CS-573
Assignment 1

Estimating Risk for Threat-Asset Pairs

(Harshala Yadav)

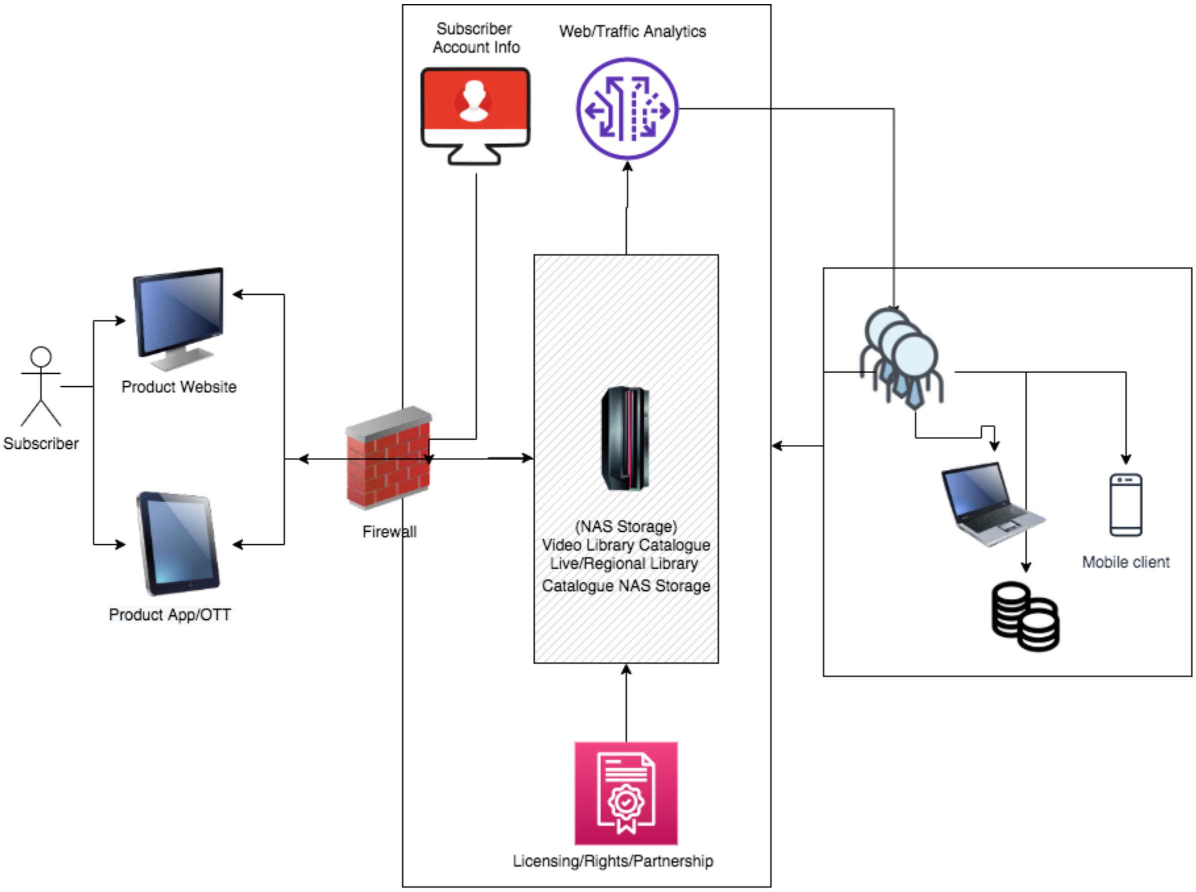
Estimating Risk for Threat-Asset Pairs

1. Fictitious Enterprise Network

The following document describes a basic cyber security threat and risk analysis, and how the threat-asset matrix can be used to determine the risk level for the different assets for a given company. The primary objective of this analysis is to map the company's "*Assets*" to the "*Threats*" to determine the risk for a given enterprise network. Quantitative evaluation using the threat/asset matrix will help justify the risk and lead to corrective recommendations on the analyst's part.

