Assignment-1

CS 573 A - Introduction to Cyber Security

FALL 2021

Rajat Rajesh Shetty CWID: 10477484

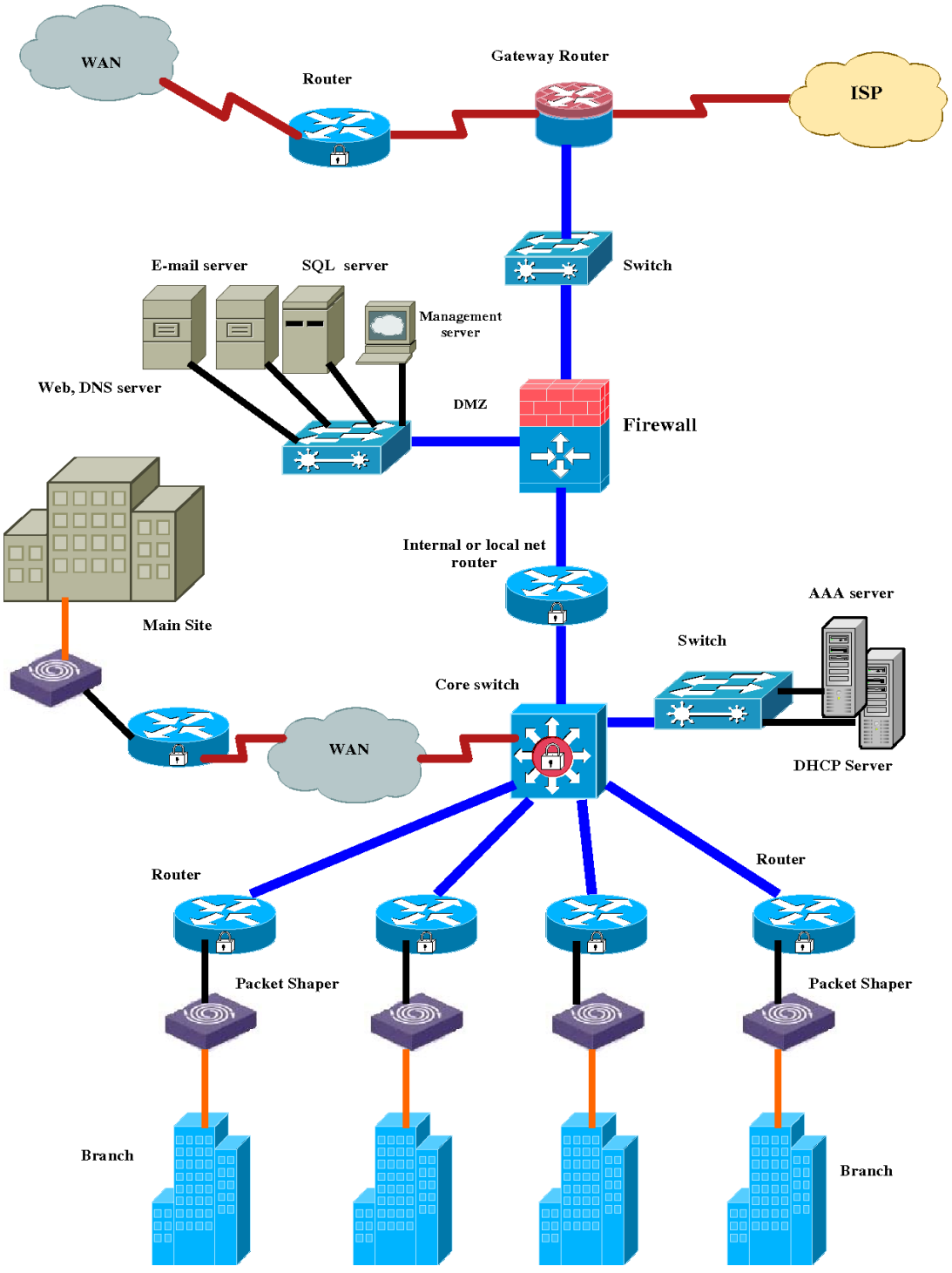
Dept. Cyber Security

Stevens Institute of Technology

Content

INTRODUCTION

This is a detailed threat assessment of a Security service provider company. It is an enterprise that provides security services to its client and also has its product.



