Sri Lanka Institute of Information Technology

Information Assurance & Security (IT3070)

Risk Management Assignment

	Student Registration Number	Student Name
Student 1	IT20146238	Jayathunga T.M.
Student 2	IT20272654	Rajapaksha R.P.S.V

Table of Contents

Freelan Enterprises (Pvt) Ltd

We selected Freelan Enterprises Pvt Ltd, a leading Sri Lankan spice company for our Risk Management Assignment. Freelan Enterprises (Pvt) Ltd is a food and beverage service provider. It distributes their spices locally and abroad. Here is a web application for launching new products for sales and promotions by the technology department in their company for management purposes. They aim to strengthen the relationship between the customer and the company and further expand their presence in the global market. Therefore, we identify the critical assets and risk opportunities they may have here and create Allegro-Worksheet 10 for those scenarios.

1. DDoS Attacks Using Botnets

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET 1	
Information Asset Risk	Threat	Information Asset	Company Website
		Area of Concern	*DDoS Attack*
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	A distributed denial of service (DDoS) attack is a malicious attempt to affect the availability of a targeted system, such as a website or web application, to legitimate end users. In case of a Distributed Denial of Service (DDoS) attack, and the attacker uses multiple compromised or controlled sources to generate the attack. To succeed in this DDos attack, our servers, devices, services, network, applications, and even specific transactions infected with malware are allowed to be remotely controlled by an attacker. These individual devices are called bots and a group of bots together is called a botnet. These infected endpoints are usually computers and servers. But most are IoT devices. Here, attackers use malware to take control of vulnerable Io T devices to block legitimate users from accessing internet services by using DDoS attacks. it takes down websites offline by consuming more resources or occupying all available bandwidth.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	In a DDoS attack, it affected to the entire company system, therefore it is possible that the online platform is unreachable. Therefore, an unreachable online platform, loss of productivity, loss of confidential data, loss valuable customer data and turn over decline and reputation damage of the brand are the results can be occurred.

	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **(75%)**	❑ **Medium** **(50%)**	❑ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
This kind of impact (DDoS Attack) on the website causes the customer to lose the reliability of the website. If it happens the company should be responsible for loss of customer data. Such things add tarnish to the reputation of the company.	Reputation & Customer Confidence	8	6
	Financial	6	4.5
If customers are not able to connect to the system properly, the productivity of the company will go down. It may also cause the company to lose its reputation and change its name. As a result, daily sales opportunities may be missed, and losses incurred.	Productivity	8	6
	Safety & Health	0	0
Customers will take legal action against the company if the data of customers bound to the company is deleted, exposed to outsiders or data is damaged.	Fines & Legal Penalties	5	3.75
	User Defined Impact Area	0	0
		Relative Risk Score	**20.25**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Contact your internet service Provider (ISP)	If you find your company is under attack, you should notify your Internet Service Provider (ISP) as soon as possible to determine if your traffic can be rerouted. DDoS traffic among a network of servers. That can help render an attack ineffective.

Get help the recognizing attacks	Companies often use technology or anti-DDoS services to help defend themselves. These can help you recognize between legitimate spikes in network traffic and a DDoS attack.
Configure firewalls and routers	Firewalls and routers should be configured to reject bogus traffic. Remember to keep your routers and firewalls updated with the latest security patches.
Investigate black hole routing	Internet service providers can use “black hole routing.” It directs excessive traffic into a null route, sometimes referred to as a black hole. This can help prevent the targeted website or network from crashing. The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.
Consider frontend hardware	Application front-end hardware that’s integrated into the network before traffic reaches a server can help analyze and screen data packets. The hardware classifies the data as priority, regular, or dangerous as they enter a system. It can also help block threatening data.
Unnecessary software should be removed.	Remove all unnecessary software from your servers to reduce vulnerabilities. This means that you only need to install and maintain the software you need to run your server. Even if walking away is completely harmless, it's safer than regretting it.