2. Company Information and Network

Paramount+ is a streaming service product for a major media company whose primary source of revenue is subscription. The secondary source of revenue is via ads for subscribers who choose a commercial-based plan. The streaming service offers movies, TV shows from the company's proprietary catalogue as well via licensing deals with partners. The subscription product also features live news coverage on a national and regional level. Sports is another category popular with consumers with the media company holding rights to major sports national and international rights. The games are streamed live in conjunction with the broadcast television coverage – covering both national as well as regional games at the high school, college, and national level.



3. Assets:

a) Product

1. All Access Website
2. All Access Mobile/OTT App

b) Backend/Database

1. Web Analytics/Traffic Portal
2. Video Library/Catalogue NAS Storage Server
3. Live/Regional Library Catalogue NAS Storage Server

c) License/Rights/Partnership

1. Movie/TV Show/Sports/News/Regional Rights

d) Network

1. Router
2. Switch
3. Firewall

e) Customer Support

1. Subscription + Account Info

f) Employer

1. Employee Hardware (PC)
2. Employee Software
3. Employee Communication/LAN
4. Business Support + Financials

4. Risk model

In determining risks associated with the assets identified, a risk model is used for classifying risk i.e. ***Risk = Threat Probability (P) x Magnitude of Consequence (C)***

4.1 Probability of Threat Occurrence

Value	Degree	Definition
3	HIGH	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
2	MODERATE	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
1	LOW	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

4.2 Scale of Consequence

Value	Degree	Definition

3	HIGH	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
2	MODERATE	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
1	LOW	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

5. Risk Assessment Matrix:

	Confidentiality	**Integrity**	**Availability**	**Theft/Fraud**
Product				
Paramount+ Website	2*2 = 4	2*1 = 2	3*1 = 3	3*1 = 3
Paramount+ Mobile/OTT App	1*2 = 2	2*1 = 2	3*1 = 3	1*3 = 3
Backend/Database				
Web Analytics/Traffic Portal	1*1 = 1	1*2 = 2	1*1 = 1	1*1 = 1
Live/Regional/Video Library/Catalogue (NAS Storage Server)	3*3 = 9	2*3 = 6	3*1 = 3	2*3 = 6
License/Rights/Partnership				
Movie/TV Show/Sports/News/Regional Rights	2*3 = 6	2*3 = 6	1*3 = 3	3*3 = 9
Network				
Router	1*2 = 2	1*1 = 1	1*1 = 1	1*1 = 1
Switch	1*1 = 1	1*1 = 1	1*1 = 1	1*1 = 1
Firewall	2*3 = 6	2*3 = 6	2*3 = 6	2*3 = 6
Customer				
Subscription + Account Info	2*3 = 9	1*2 = 2	1*1 = 1	3*3 = 9
Employer				
Employee Hardware (PC)	1*3 = 3	1*2 = 2	1*3 = 3	1*2 = 2
Employee Software	1*3 = 3	1*2 = 2	1*3 = 3	1*2 = 2
Employee Communication/LAN	1*3 = 3	1*2 = 2	1*3 = 3	1*2 = 2
Business Support + Financials	1*3 = 3	1*3 = 3	1*3 = 3	1*3 = 3

6. Risk Assessment Matrix Breakdown / Quantitative Evaluation

a) Product:

1. Paramount+ Website:

Confidentiality: Adequate protections are already in place to secure the website from cyber-attacks. Although zero-day attacks still loom a threat, and the source code of the website is available to tinker with. However, with access to the website via a SQL injection customer data may be exposed although it is limited to demographics, and credit card information (hashed/masked) in this case. Hence, a moderate occurrence probability level and moderate consequence as the subscriber data is limited.

Integrity: Integrity in case of a subscriber based streaming service is important
because the service has news coverage, as well as live games. Timely and accurate news portrayal as well as live and accurate score for live games is of primary importance from the customer's point of view. The consequence level is moderate as an attack website will defunct the company's core revenue generation model. However, with adequate security measures in place the likelihood of it happening are low, hence the Probability of threat occurrence is low.

