IFN541 Information Security Management
Task 2: Report

Group 1

Student Name	Student Id	Contribution
Audun Stjernelund Lien	n11371854	Section 3, Section 1, report formatting
Chih-Yu Chuang	n10952535	Section 1, Section 2, Seation3, Reflection
Priyanka Kotla	n11254904	Section 2, Reflection

Innholdsfortegnelse

Introduction 3

Risk Management Plan 5

RACI Chart 7

Analysis and recommendations 8

Cost Benefit Analysis 9

Recommendations 9

Appendix – Teamwork Reflection 11

Bibliografi 13

Introduction

Target Australia is a retail company, owned by the Australian conglomerate Westfarmers (Target Australia, 2022). Their headquarters is located at North Geelong in Victoria. Target sells its products through department stores and online shopping. Target has around thirteen thousand employees and their annual revenue is about 3 billion. Target main products are food, clothing, household goods, and electronics. Target also provides online shopping through its website.

Target have four main critical assets (Trend Micro, 2019).

1. Competitive information: Research and Development information, formulas of products, project data (Trend Micro, 2019).
2. Legal information: copyrights, contracts of third-party companies, intellectual properties.
3. Personal information: customer identities (name, address, card number), employee identities (name, address, bank, insurance)
4. Data of daily operations: daily operations, human resource, salary, inventory.

There are many reasons why it is important for management at Target to have knowledge about cybersecurity. According to Abi (2022), the society is more rely on technology than before, and the trend is rising up as well. There are many kinds of information that should be protected by cybersecurity such as business strategies, sensitive information, personal information. Cybersecurity is not only about digital, so is the psychical security to any one of us. In today's world, data breaches are becoming increasingly common, and if a company is not prepared to handle them, they can be devastating. A data breach can not only lead to the loss of customer data, but also to the loss of customer trust and confidence. By understanding cybersecurity and being prepared for a breach, Target can help to protect its customers and its own reputation.

Target has focused on six main threat/vulnerability pairs.

1. Malware – Third-party vendor’s account and password.
2. DDoS - Database server can be accessed by UDP (User Datagram Protocol) with public internet, and spoofing of IP (Internet Protocol) address allows it to response it.

3. Cloud storage misconfiguration - Cloud storage can be accessed without password and the other authentication.
4. Phishing - Remote workers accidentally provide hackers with login privileges via e.g., Twitter or email.
5. Flooding - Some buildings of the company are in low-lying areas that are vulnerable to flooding
6. Earthquake - Buildings in an earthquake area.

Target has three main organizational objectives they would like to achieve:

1. Provide a wide range of affordable and high-quality products
2. Support community, charity, bushfire
3. Be an environmentally friendly company

The six threat/vulnerability pairs above are likely to affect these organizational objectives. Firstly, Flooding and Earthquake are going to cause a huge damage in the supply chain for industry. Carey(2020) reported that an earthquake initiates Tsunami in Japan in 2011 costed 210 billion for the supply chain. Globe business such as Toyota and Nissan are necessary to shut down factories in America and Japan temporarily. If natural disasters like earthquake and flooding happened in Target's factories, it will affect a stable supply of products. Invest in draining machines and systems can help companies control the damage from flooding within a short time. And more, locating companies in an area less prone to earthquakes is the most stable solution.

The second objective is Support community, charity, bushfire which are more related to company's reputation. For charity and bushfire rebuilding plan, it usually requires companies to organise donations. Phishing is the easiest way used to stolen money from people. Wagner (2020) indicated that Remote workers accidentally provide hackers with login privileges via twitter, caused some user lost bitcoin. Hacker uses social engineering to obtain login credentials and post fake URL link in social media lead to account lost money on Internet. Conducting

security awareness program for employees regularly can increase employee's awareness, it is an expensive cost for each company, but efficient for companies solve it.