Attribute	Value	Justification
Probability	75%	By attacking the website, the company and the users also must face various obstacles. This can be a huge blow to the company's reputation and hence the probability of this is high.
Reputation & Customer Confidence	8	Reputation and the trust of the company will be damaged due to this kind of attack. (8/10)
Financial	6	Due to reputation and trust issues, the customer has stopped communicating with the company, and the company is still responsible for the financial loss and must repay the customer, which has a major impact on the company. (6/10)
Productivity	8	Due to slow internet access, the company cannot continue to work as before, which directly affects the productivity of the company. (8/10)
Safety & Health	0	No serious impact for the safety and healthy, so no value is given. (0/10)
Fines & Legal Penalties	5	Company must fine be due to the legal penalties. It's given low value. (5/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

2. Recipe Information Database

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET 2			
Information Asset Risk	Threat	Information Asset	Recipe Information Database		
		Area of Concern	*Disclosure of recipe information by the database for a personal gain.*		
		(1) Actor *Who would exploit the area of concern or threat?*	Internal Staff Member (Inside Attacker)		
		(2) Means *How would the actor do it? What would they do?*	The staff member who has access to spice mix information database steal the information. The staff member can physically access by removing device and copy all the recipe information from the database. If not, staff member can install malware and take the information. It is a network access to the database. If not, the staff member can give money for the authorized person or the operator to get access for the database. The objective of this is to transfer spice mix information to 3rd parties.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the authorized person can view the data and information of the recipes. People who have access to the recipe information database are not allowed to transfer recipe information to 3rd parties.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **(75%)**	❑ **Medium** **(50%)**	✓ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Same products can be come out with other competitive manufacturing Company. Then its uniqueness of the company	Reputation & Customer Confidence	8	2

	will reduce. So, the reputation will go down. If customers decrease, the financial impact can be happened to the company.	Financial	8	2
	The internal person can ask for money from the Freelan Company and if they not pay, he will hand over the information to 3rd parties. So, financial impact is there.	Productivity	8	2
		Safety & Health	0	0
	The Freelan Company must take legal action against its internal employees and bear financial costs. Productivity goes down because the same product comes with some improvements with their knowledge.	Fines & Legal Penalties	6	1.5
		User Defined Impact Area	0	0
			Relative Risk Score	**7.5**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Give access to a loyal person that has been with the company for a long period	A person who initiates the establishment of the company should be given its administrative privileges. They are loyal people and can believe them. The recipe of the restaurant is the most important to produce unique products.
Divide the spice mix recipe information to parts and one person cannot access all information without others participating.	By sharing the secrets of the recipe of the ingredients used in the production of a certain spice, it is avoided that those recipes are improperly transferred from one person to other companies.
Maintaining a high standard of spice mix	Search about new spice mix item recipes and upload all the information and maintain a standard in the system. If someone leak the information that spice mix recipe, it's easy to access and check who did it.
Divide manufacturing process to parts so a one person does not know about the production.	Two-way authentication can be used to access the company's valuable information. Then it is impossible for a single person to access the data without the participation of all the people.

Attribute	Value	Justification
Probability	25%	It's unlikely because many users don't have access to recipe information. The accessible persons are mostly loyal to the company.
Reputation & Customer Confidence	8	The reputation of the company depends on the quality of the product. Therefore, if another company sells products using the same recipe, it will reduce the trust of the customers in the company. (8/10)
Financial	8	Due to other reasons, the company suffers economic loss Competitors may enter the market with the same products, demand for those products increases, and customers may purchase them. Therefore, it is assigned a high value. (8/10)
Productivity	8	When demand for your products dwindles and you no longer have a customer base, you can't continue your business processes. Employees leave the company and productivity declines. Therefore, it is assigned a high value. (8/10)
Safety & Health	0	There are no safety & health Impact Areas. Therefore, no value is given. (0/10)
Fines & Legal Penalties	6	Since this is an internal attack, the potential for fines is high. If an internal employee discloses this information to a third party, the company may take legal action. The Company may have to pay its customers legal costs, fines, and penalties. Therefore, it is given a medium value. (6/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given. (0/10)

