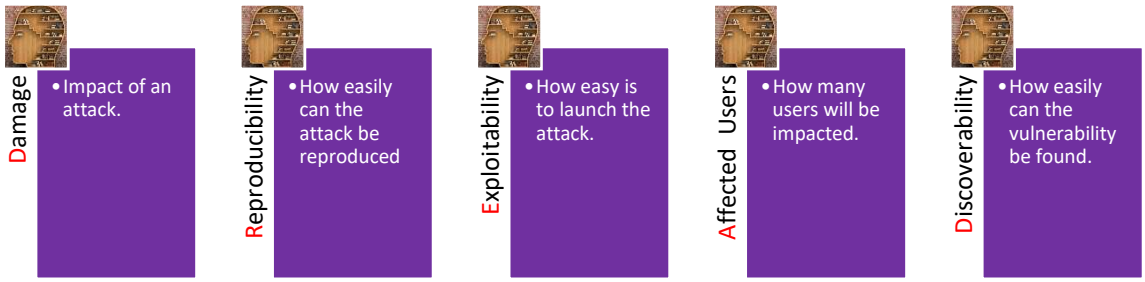
Unit 2: Real-World Issues and Implications of Information Security Threats and Vulnerabilities.

Unit two(2) focused on threat modelling frameworks and methodologies used to classify threats and risks. While several cyber threat modelling methodologies are used to approach cybersecurity and threat intelligence practices, the two that are of interest to me are STRIDE and DREAD. DREAD was a model that I can relate with since I was able to map it to the risk assessment tool on the change request form where I a currently employed. Figure 1 depicts one of the change requests I have submitted, and I was able to relate DREAD to the risk management portion of the form.

STRIDE Threat	STRIDE Threat	STRIDE Threat
Spoofing	A spoofing attack is when a malicious party impersonates a device or user on a network to gain the privileges of that user, pretend to be them to launch an attack, steal data, spread malware, or bypass access controls.	An email address is made known on the internet that shows an attacker how corporate email addresses are constructed. The attacker uses LinkedIn and other online tools to gather numerous names that identify themselves as working for the company. The attacker arranges these names in the same way as the email address found on the internet and crafts an email that compels the victims in the company to click on a link in the email and enter their work credentials. The attacker can gather numerous credentials for the company and can log into corporate sites by impersonating the victims.
Tampering	Data tampering is the malicious act of modifying data to make the data unusable, incorrect, or not trustworthy.	An employee or an attacker posing as an employee deletes all the information in a critical corporate database to hurt the business and make a recovery difficult. An employee could have received a poor review, found another job, and is angry at the company.
Repudiation	Repudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. A repudiation attack happens when an application or system does not adopt controls to track and log users' activities properly, thus permitting malicious manipulation.	When an attacker accesses an email server, finds inflammatory information that might embarrass the company, and forwards that information out to a news media outlet. This type of breach can be as simple as many email systems requiring authentication and not logging outbound emails. Once the news is made public, there is no ability to know who send the email out of the corporate network.
Information Disclosure	Information disclosure enables an attacker to gain valuable information about a system. Therefore, when configuring systems or applications, always consider what data could potentially be revealed and whether an attacker could use it.	Recent examples have included a corporate software developer using past customer data extracts in the testing environment to validate the functionality of new software features. Since the testing was in development only, the developer did not implement the same protections over the data, and as a result, the data was left on an open share in the cloud. Thousands of corporate customer records, including PII data such as names, addresses, and phone numbers, were made public.
Denial of Service	A denial of service attack is an interruption in an authorised user's access to a computer network or access to data, typically caused by malicious intent.	One example of a Denial-of-Service (DoS) attack is when a malicious actor uses multiple computers (sometimes thousands) to send network traffic to a web server on the internet. Since the traffic is more than the webserver is expecting, it overwhelms the server not to access their standard applications. Such an attack is often the result of multiple compromised systems, such as a botnet that floods an online retailer, preventing customers from purchasing anything for hours.
Elevation of Privilege	A privilege escalation is a type of network intrusion that takes advantage of programming errors, design flaws, or process gaps to grant the user elevated access to the network, such as administrator equivalent privileges.	In most privilege escalation cases, an attacker first uses a standard employee login. They then search for exploitable flaws in the system that can be used to elevate privileges. If the attacker successfully exploits such weaknesses, they can create new accounts for Spoofing, delete logs, access files, or seal or change sensitive data.

The DREAD methodology is used to assess, analyse, and find the probability of risk by rating the threats.



Risk Management

#	Description	Impact	Likelihood	Consequence	Weighted Score
1	The new copies of databases not synchronizing up to the state of being passive healthy.	0	1	0	1
2					
3					
4					
RISK COUNT			TOTAL SCORE		1

Perceived Risk Score (Mark applicable range)					
RISK	**Insignificant**	**Low**	**Moderate**	**High**	**Extreme**
RANGE	**=0 < 2**	**= 2 < 3**	**=3 < 4**	**= 4 < 5**	**>= 5**

Figure 1: NICD Change Request Form