Availability:
The probability of disruption is high due to the fact that it is the core front facing product for the company – the primary source of revenue in terms of subscription fees and ads. A DDoS attack can take down the availability of live news coverage as well as live games thus garnering subscriber's ire. The consequences of this happening are low as the consumers might get annoyed by the unavailability but are bound to forget about it after a while and care less as most likely there's no personal loss involved.

Theft/Fraud:
Even though adequate security measures are already in place the Probability of threat occurrence is high since it is a matter of simply sharing the access credentials with friends and family to watch the content beyond the paywall with a single subscription. The consequence of this happening is low as this affects a portion of the revenue the company generates. The company regularly identifies and deactivates such accounts and has an "account sharing across multiple-device deterministic detection model" in place.

2. Paramount+ Mobile/OTT App:

Confidentiality:
Adequate protections are already in place to secure the app (based on major OS platforms) from cyber-attacks. Although zero-day attacks and vulnerabilities still loom a threat. The subscriber data is handled by the major mobile OS providers in this case via single sign-on (Android or Apple) or authentication via cable provider and has another layer of security. Hence the Probability of threat occurrence is low. Also, if it would've been a mobile website then the consequence level would've been low as well as it would be the same as attacking the actual website. However, the consequence of this happening is high as it would also expose the customer data for many other apps which the subscriber uses.
Hence, a low occurrence probability level and moderate consequence as the subscriber data is limited.

Integrity:
Integrity in case of a subscriber based streaming service is important because the service has news coverage, as well as live games. Timely and accurate news portrayal as well as live and accurate score

for live games is of primary importance from the customer's point of view. The consequence level is moderate as an attack website will defunct the company's core revenue generation model. However, with adequate security measures in place the likelihood of it happening are low, hence the Probability of threat occurrence is low.

Availability:
The probability of disruption is high due to the fact that it is the core front facing product for the company – the primary source of revenue in terms of subscription fees and ads. A DDoS attack can take down the availability of live news coverage as well as live games thus garnering subscriber's ire. The consequences of this happening are low as the consumers might get annoyed by the unavailability but are bound to forget about it after a while and care less as most likely there's no personal data/financial loss involved.

Theft/Fraud:
Compared to Paramount+ website the Probability of threat occurrence in case of mobile app/OTT is low as the Paramount+ relies on single sign or authentication via cable provider on provided by Google or Apple to sign in the user to the service. The consequence of this happening is high as this affects not only a portion of the revenue the company generates but also puts other subscriber information at risk due to the single sign-on used.

b) **Backend/Database**:

1. **Web/Traffic Analytics**:

Confidentiality:
Probability of threat occurrence is low due to the fact the portal is accessible by employees only and that too on the local LAN. Consequence of happening is low too since a part of this data is already available via B2B products like ComScore or Alexa which tracks website traffic metrics for websites having high number of unique viewers.

Integrity:
Probability of threat occurrence is low due to the fact the portal is accessible by employees only. Consequence of this occurrence is moderate as altering the integrity of this data might mislead a business decision/deal/ad sale but most probably will not have a major impact on streaming service business. And also due to the fact that the evaluation of the analytics data relies on the model of frequency, recency, and monetary (in this case viewers, streams per viewer) value.

Availability:
Probability of threat occurrence is low due to the fact the portal has a fault tolerance mechanism in place and is accessible by employees only. Consequence of threat occurrence is low too as the data is evaluated mostly on a monthly, annual level and not evaluated daily.

Theft/Fraud:
Minimal chance of theft as the data although valuable to competition is available and confidential only to employees on the local LAN. Moderate consequence of fraud as the website traffic data can be used by a competitor to close a streaming deal or an ad deal as well.

2. **Live/Regional/Video Library/Catalogue (NAS Storage Server)**:

Confidentiality:

State cyber-threat groups are always on the prowl to conduct attacks on tv shows/movies before their release to avenge mockery of state officials (North Korea's ransomware attack resulting in the leak of movies produced by Sony Pictures thus resulting in financial loss is a good example). Thus, the occurrence level is high as there is a constant attempt to gain this treasure trove of data which is the oil for a media company like Paramount. Consequence level is high as well in this case due to piracy or state actors which result in a significant political/financial loss for companies like Paramount+.