3. POS Application & POS Device

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET 3			
Information Asset Risk	Threat	Information Asset	POS Application & POS Device		
		Area of Concern	*POS Application got hacked using malware to change the information about the company secret spice recipes.*		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder (Outside Attacker)		
		(2) Means *How would the actor do it? What would they do?*	Intruders can steal your company's POS devices and access your data via Bluetooth. Intruders can easily remove and return the device before business reopens the next day, as the POS hacking process takes only about an hour. Malware can be installed during what appears to be a normal consumer transaction. All an intruder has to do is find an unprotected IP address or hack into your Wi-Fi connection. You can then change the discount details for the item by subtracting the price of each unit.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Data in the POS system can only be viewed and modified by authorized personnel or cashiers who are aware of risks and unit costs. The company should use a highly rated antivirus guard in its system to protect her POS devices in the company from all kinds of viruses and threats.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **(75%)**	✓ **Medium** **(50%)**	❑ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
The output of the customers' bill has many changes comparing to the original bill because of the virus changed the unit prices	Reputation & Customer Confidence	8	4

	of all the units. This reduces the customer's reputation and trust within the company. So, if the number of customers is small, the company will receive a lowest financial.	Financial	8	4
	It takes time to analyze evidence of virus processes and identify system vulnerabilities that can help viruses infect your system. Therefore, the POS system becomes less productive.	Productivity	6	3
		Safety & Health	0	0
	If a customer takes legal action against the company for invalid billing content, the company does not take full responsibility for the POS attack directly and does not promptly support paying the full number of deductions to the customer. may require more resources for justification and legal services.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	0	0
			Relative Risk Score	**13.5**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Check the Hardware and Software Components	Check all hardware and software components in your POS system network. Next, install the virus protection device associated with your POS system and update all software components of your POS system appropriately. Update hardware components that are not working properly.
Maintain and follow standards	Search about new inventions of the POS systems and update the systems with the latest modern technologies. Hire a qualified IT person or company to help you keep your POS system up to standard.
Implement a password policy	Make sure all Wi-Fi connections on your network are secure and always change the default password on your device. Follow best practices for creating secure passwords. Password should be strong with more than 8 characters.
Conduct workshop and Conferences	The company system admin should be given a proper induction on data security and its risks. Even after the initial training sessions it is important to keep them updated about the possible attacks and new risks.

Attribute	Value	Justification
Probability	50%	Chances are moderate as most POS systems support antivirus and anti-scanning tools. Only the administrator uses their POS system to log into the system and update financial details and product information.
Reputation & Customer Confidence	8	An attack on your POS system puts your company's reputation at risk. Customers will lose their trustworthiness and confidence about company. Due to the high cost of living and the carelessness of the company's employees, you end up moving to another company. It's unfair for customers to pay more for cheap products. Therefore, it is given high priority. (8/10)
Financial	8	Incorrect billing information from the POS system causes financial loss for both the company and the customer. So, company must spend money to investigate and pay to better virus guards. Therefore, it is given high priority. (8/10)
Productivity	6	Productivity of the POS system goes down because of the attack. This leads to a reduction in the company's total annual revenue. Therefore, the productivity impact is given as a moderate value. (6/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given. (0/10)
Fines & Legal Penalties	5	Attacks are external attacks and are more likely to be fined. The company might have to pay lawyer fees, law court fines and penalties for the customer. Therefore, a medium value is given. (5/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given. (0/10)

