Midterm Assignment

Pawan Kumar

Department of Computer Science, Stevens Institute of Technology

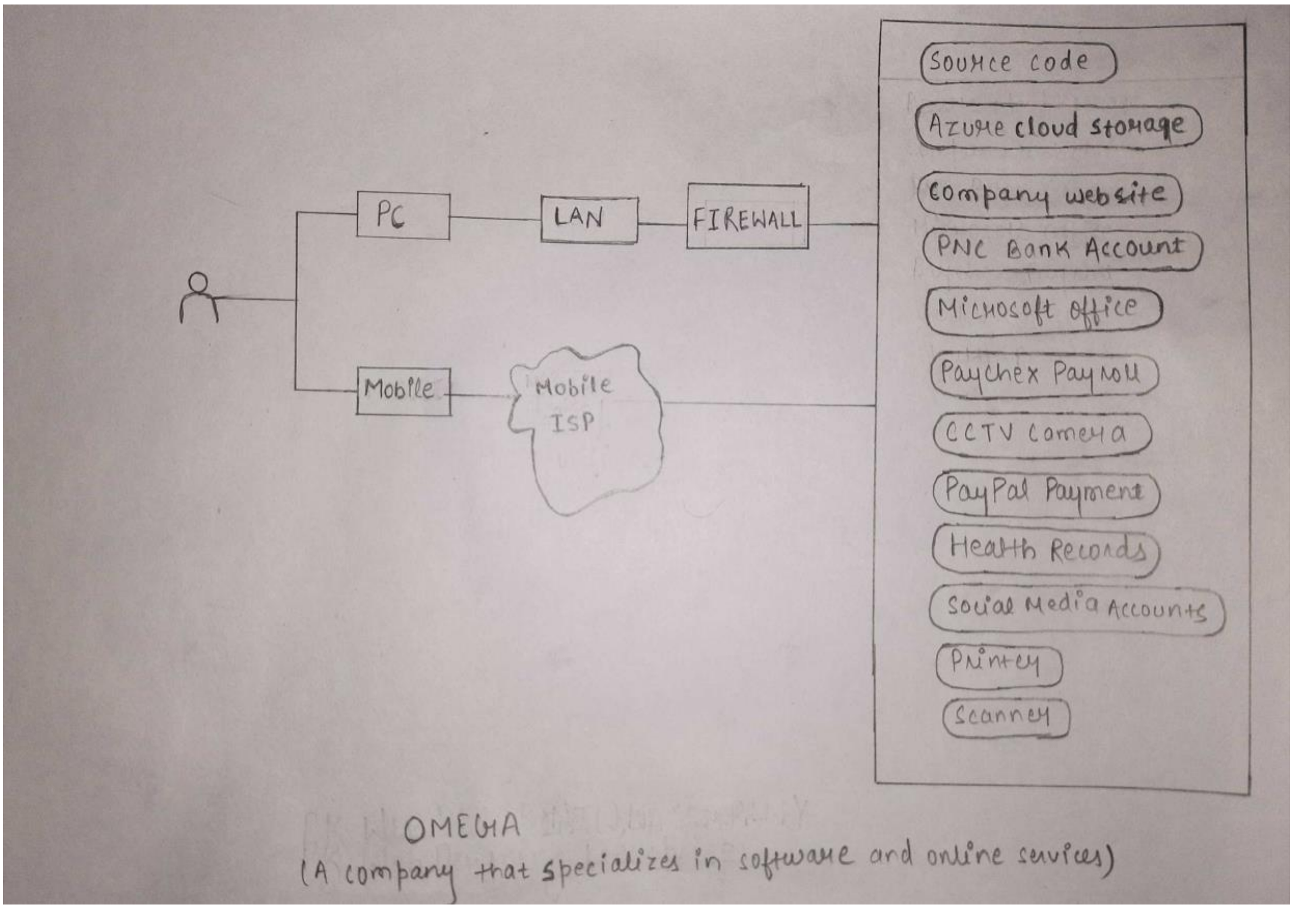
CS 573-A, Fundamentals of Cybersecurity

Dr. Edward Amoroso

March 9th, 2022

Assignment

Q) Identify and describe a fictitious enterprise network (you can draw or describe) and carefully list the valued assets for this network. (It would be recommended to keep the number of assets more than 10 but less than 25). Then, create a threat-asset matrix for your fictitious example and estimate the security risk for each individual cell in the matrix. Write a 1-2 sentence justification for each risk estimate. You are welcome to draw the matrix by hand (scan and cut the image into your paper) or you can use a tool such as Excel or PowerPoint.



OMEGA

(A company that specializes in software and online services)

Four Major threat types: -

1. Confidentiality

2. Integrity

3. Availability

4. Theft/Fraud

Assets mentioned in the enterprise: -

1. Source Code

2. Mobile Phone

3. PC

4. Firewall

5. Azure Cloud Storage

6. Company Website

7. Local Area Network

8. PNC Bank Account

9. Microsoft Office

10. Paychex Payroll (For billing employees' salary)

11. Closed-Circuit Television (CCTV Camera)

12. Health Records (Aetna Health Insurance)

13. Social Media Accounts

14. Printer

15. Scanner

16. PayPal Payment

Calculation of Risk: -

P = Probability, C = Consequences,

R = Risk (P *C)