Moreover, the Target USA has been through a cyberattack in 2015. In this incident, third-party company was compromised by cybercriminals. Forty million credit cards, debit cards and seven million customer records were stolen (Jones, 2021). Stempel (2020) found that hacker compromised third-party vendor's accounts and passwords to install malware in the inner network. Even the cybercriminals are not attack Target Australia at first time, but the cyber-attack like Malware, DDoS, misconfiguration or any kind of human error can be threat of Target Australia.

Risk Management Plan

Threat	Threat Agent, Intentional / unintentional	Asset	Asset Value	EF, ARO	Vulnerability	Exploit	Organisational Risk Impact (H, M, L)	Risk Mitigation	Justification	Annualized Control Cost
Malware	Technology, intentional	Customer purchase history	500,000	40%, 6	Third-party vendor's Account and password	Hacker use Third-Party's account to install malware in the inner nework of target.	M	Review and update user authenication	Will ensure more secure access control and authentication	20,000
DDoS	Technology, intentional	database server	50,000	20%, 10	database server can be access by UDP with public internet, and spoofing of IP address allows it to response it	The server was flooding by a huge number of spoofed requests	M	Install DDOS protection mechanism	DDOS protection can help company to stop a big scale attack when it just initiated	$35,000

Cloud stroage misconfiguration	Human / unintentional	Metadata of CVS Health Systems	500,000	30%, 0.5	Cloud stroage can be accessed wothout password and the other authentication	database is not protected by authentication	M	Perform vulnerability scanning	Company should moniting the change of cloud stroage configuration and doing a vulnerability regularly.	$10,000
Phishing	Human / intentional	Company social media account	10,000	10%, 3	Remote workers accidentally provide hackers with login privileges via twitter	Hacker uses social engineering to gain login details	L	Company to conduct security awareness program for remote workers	Remote worker didn't check if the request of privileges are real.	$10,000
Flooding	Environment / unintentional	Computers	$ 3 million	50%, 1	Some buildings of company are in low-lying areas	Low-lying surface make it hard to drain water , extreme climate cause compous affected by raining and flooding	M	Invest in draining mechine and system	compare with relocate whole campous, invest in draining system are more economical	$8,000
Earthquake	Environment / unintentional	Company buildings	$10 million	90%, 2	Biuldings in an earthquake area	Earthquake	H	Relocate to areas less prone to earthquakes	Earthquake is inevitable, but stay away from the hotspot of earthquake are best way.	$10,000,000

According to approximate guide, high EF and low ARO result in Median organization risk impact. Considering rebuilding a structure and relocating is a significant impact for a company, we put High in organization risk impact.

RACI Chart

	Project manager	Facility manager	Human resource	IT Manager	Chief Technology officer	Network Administrator	Security Department
Review and update user authenication	-	I	-	C	A	R	-
Install DDoS protection mechanism	-	-	-	A	I	R	-
Perform vulnerability scanning	-	-	-	A	I	R	-
Company to conduct security awareness program for remote workers	-	-	I	I	C	-	R
Invest in draining mechine and draining system	A	R	-	I	I	-	-
Relocate to areas less prone to earthquakes	A	R	-	C	C	-	-

Justifications

	Project manager	Facility manager	Human resource	IT Manager	Chief Technology officer	Network Administrator	Security Department
Review and update user authenication	-	I	-	C	A	R	-

Review and update user authentication:

- The Network administrator is responsible for reviewing and updating user authentication, ensuring access control and authentication are the latest.

- While Network administrator is leading this project, Chief Technology officer is accountable for making sure the implement is done well.
- Usually, IT manager and its team can consult some useful information to responsible unit (Network administrator) for enhancing the security.
- Facility managers need to be informed, in case facility manager not sure which authentication is changed

	Project manager	Facility manager	Human resource	IT Manager	Chief Technology officer	Network Administrator	Security Department
Install DDoS protection mechanism	-	-	-	A	I	R	-

Install DDoS protection mechanism:

- The Network administrator is responsible for installing DDoS protection mechanism, ensuring network traffic is safe.
- IT manager is accountable for leading a white box testing for this project, make sure the protection mechanism is working.
- Chief Technology Officer would like to be informed after the DDoS protection mechanism is applied.