4. Server Down

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET 4			
Information Asset Risk	Threat	Information Asset	Servers of the Freeland Enterprises		
		Area of Concern	*Fire Originated inside the server room cause damage to the servers.*		
		(1) Actor *Who would exploit the area of concern or threat?*	Natural		
		(2) Means *How would the actor do it? What would they do?*	Server rooms are at a heightened risk for fire without proper temperature and humidity level regulation and fire suppression measures, the server room is more prone to sudden fires. Electrical failure of its equipment, Issues with subfloor wiring, Overheated electronics and Unrelated fires can be mentioned as the main factors that cause fire in the server room. In addition to the servers in the server room, other physical devices were also damaged in case of a natural fire in the server room. can.		
		(3) Motive *What is the actor's reason for doing it?*	Accidental		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	✓ **Destruction**	
			❑ **Modification**	❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Fire warning measures should be installed to prevent fires. That way, fire detectors and carbon monoxide detectors can help alert you to the issue before it has a chance to spread and get out of hand. Apart from that, the server room should always be kept clean, and the cooling system should be installed.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **(75%)**	✓ **Medium** **(50%)**	❑ **Low** **(25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
When a server failure occurs, the company reputation is at risk if there are urgent client projects that need to be given on time. In	Reputation & Customer Confidence	7	3.5

	order to install a new server system, a high cost should be spent. Therefore, the financial expenses will be high as well.	Financial	6	3
	If services are not available for approximately three hours, employees will not be able to complete their assigned tasks each day, delaying ongoing projects and can have a significant impact on productivity. Employee safety is also at risk if a fire from a server room spreads to other company premises.	Productivity	5	2.5
		Safety & Health	4	2
		Fines & Legal Penalties	0	0
		User Defined Impact Area	0	0
			Relative Risk Score	**11**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Use the backup servers	Backup servers can be implemented to provide the service continuously if the main server gets damaged or in a condition of improper functioning.
Cool the Server Room according to the system required	It's important to keep your server room cool to prevent devices from getting overheat and pose a fire hazard. check cooling the system is operating normally and we are closely monitoring the alarms system is required.
Give hands-on training for the IT area personnel	Train employees in the use of portable or installed fire extinguishers Suppression system in case of emergency. Even if the fire doesn't go out If it originates from a server room, it can spread rapidly there. reach out Enabling firefighting training and rapid action for employee's fire face.
Keep server rooms cleaned and well maintained.	Keeping client rooms clean is essential to prevent fires. Make it easy for dirt and dust to accumulate Equipment contributes only combustibles and increases the heat load. When sparks, dust and debris from fire are ignited and stored A clean server room environment is a must.

Regular inspections both internally and externally.	Regular checks to ensure that the installed fire protection devices are in place Well tested and maintained. Inspection to make sure the space is safe Compliant.
Professional fire risk assessment	Conducting a complete fire risk assessment by a fire protection expert as a first step into the server room. It will minimize the damage that can happen from the fire.

Attribute	Value	Justification
Probability	50%	The probability is moderate as the risk affects many areas of the company, impacts the daily work of employees, and delays ongoing projects and deadlines. Therefore, the probability of this scenario is moderate.
Reputation & Customer Confidence	7	The company's reputation is high risk even though many controls are in the employees' hands. Client satisfaction will be lost when the employees will have to delay their daily work due to the issue. Therefore, a high value is given. (7/10)
Financial	6	This problem results in economic losses and additional costs for implementing new cooling systems. Therefore, it is assigned a high value. (6/10)
Productivity	5	Employees are unable to concentrate on their daily tasks for a period and become less productive. However, it will be restored when the server comes back up. Therefore, an average value is given. (5/10)
Safety & Health	4	Employee may be injured fire. However, with the Quickfire prevention system, this is unlikely. Therefore, it is given a low value. (4/10)
Fines & Legal Penalties	0	There is no impact on Fines & Legal Penalties. Therefore, no value is given. (0/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given. (0/10)