Integrity:

A good example would be an attack on the media coverage of national importance to hamper say election results. Attacks in this case can be done using NAS storage vulnerabilities to disrupt the accuracy of information across regions.

A much scarier example would be manipulation to the existing video library database with a deep face attack wherein existing videos might be replaced with a misleading message. Occurrence level is moderate due to state actors constantly trying to manipulate the integrity of data of national importance. Consequence level high. Attackers might intend to target the integrity of the website shows/coverage but the given the security mechanism already in place it's not as valuable compared to say a DoS attack. However, the consequence level is high in this case as this major media company website streams election coverage at a national level which can be blocked to manipulate election results. At the same time live/regional games might be blocked to manipulate betting odds for financial fraud.

Availability:

The probability of disruption is high due to the fact that it is the core front facing product for the company – the primary source of revenue in terms of subscription fees and ads. Depiction of correct news and up-to-date portrayal of sporting events is the heart of a media company. A DDoS attack can take down the availability of live news coverage as well as live games thus garnering subscriber's ire. The availability might also be affected by a network outage or a power failure. The consequences of this happening are low as the consumers might get annoyed by the unavailability but are bound to forget about it after a while and care less as most likely there's no personal data/financial loss involved.

Theft/Fraud:

Ransomware is a primary threat to a video catalogue as the pirates can uphold the release of a movie/tv show with the possibility of releasing it for free on the dark web. Probability of threat occurrence is moderate due to security measures in place. Consequences of it happening are high as it involves significant financial loss.

c) License/Rights/Partnership:

1. Movie/TV Show/Sports/News/Regional Rights

Confidentiality:

Probability of threat occurrence is moderate here as a subscriber can use VPN to spoof the location. Movie/TV Show/Sports/News/Regional Rights are highly location dependent. Consequence of it happening are high as it can affect upcoming licensing/rights/partnership deals in a major way as those can be the foundation for the company's source of revenue for the upcoming years.

Integrity:

Licensing/Rights/Partnership integrity is critical as a conformance to the contract of the deal. Should conform to regional rights in real-time. Probability of threat occurrence is moderate here as a subscriber can use VPN to spoof the location. Consequence of it happening are high as a breach to the contract might threaten the deal itself or a portion of the revenue made from the deal.

Availability:

Availability of licensing/rights/partnership information in a timely manner so as to make the right content available to the viewer at the right time. Probability of threat occurrence is low here as a subscriber can use VPN to spoof the location. Consequence of it happening are high as a breach to the contract might threaten the trust in the deal itself or a portion of the revenue made from the deal.

Theft/Fraud:

Theft/fraud in the case of streaming services might be attributed to use of VPN to spoof the location thus consuming content meant for another region or level of subscriber. The Probability of threat occurrence is high as misuse of VPN is fairly common with freemium VPN providers abundant on the internet. Consequence of threat occurrence is high as well due breach of license.

d) Network:

1. Router

Confidentiality:

Attackers might snoop on the network data via router vulnerabilities. Although the routers in use at the company are fairly old there are adequate measures in place to make sure the security patches are applied promptly. Probability of threat occurrence is low. Consequence of threat occurrence is moderate as it will be tough to cause considerable damage to user PII data which is sent encrypted over the network.

Integrity:

With modifications in the configurations of the router it might be possible to disrupt traffic in different direction thus lowering the throughput of the service and causing an inconvenience to the viewers. Probability of threat occurrence is low as it not worth spending time and resources for the attacker to slow down a media company's streaming speed for fun. Consequence of threat occurrence is just annoyance and thus low.

Availability:

Sources of threat might disable a router for a vague purpose, but it shouldn't threaten availability as the packets can reach the destination via another route. At most this might cause a congestion of traffic to the inconvenience of viewers. Probability of happening is low. Consequence of threat occurrence is low.