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

Threat Asset Matrix: -

Assets/Threats	**Confidentiality**	**Integrity**	**Availability**	**Theft/Fraud**
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
Mobile Phone	P=2, C=3, R=6	P=1, C=2, R=2	P=1, C=2, R=2	P=1, C=2, R=2
PC	P=2, C=3, R=6	P=1, C=2, R=2	P=1, C=2, R=2	P=1, C=2, R=2
Firewall	P=3, C=3, R=9	P=3, C=3, R=9	P =1, C=3, R=3	P=1, C=1, R=1
Azure Cloud Storage	P=3, C=3, R=9	P=3, C=3, R=9	P=3, C=3, R=9	P=3, C=3, P=9
Closed-Circuit Television (CCTV Camera)	P=2, C=1, R=2	P=2, C=1, R=2	P=2, C=1, R=2	P=2, C=3, P=6
Social Media Accounts (Company or Employee account)	P=2, C=1, R=2	P=2, C=2, R=4	P=1, C=1, R=1	P=2, C=3, R=6
Company Website	P=2, C=2, R=4	P=2, C=2, R=4	P=1, C=3, R=3	P=2, C=3, R=6
Local Area Network	P=1, C=2, R=2	P=1, C=2, R=2	P=1, C=2, R=2	P=1, C=2, R=2
PNC Bank Account	P =1, C=2, R=2	P =1, C=2, R=2	P=1, C=1, R=1	P=2, C=3, R=6
Microsoft office	P=2, C=3, R=6	P=2, C=3, R=6	P=1, C=3, R=3	P=1, C=1, R=1
Paychex Payroll	P =1, C=2, R=2	P=1, C=2, R=2	P=1, C=1, R =1	P=1, C=1, R=1
Scanner	P=1, C=1, R=1	P=1, C=1, R=1	P=1, C=1, R=1	P=2, C=1, R=2
Health Records (Aetna Health Insurance)	P=2, C=1, R=2	P=2, C=1, R=2	P=1, C=1, R=1	P=2, C=3, R=6
Printer	P=1, C=1, R=1	P=1, C=1, R=1	P=1, C=1, R=1	P=2, C=1, R=2
PayPal Payment	P=3 C=3, R=9	P=1 C=3, R=3	P=1 C=3, R=3	P=1 C=3, R=3

Source Code: - As organizations of all types are increasingly defined by their software, protecting source code can be equivalent to protecting the business itself. A source code breach could mean the loss of a business' primary competitive advantage or exposure of your proprietary business logic to attackers and competitors. So, a high-risk asset.

Mobile Phones: - Now a days, phones are having fingerprint or face recognition system to unlock the phone which makes it difficult to steal information, even if the phone is in wrong hands. But, if the phone is being hacked using phishing or something else, then hacker can see the sensitive documents related to work or might see personal data. So, Phones are medium risk assets.

PC: - Laptop and work desktops are well protected from hackers using multilayer securities.

Firewall: - A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet. As firewall act as a defence against cyberattacks, so if firewall is breached then there is a chance hackers can see sensitive data from the devices.

Azure Cloud Storage: - It is a very high-risk asset, as it stores a large amount of data and many other sensitive information and files of a company.

Closed-Circuit Television (CCTV Camera): - If a CCTV of a company is hacked then it does not do any damage, unless a hacker can see someone laptop screen from company clearly and may see some data. Usually, CCTV are installed at high position, so not an issue.

Social Media Accounts (Company or Employee account): - Most companies have a social media page on different platforms for marketing of their company. If it is hacked then hackers can use it to post false information about the company which may damage the reputation of the company.

Company Website: - If a company website is compromised, then client information can be stolen.

Local Area Network: - Difficult to access information. Low risk asset.

PNC Bank Account: - Hackers can also operate by planting malicious software known as malware on a company computer, often via an email that has a link or attachment. If the computer is used to log into a bank account, the malware can record the login and password and send it back to the criminals, who then withdraw funds.

Microsoft office (Email, Calendar etc): - Hackers may sent corrupt email containing a link to get the data but as long as the link is not opened by the receiver, he/she is fine.

Paychex Payroll (For billing employees' salary)-Suppose when OMEGA Company hire Paychex payroll, to handle their employees' payroll and Paychex is hacked then the data of employees of OMEGA also gets compromised. Medium Risk Asset.

Health Records (Aetna Health Insurance): - Employees' health information can get compromised if the company handling the health insurance is under cyber-attack. Low risk asset.

Printer/Scanner: - Does not contain any sensitive information. Low risk asset.

PayPal Payment: - Not easy to get information about a company payment method or hack into it. Medium risk asset

Asset	**Estimated Risk**
Source Code	Total Risk = 36 - 1st Highest Risk Asset
Mobile Phone	Total Risk = 12- Medium Risk Asset
PC	Total Risk = 12- Medium Risk Asset
Firewall	Total Risk = 22 – 2nd Highest Risk Asset
Azure Cloud Storage	Total Risk = 36 – 1st Highest Risk Asset
CCTV Camera	Total Risk = 12 – Medium Risk Asset
Social Media Account	Total Risk = 13 – Medium Risk Asset
Company Website	Total Risk = 17 – 4th Highest Risk Asset
Local Area Network	Total Risk = 8 - Low Risk Asset
PNC Bank Account	Total Risk = 11 – Medium Risk Asset
Microsoft Office	Total Risk = 16 – 5th Highest Risk Asset

Paychex Payroll (For Billing Employee's Salary)	Total Risk = 6 - Low Risk Asset
Health Records (Aetna Health Insurance)	Total Risk = 11 – Medium Risk Asset
Printer	Total Risk = 5 - Low Risk Asset
Scanner	Total Risk = 5 - Low Risk Asset
PayPal Payment	Total Risk = 18 – 3rd Highest Risk Asset