5. Alarm System & CCTV Network

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET 5			
Information Asset Risk	Information Asset	Alarm system and CCTV network		
	Area of Concern	*Denial of Service (DoS) attack against CCTV & Alarm network system of the Company.*		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Intruder (Outside Attacker)		
	(2) Means *How would the actor do it? What would they do?*	Intruders use Denial-of-service (DoS) as an attack to deny legitimate users access to resources. Accessing or extremely slowing down the cloud server network. So, the security system automatically slows down. Attacks are typically implemented by attacking a target resource (cloud server) is making too many requests at the same time. This causes the server to stop responding to all requests. After the attack, the intruder has no security and can carry out another physical attack. This allows intruders to attack over the network. This can cause large amounts of data loss on the network.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	✓ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only CCTV operators or individuals authorized person can view this information asset. This person is responsible for maintaining the system and checking for attacks affecting the system. A firewall can stop simple denial of service (DoS) attacks by identifying IP addresses and blocking all traffic from attackers.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **(75%)**	✓ **Medium** **(50%)**	❑ **Low** **(25%)**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**

	If the customer's or something lost at the security counter or inside at the company, the CCTV system is responsible for the security of the customer's things at the company. This can result in financial loss if a customer withdraws due to reduced security. it will affect to the company overall system and company brand name.	Reputation & Customer Confidence	6	3
		Financial	8	4
	Investigate about this problem and take some effort to keep more backups about CCTV records in the paid or non-paid secured cloud stores and analyze the backups for better security.	Productivity	3	1.5
		Safety & Health	7	3.5
	Although the company is not directly responsible for the losses of customers, legal services may cost resources if customers take legal action against the company.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	0	0
			Relative Risk Score	**14.5**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Use a backup System	Simply add a backup run and keep second copy of the backup footages stored on CCTV system.
Install Firewalls	Find a new service provider who has more robust connectivity. it will help to more supportive in preventing DoS attacks. Work with insurance companies to develop alternative delivery methods such as a direct connection.
Share Experience	Sharing risk experiences, it will help to improve company future security. It should be properly documented for future work.

Observation	Train a good person to check your CCTV camera system constantly. Purchase a top-rated superior server to store your CCTV video backups and maintain them with proper security by qualified personnel.

Attribute	Value	Justification
Probability	50%	Most CCTV systems come with huge backup plans. Always hire a qualified person to properly maintain your server and keep your CCTV system up and running without data loss as seen in many shops and businesses. Therefore, there is a medium probability risk.
Reputation & Customer Confidence	6	The company's reputation is at moderate risk and customer trust is lost. Because the company has a great responsibility to protect his CCTV data and build customer trust to preserve the company's name. Therefore, it is given a moderate value. (6/10)
Financial	8	Financial loses will occur to the company. If the customer loses the goods from the company and the customer files a lawsuit against the company, the company must pay the value of the lost goods. Therefore, it is given high priority. (8/10)
Productivity	3	Productivity of the company goes down with the data loss. Less security cannot find the correct information about in and out details properly. However, the impact on productivity is for a short time. That is why the value is low. (3/10)
Safety & Health	7	Losing data on CCTV servers is a huge security risk. This affects the security of your entire business process. Therefore, the safety value is high. (7/10)
Fines & Legal Penalties	5	Since the attack is an external attack the chances of getting fines are high. There is a possibility for loss any item of a customer during this period. The company might have to pay lawyer fees, law court fines and penalties for the customer. Therefore, a moderate value is given. (5/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given. (0/10)

References

https://aws.amazon.com/shield/ddos-attack-protection/

https://coolingpowercorp.com/news/common-causes-server-room-fires-might-surprise/

https://cloudsecurityalliance.org/

https://www.esecurityplanet.com/

https://www.scribd.com/document/344795891/OCTAVE-Allegro-Method-v1-0-doc

https://sunlightmedia.org/business-data-threats/

https://www.cloudflare.com/

https://blog.icorps.com/bid/137975/new-trend-the-point-of-sale-system-hack

https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/

https://solutionsreview.com/identity-management/the-top-7-password-attack-methods-and-how-to-prevent-them/