Analysis and recommendations

TV pair (from section 1)	Critical, Normal, Minor?	Likelihood (within the next 12 months) (0-100)	Impact (0 -1)	Risk Value
TV 1	N	65	0.9	58.5
TV 2	N	80	0.8	64
TV 3	M	20	0.8	16
TV 4	M	30	0.9	27
TV 5	M	30	1	30
TV 6	M	30	1	30

Cost Benefit Analysis

TV Pair	Asset	Asset Valuation	Exposure Factor	Single Loss Expectancy	Annual Rate of Occurrence (pre-control)	Annualized Loss Expectancy (pre control)	Annualized Control Cost	Annual Rate of Occurrence (post-control)	Annualized Loss Expectancy (post control)	Cost Benefit Analysis
		AV	EF	SLE = AV * EF	ARO	ALE=SLE*ARO	ACC	ARO_1	ALE=SLE*ARO_1	CBA = ALE_{pre} - ALE_{post} - ACC
1	Customer purchase history	500,000	40%	200,000	6	1,200,000	20,000	2	400,000	780,000
2	Database server	50,000	30%	15,000	10	150,000	35,000	4	60,000	55,000
3	Metadata of CVS Health Systems	500,000	30%	150,000	0.5	75,000	10,000	0.25	37,500	27,500
4	Company social media account	10,000	10%	1,000	3	3,000	10,000	3	3,000	(10,000)
5	Computers	3,000,000	50%	1,500,000	1	1,500,000	8,000	1	1,500,000	(8,000)
6	Company buildings	10,000,000	90%	9,000,000	2	18,000,000	10,000,000	2	18,000,000	(10,000,000)
										844,500

Recommendations

According to the recommendations to rewrite it

This section will provide recommendations to what actions the management of Target should take to ensure they are secure from the threats introduced earlier.

TV 1 - Malware

As can be seen in the risk evaluation, this TV pair has a high-risk value. This team still believes that Target should try to defend this asset by applying various controls. This is because some controls are easy to implement and they can decrease the threat a lot. From the cost-benefit analysis, we have estimated that by implementing such controls we can decrease the ARO and the benefit is close to $780 000. Some of the controls Target can implement will be explained below.

Malware can be used to steal information, such as third-party vendor's account and passwords. Malware usually occurs when employees click into maliciously email attachments or fake internet ads. Target could therefore implement email security controls limit the amount of unwanted incoming emails. Software developers are providing patches regularly to ensure the new threats are being closed (Brooks, 2020). Therefore, Target must implement updating user's authentication to defense threat like malware. Must implement routines and reviewing update

TV 2 - DDoS

DDoS attacks have a high risk-value. This is usually done in by sending an overwhelming the amount of packages. Target is a retail company, there are thousands of products on its website. Any people are potential customer to Target. In order to protect accessary of Network, Target should install a DDoS protection for server. It can help Target defense this kind of cyberattack when DDoS attack still in an initial stage. Yet, there exists technology controls that help company lower this risk a great amount, and saving $55,000 per year. We will therefore advice Target to choose a defense strategy for this TV pair. Recommendations for technology controls that can be implemented will be discussed down below.

TV 3 - Cloud storage misconfiguration

Cloud storage misconfiguration also has a low-risk value. Yet, cloud storage is a very important asset for a big company like Target that possess a very large amount of data. The option of transfer this risk to other entitles is therefore excluded, as well as terminating or accepting the threat. This team will advise target to choose a mix between defense and mitigation strategy. First of all, they will need to apply defense controls to reduce the threat they are facing, but also reduce the impact on the asset if an attack should occur. This it is very difficult to reduce cloud misconfiguration threat 100%.

