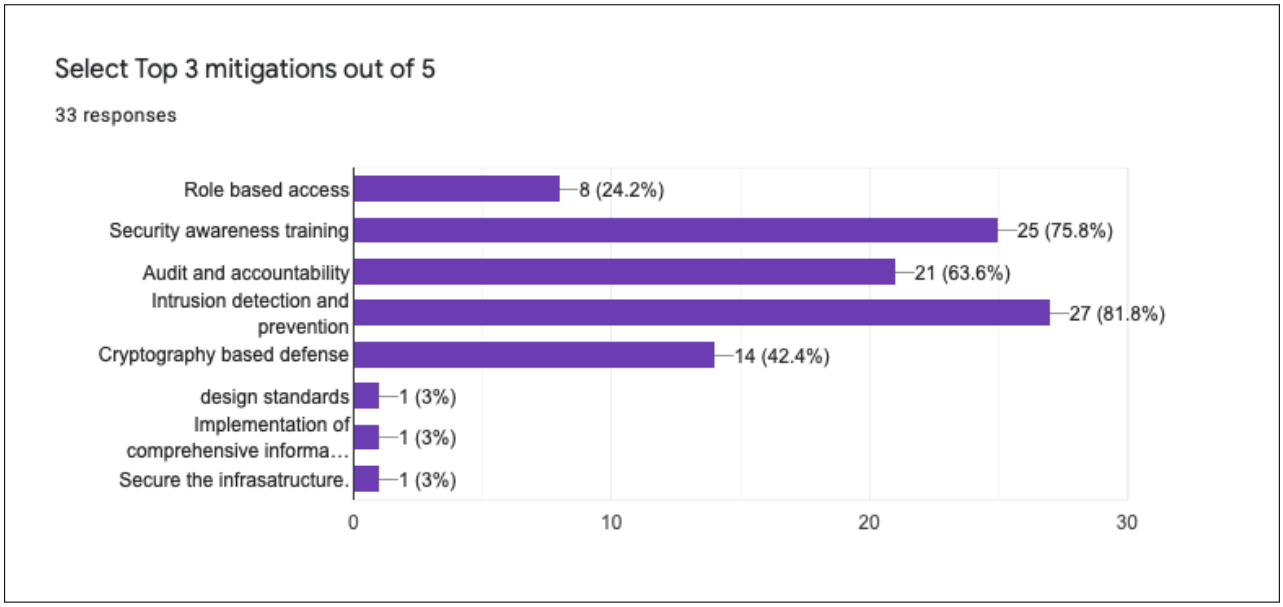

Figure 3: Smart buildings mitigation's survey

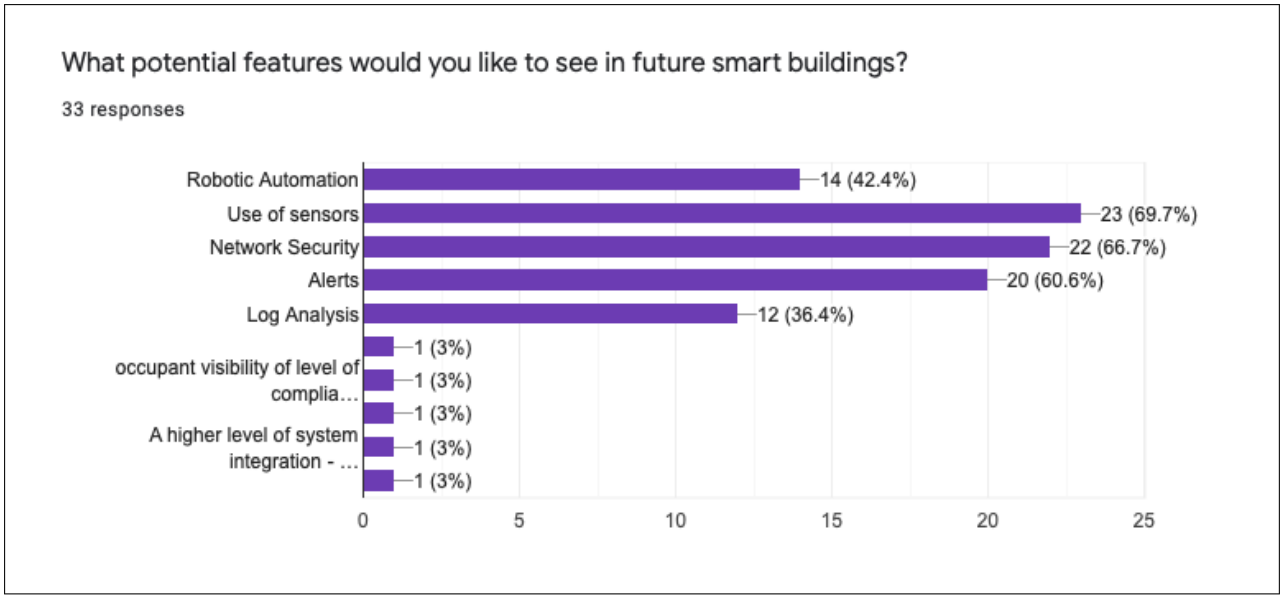

Figure 4: Smart buildings potential surveys

Bar graphs give description about what do you consider as smart buildings, threats to smart buildings, mitigation of those threats, and potential features for future smart buildings.

4 Internship Task Report

Monthly Internship Activity Report

The Internship Activity Report is a 1 page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and uploaded to Moodle on a monthly basis.

Student Name: Siddhant Student number: x18203884

Company: ARUP Month Commencing: June 20 – Aug 20

Role Description:

The primary objective was to support the team in delivery of managed security services. The role required, with assistance from the team, to provide cyber risk management services and advisory support to the clients as they deliver critical and timebound projects and programs.
List of tasks performed:

- Supported the review of vulnerability assessments and penetration testing reports as part of client Digital Asset Assurance Program.
- Followed up with relevant staff (internal and external) to obtain evidences and assurances in response to client Digital Asset Assurance program.
- Carried out research and investigation for internal and external clients. Areas of research includes, information security, data protection, Governance, Risk and Compliance.
- Developed operational documentation and processes.
- Collaborated in providing cyber security expertise to deliver projects.
- Carried out cookie security scan with respect to GDPR.
- Worked on threat and vulnerability risks for different websites.
- Worked on WordPress vulnerabilities and mitigations.

Employer comments

Siddhant demonstrated good technical understanding and was thorough in the investigation work that he carried out. The cookie security scan work he carried out demonstrated the comprehensive way that he approached a piece of work, ensuring that the information obtained what double checked for accuracy.

Sid was also adaptable in his work, working on cyber queries, websites and incident management. These elements will provide Siddhant with great grounding for application during his career.

Through support and guidance Siddhant can learn to understand what's important when delivering services to our clients and in turn can improve of his reporting skills.

Student Signature: Date: 1 Sep 2020

Industry Supervisor Signature: _ _____Date: 1 Sep 2020

References

[1] N. Komninos, E. Philippou, and A. Pitsillides, \Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933{1954, 2014.

[2] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, \Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *2016 IEEE International Smart Cities Conference (ISC2)*, 2016, pp. 1{6.