Fictitious Enterprise Network of Company that provides security

Threat-Asset Matrix for Security Service Provider Company

Assets	Confidentiality	Integrity	Availability	Theft/Fraud
Product Prototype	P=3, C=3 | R=9	P=1, C=3 | R=3	P=2, C=2 | R=4	P=3, C=3 | R=9
Client Data	P=3, C=3 | R=9	P=3, C=3 | R=9	P=2, C=3 | R=6	P=3, C=3 | R=9
Algorithm	P=3, C=3 | R=9	P=3, C=3 | R=9	P=2, C=3 | R=6	P=3, C=3 | R=9
Firewall	P=2, C=3 | R=6	P=2, C=3 | R=6	P=1, C=2 | R=2	P=1, C=2 | R=2
Developer MAC	P=2, C=3 | R=6	P=2, C=3 | R=6	P=1, C=2 | R=2	P=1, C=2 | R=2
Developer Mobile	P=2, C=3 | R=6	P=2, C=3 | R=6	P=1, C=2 | R=2	P=1, C=1 | R=1
Cloud Storage (Software source code)	**P=3, C=3 | R=9**	**P=3, C=3 |R=9**	**P=3, C=3 | R=9**	**P=3, C=3 | R=9**
Website	P=1, C=1 | R=1	P=2, C=3 | R=6	P=1, C=2 | R=2	P=1, C=1 | R=1
Email/Office 365	P=3, C=3 | R=9	P=3, C=3 | R=9	P=2, C=3 | R=6	P=3, C=3 | R=9
Employee Privilege Accessibility	P=3, C=3 | R=9	P=2, C=3 | R=6	P=1, C=2 | R=2	P=2, C=3 | R=6
Payroll	P=2, C=2 | R=4	P=1, C=3 | R=3	P=1, C=2 | R=2	P=1, C=2| R=2
Infrastructure	P=1, C=2 | R=2	P=1, C= 1| R=1	P=1, C=3 | R=3	P=1, C=3 | R=3
LAN,DMZ Switch	P=1, C=1 | R=1	P=1, C= 1| R=1	P=1, C=1 | R=1	P=1, C=1 | R=1

P- Probability | C- Consequences | R-Risk | R= P*C

Range: 3 = High, 2 = Medium, 1 = Low

Business Asset	Estimated Risk
Cloud Storage (Software source code)	Total Risk = 36 – 1st Highest Risk Asset
Client Data	Total Risk = 33 –2nd Highest Risk Asset
Algorithm	Total Risk = 33 – 3rd Highest Risk Asset
Email/Office 365	Total Risk = 33 – 4th Highest Risk Asset
Product Prototype	Total Risk =25 – 5th Highest Risk Asset
Employee Privilege Accessibility	Total Risk = 23 – 6th Highest Risk Asset
Developer MAC	Total Risk = 16 – 7th Highest Risk Asset
Firewall	Total Risk = 16 – 8th Highest Risk Asset
Developer Mobile	Total Risk = 15 – 9th Highest Risk Asset
Payroll	Total Risk = 11 – 10th Highest Risk Asset
Website	Total Risk = 10 – 11th Highest Risk Asset
Infrastructure	Total Risk = 9 – 12th Highest Risk Asset
LAN,DMZ Switch	Total Risk = 4 – 13th Highest Risk Asset

Explanation

Product Prototype

Confidentiality(R=9): This is very important for competitors and it's always at **high risk**.
Integrity(R=3): The probability of this happening is less so, the risk is **low** and if it does and the competitor gets access to this prototype then the prototype can be changed and a new prototype can be formed.
Availability(R=4): Since it won't be easily available the Risk would be **medium**.
Theft/Fraud(R=9): Since it's very important and can be a game-changer so if it's stolen, the competitors can build the same protocol and modify few things and use it for their benefit. So, the risk is **high.**

Client Data

Confidentiality(R=9): This is very important and it's always at **high risk**.
Integrity(R=9): The client information can be misused and if someone is into a security business they can try to sell their product at a lower cost. As a reason, we will lose a client, so the risk is **high**.
Availability(R=6): Client data won't be easily available because it will be confidential and getting access to it will be difficult. So the risk is **medium**.
Theft/Fraud(R=9): If the client Data is stolen then it will be a huge loss to the company so the risk is **very high**.

Algorithm

Confidentiality(R=9): This is very important for everything as it's the base at which the product is been coded so the risk is **high**.
Integrity(R=9): So if the person gets access to the algorithm things can be changed and it can have severe consequences. So the risk is **high.**
Availability(R=6): Generally it will be secured and it won't be made available to the public so the risk is **medium**.
Theft/Fraud(R=9): If someone gets unauthorized access and copies the algorithm then that can be sold to competitors so the risk is **high**.