There is a big chance for every company occurred a cloud storage misconfiguration. Especially when company is keep expanding. Cloud configuration should keep updating frequently. Lisa (2021) reported that 1.1 billion customers information are exposed to pubic. In this case, a vendor access into database server without any authentication and password. Target should be ware about cloud configuration due to Target has a member system. A member system usually contains a huge number of customer information like name, bank, card number and address. Company should keep monitoring the change of cloud storage, and conducting vulnerability scanning frequently, can help Target defensing breach leak or misconfiguration.

TV 4 - Phishing

This TV pair has a low-risk value. It is also a threat that can be easily avoided by implementing some defense mechanisms.

The biggest reason that Target should implement security awareness program for employees, is that phishing can entraining the other attack. Some of the attacks explained in the recommendations. Phishing is the part where the attackers send out trustworthy links or messages and hopes that people might click on them, malware can be existed in the links. The most effective way of preventing phishing attacks is security awareness program for employees. Human error is the most common vulnerability for hacker.

TV 5 - Flooding

Flooding has medium- risk value for Target, this team suggest two risk treatment strategies mitigation and acceptance.

Natural disasters sometimes are inevitable, there are many reasons that lead flooding to occur. While the flooding occurs, the worst thing is not just stopping traffic, but stopping the supply chain. Polycarpou (2014) shows that a study about how flooding impact car industry in Thai land. A flooding reduced production for global industry by 2.5 proportion in 2011. Most famous car companies like Nissan, Honda and Toyota, lost 33,000, 150,000, 240,000 cars respectively. A retail company like Target relies on a stable supply chain to supply products for trading. Compared with defense flooding, accepting and using a mitigation could have a real effect on this threat. An alternative plan for mitigation like investing in a draining system and machine. Although, it will cost $8,000, but it can help companies mitigate flooding rapidly.

TV 6 - Earthquake - Buildings in an earthquake area.

Earthquake has a medium-risk value for Target, seems it is an acceptable disaster. When it is happened to Target, it could cause a big impact. This team suggest Target acceptance and mitigation.

Earthquake is an action that earth releases energy from Crust. After the earthquake occurred, there is a good chance that a Tsunami is going to hit the coastline city or town in a few minutes. The most efficient way to avoid the impact of earthquakes is choosing a location or relocating to an area less prone to earthquakes. According to Washington Office of Superintendent of public instruction, a report describes six methods for earthquake. One of the mitigations straight to the point about what if the building needs to repair and maintenance frequently. Relocating sounds very expensive, and not all companies can be afraid of it, but it is the most efficient way to fix the impact from earthquake. Earthquake is a truth that people can only accepted its existence. Target has a lot of branches around the world, of course not all branches are in an earthquake area. Moreover, a mitigation for searching an area is less prone to earthquake can help Target avoiding rebuilding local branch.

Appendix – Teamwork Reflection

Separate into 5 different paragraph and fit the task based on the task sheet

Team process

The Team Orientation meeting was organized soon after the group formation. The meeting was informal discussion with the members sharing their background, their previous education and

experience, and their interest. Later, we assigned some roles for each member like **Meeting chair** responsible for schedule some to-do list and try to complete it within timeline, **Clarifier** and solution searcher actively work towards problem identification and solution, **Wellness checker** is making sure teammates are feeling well, supported, and comfortable.

The next meeting started with the focus on the discussion about the completion of the Assignment Task. The members concentrated on preparation of the plan of action, with sharp deadline for the course of action towards the assignment tasks. It was agreed by the team that the members would initially work individually on the specific part of the assignments. Therefore, the division of the work based on the assignment sections were assigned to the team members. The individual works were combined through number of the team members discussions – physically, and electronically.

The three parts Risk Management Plan, RACI chart, Analysis and Recommendations of the assignment assigned to the three team members were based on their interest.