Theft/Fraud:

Theft of a physical router is quite unlikely and invaluable given the time and resources for a threat source. Thus, Probability of threat occurrence is low. Consequence is low as well as there will be alternative routes for the packets to travel through.

2. Switch

Confidentiality:

Attackers might snoop on the network data via switch vulnerabilities. Unlike routers, switches simply forward packets received from other routers. Probability of threat occurrence is low. Consequence of threat occurrence is low as it will simply not forward the packet to the intended destination thus needing another attempt.

Integrity:
With modifications in the configurations of the switch it might be possible to disrupt traffic in different direction thus lowering the throughput of the service and causing an inconvenience to the viewers. Probability of threat occurrence is low as it not worth spending time and resources for the attacker to slow down a media company's streaming speed for fun. Consequence of threat occurrence is just annoyance and thus low.

Availability:
Sources of threat might disable a switch for a vague purpose, but it shouldn't threaten availability as the packets can reach the destination via another switch. At most this might cause a congestion of traffic to the inconvenience of viewers. Probability of happening is low. Consequence of threat occurrence is low.

Theft/Fraud:
Theft of a physical switch is quite unlikely and invaluable given the time and resources for a threat source. Thus, Probability of threat occurrence is low. Consequence is low as well as there will be alternative routes for the packets to travel through.

3. Firewall

Confidentiality:
Attackers might be able to compromise the firewall to gain access to confidential data. Probability of threat occurrence is moderate. Consequence of threat occurrence is high as critical data is at stake – possible unreleased episodes of tv shows or unreleased movies.

Integrity:
Attackers might be able to compromise the firewall to gain access to data. Attackers might disrupt the integrity of the content in a region or make it available in an unauthorized region. Probability of threat occurrence is moderate. Consequence of threat occurrence is high as critical data is at stake – possible unreleased episodes of tv shows or unreleased movies.

Availability:
Attackers might be able to compromise the firewall to gain access to confidential data. Attackers might disrupt the availability of the content in a region or make it available in an unauthorized region. Probability of threat occurrence is moderate. Consequence of threat occurrence is high as critical data is at stake – possible unreleased episodes of tv shows or unreleased movies.

Theft/Fraud:
Attackers might be able to compromise the firewall to gain access to confidential data. Theft of intellectual property is possible as was in the case of North Korea's cyber espionage on Sony Pictures Entertainment. Probability of threat occurrence is moderate. Consequence of threat occurrence is high as critical data is at stake – possible unreleased episodes of tv shows or unreleased movies.

e) Customer Support

1. Subscription + Account Information:

Confidentiality:
Confidentially of customer's personal identifiable information is critical part of the business which also ensures a trust in the brand the company represents. Attackers might access the customer subscription service to gain demographic information and also possibly credit card details to commit theft/fraud.

Although adequate measures have been put in place in terms of security. Probability of threat occurrence is moderate. Consequence of threat happening is devastating (thus high) as it will impact subscriber confidence in the brand for a long time and might also deal with monetary penalties.

Integrity:
Integrity of customer personal data is not much of a concern unless about location. A user might be able to spoof his/her location using VPN to access movie/tv show rights only available to certain viewers. However, probability of this occurring is very low. Consequence of this occurring will be moderate as it might result into breach of contract for certain partnership/deals.

Availability:
Availability of customer data is crucial to the correct functioning of the business as unavailability might result into denial of service for a user. This may cause inconvenience for a brief period of time and also possibly loss of revenue and brand trust. Probability of threat happening is low. Consequence of threat occurrence is low.

Theft/Fraud:
Although data behind the subscription service server might be safe, another possible way to crack this data source would be to mine user data through phishing or social engineering. Theft of consumer data can be devastating to the company's image. Social engineers are always on the go to try to deceive users to divulge details regarding their profiles, demographics, and credit card information. Probability of threat occurrence is high and consequence of threat happening is high as well.

f) **Employer**:

1. Employee Hardware:

Confidentiality:
Employee hardware is in encrypted format. Probability of threat occurrence is low here as all the employee communication occurs on encrypted devices. However, the Consequence of threat occurrence is moderate to high in case critical business or financials are leaked.