Firewall

Confidentiality(R=6): When we talk about firewalls the probability of getting access is not high the only possible way to get access would be through some open ports so the risk would be **medium**.
Integrity(R=6): If someone does get access to the firewall then the firewall settings can be changed and changes are altered so the risk is **medium**.
Availability(R=2): Getting access to it won't be easy and there will be a separate team who will monitor if there is some port that is been opened and if it's been accessed by an unauthorized person. So the risk is **low**.
Theft/Fraud(R=2): The risk would be **low** as it is been well monitored and if it's been used by someone then it will be detected.

Developer MAC

Confidentiality(R=6): So the Source code in development on MAC is valuable to competitors but Mac is reasonably well protected against malware and that's the reason the risk is **medium**.
Integrity(R=6): So if someone gets access then the source code can be modified. Thus, the risk is **medium**.
Availability(R=2): It won't be easily accessible and available so the risk is **low**.
Theft/Fraud(R=2): Since it's a MAC even if it's stolen it will be difficult to open it without an authorized username and password. So the risk is **low**.

Developer Mobile (iPhone)

Confidentiality(R=6): Since contacts and emails will be available it is valuable for competitors so the risk is **medium**.
Integrity(R=6): So if someone gets access then malware can be installed and confidential emails can be read. So the risk is **medium**.
Availability(R=2): Even though developers Mobile is available it might be locked or 2-step authentication will be enabled so the risk is **low**.
Theft/Fraud(R=1): Since IOS devices are well secured so even if it's stolen it cannot be opened by an unauthorized person. The risk is **low**.

Cloud Storage (Software source code)

Confidentiality(R=9): Since it's sensitive content it is very important and if these things are stored on public clouds then the risk is very **high** as well.
Integrity(R=9): Source code can be modified and security features can be switched off by the competitors so the risk involved is **high**.
Availability(R=9): As the software will be available for general public usage so the risk is **high** as hackers can maliciously block authorized users and thereby use client data.
Theft/Fraud(R=9): If it's stolen then it will be a huge loss to the company and thereby the risk would be **high** as well.

Website

Confidentiality(R=1): Website reasonably well-administered but nothing all that sensitive is stored in the marketing-oriented site so the risk is **low**.
Integrity(R=6): Things on the website can be modified like the contact us details and thereby it will help competitors to get those clients. So, the risk is **medium**.
Availability(R=2): Since it's available and even if authorized people are blocked it won't be a major concern. The risk is **low**.
Theft/Fraud(R=1): The risk associated with this is **low** since it's more of an advertising website.

Email/Office 365

Confidentiality(R=9): Since sensitive data related to the product are discussed and share here, the risk is **high**.

Integrity(R=9): Emails and PDFs can be modified and discussion with the client can be changed as well so the risk is **high**.
Availability(R=6): It will be available for the employees for reference but unauthorized access will be blocked so the risk is **medium**.
Theft/Fraud(R=9): This sensitive information can be stolen and sold to competitors thereby exploiting the threats of the client and also phishing links can be sent to the client. So the risk is **high**.

Employee Privilege Accessibility

Confidentiality(R=9): This is very important as every company will have a different level of accessibility and if someone gets full access then it will be very risky so the risk is **high**.
Integrity(R=6): The probability of this happening is medium and if it does happen then the privileged access can be modified and unauthorized people can be given access. So the risk is **medium**.
Availability(R=2): The privileged access will be available only for the employees so the risk is **low**.
Theft/Fraud(R=6): If the access is stolen then sensitive information can be sold to the competitors and malware can be installed as well. So the risk is **medium**.

Payroll

Confidentiality(R=4): Again this is sensitive information as access to this will give the competitors a chance to hire some of the developers by giving them 1.5 times the salary that they are currently offered. So the risk is **medium**.
Integrity(R=3): Changes can be done and instead of getting a $1000 salary a person might be getting $1200. Since the possibility is low the risk is **low** as well.
Availability(R=2): It's sensitive data and it will be restricted to a particular person and not made available to anyone, the risk is **low**.
Theft/Fraud(R=2): If it's stolen and sold to a competitor then they might buy the Employee at a much higher salary (Loss of talent) so the risk is **medium**.

Infrastructure

Confidentiality(R=2): When we talk about the infrastructure even though it has sensitive information it will be hard to sneak in so the risk is **low**.
Integrity(R=1): No changes can be made so the risk is **low**.
Availability(R=3): It is available to employees but will prevent unauthorized access so the risk is **low**.
Theft/Fraud(R=3): In general cases, the infrastructure will be well guarded so the probability of risk is **low**. On the other hand, if someone still manages to sneak inside the premises and finds a hard disk containing sensitive information it can be misused or sold. So the risk is **medium**.

LAN/DMZ Switch

LAN and DMZ Switch are used to route different servers to different zones and networks and do not necessarily affect the CIA of the overall system

THANK YOU