1. A team member explained information security threats relevance to client. And table entries for each threat, threat agent, Intentional / unintentional, asset, asset value, EF/ARO, vulnerability, exploit, Risk impact, mitigation, justification, annual cost control.
2. The team member provides a list of six relevant mitigations, allocate roles and responsibilities to personnel for each mitigation and justifications for 3 mitigations
3. Another team member presents a spreadsheet TV Pair, Asset, Asset Valuation, Exposure Factor, Single Loss Expectancy, Annual Rate of Occurrence(pre-control), Annualized Loss Expectancy(pre-control), Annualized Control CTSS, Annual Rate of Occurrence (post-control), Annualized Loss Expectancy (post control), Cost Benefit Analysis and recommendations with justification

Reflection for planning and performance

The least effective approach among the team members was the knowledge gap during the learning process. One member was advanced in concepts in which the other member was lacking completely. The less experienced member took time to understand and required time to pick-up some concepts and understanding.

The team members where from different countries, the knowledge and background of the members were quite different. Such diversity in the teamwork is common in the workplaces and paradigmatic shift in thinking and learning emerged as part of the assignment activity. This unique approach in the assignment requires a different way of learning and relationship. This is the key for the success in our future workplaces.

The group assignment was the enriching learning experience, with the success dependent on the individual efforts of the team members, and the uniting group efforts. Overall, the group assessment work helped to complete the assessment successfully with different perspective and ideas recognized and included as part of the assessment work.

Bibliography

Amazon. (2022, October 22). *What is a DDoS Attack?* https://aws.amazon.com/shield/ddos-attack-protection/

Abi, T. (2022, October, 20) *Why is Cybersecurity Important?* https://www.upguard.com/blog/cybersecurity-important#toc-1

Brooks, R. (2020, June 12). *How to Prevent Malware Attacks: 10 Security Tips.* https://blog.netwrix.com/2020/06/12/malware-prevention/

Carey, H. (2020, August 19). *The impact of Natural Disasters on Economy and Supply Chain - and How to Prepare for the Worst.* https://www.thomasnet.com/insights/how-natural-disasters-affect-the-supply-chain-and-how-to-prepare-for-the-worst/

Jones, C. (2021). *Warnings (& lessons) of the 2013 Target data breach.* https://redriver.com/security/target-data-breach

Lisa, V. (2021, June 17) *CVS Health Records for 1.1 Billion Customers Exposed* https://threatpost.com/cvs-health-records-billion-customers-exposed/167011/

Polycarpou, L. (2014, November 17). *Floods, Companies and Supply Chain Risk.* https://news.climate.columbia.edu/2014/11/17/floods-companies-and-supply-chain-risk/

Stempel, J. (2020, November 15). *Home depot reaches $17.5 million settlement over 2014 data.* https://www.reuters.com/article/us-home-depot-cyber-settlement/home-depot-reaches-17-5-million-settlement-over-2014-data-breach-idUSKBN2842W5

Sukianto, A. (2022, May 1). *Common Cloud Misconfigurations and How to Avoid Them.* https://www.upguard.com/blog/cloud-misconfiguration

Target Australia. (2022, October 10). *Wikipedia.* Retrieved from Target Australia: https://en.wikipedia.org/wiki/Target_Australia

Trend Micro. (2019, September 13). *Trend Micro.* Retrieved from Recognizing Enterprise Mission-Critical Assets: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/recognizing-enterprise-mission-critical-assets

Wagner, K. (2020, July 17). *Twitter says hackers targeted 1130 accounts in cyber-attack.* https://time.com/5868008/TWITTER-HACK-ACCOUNTS-TARGETED-BITCOIN-SCAM/

Washington Office of Superintendent of public instruction. (u.d.). https://www.k12.wa.us/sites/default/files/public/schfacilities/pdm/pubdocs/mitigation_measures_summary.pdf