Integrity:
Employee hardware is in encrypted format. Integrity is critical to the operation of business. Probability of threat occurrence is low here as all the employee hardware are encrypted devices and have back up mechanisms. However, the Consequence of threat occurrence is moderate in case critical business or financials are modified.

Availability:
Employee hardware is in encrypted format. Probability of threat occurrence is low here as all the employee hardware are encrypted devices and have back up mechanisms. However, the Consequence of threat occurrence is high in case of unavailability of live coverage or live sporting events.

Theft/Fraud:
Employee hardware is in encrypted format. Probability of threat occurrence is low here as all the employee are trained regularly for security considerations. However, the Consequence of threat occurrence is moderate as confidential data is stored on encrypted devices and requires a certificate to view/edit data.

2. **Employee Software**:

Confidentiality:
Employee software is critical to the operation of business. Software is licensed and authorized to the company only. Data is accessible via authentication mechanisms hence unavailable outside of company owned hardware. Probability of threat occurrence is low here as all the employee communication occurs on encrypted devices along with an authentication mechanism. However, the consequence of threat occurrence is high in case critical business or financials are leaked.

Integrity:
Employee software is critical to the operation of business. Software is licensed and authorized to the company only. Data is accessible via authentication mechanisms hence unavailable outside of company owned hardware.

Availability:
Employee software is critical to the operation of business. Software is licensed and authorized to the company only. Data is accessible via authentication mechanisms hence unavailable outside of company owned hardware.

Theft/Fraud:
Employee software is critical to the operation of business. Software is licensed and authorized to the company only. Data is accessible via authentication mechanisms hence unavailable outside of company owned hardware.

3. **Employee Communication/LAN**:

Confidentiality:
Employee communication is highly confidential as it underlays the operational details of the backend and business data. Probability of threat occurrence is low here as all the employee communication occurs on encrypted devices. However, the Consequence of threat occurrence is moderate to high in case critical business or financials are leaked.

Integrity:
Employee communication is fairly flexible on integrity as it relies on the inputs from all the employees. Probability of threat occurrence is low here as all the employee communication occurs on encrypted devices. However, the Consequence of threat occurrence is moderate in case critical business or financials are modified.

Availability:
Employee communication must have high availability at least for live coverage events and sporting events. Probability of threat occurrence is low here as all the employee communication occurs on encrypted devices and fault tolerance mechanisms. However, the Consequence of threat occurrence is high in case of unavailability of live coverage or live sporting events.

Theft/Fraud:
Employee communication leakage might be a possible victim of social engineering or phishing attacks. Probability of threat occurrence is low here as all the employee are trained regularly for security considerations. However, the Consequence of threat occurrence is moderate as confidential data is stored on encrypted devices and requires a certificate to view/edit data.

4. **Business Support + Financials**:

Confidentiality:

Information critical to support the business and ensure it runs smoothly. High confidentiality is expected. Probability of threat occurrence of a breach is low - example in case of a insider breach. Consequence of threat occurrence is high as business impact on the confidentiality of critical business data or financials can alter the core operation of the streaming service.

Integrity:

Integrity of critical business data is crucial to ensure smooth functioning. High integrity is expected at all times. Probability of threat occurrence is limited to internal mistakes or mishaps, and thus low. Consequence of threat occurrence is high as impact on the integrity of critical business data or financials can alter the core operation of the streaming service.

Availability:

Availability of critical business data is crucial to ensure smooth functioning. High integrity is expected at all times. Probability of threat occurrence is limited to internal mistakes or mishaps, and thus low. Consequence of threat occurrence is high as impact on the availability of critical business data or financials can alter the core operation of the streaming service.

Theft/Fraud:

Theft or fraud is totally possible by an insider or by an outsider via social engineering or phishing attacks. Adequate training is provided to the employees hence the possibility of it happening is low. Consequence of threat occurrence is high as it impacts business operations and possible has a profound financial impact as well.