Assignment 2

Part a

Attack scenario 1

Attack name	*DOS Attack*
Threat / Threat Agents	*An attacker / many clients ordering at the same time causing a traffic*
Vulnerabilities	*flooding the URL with unlimited requests / Cheap Hosting/Lack of Preparation/Insecure or Out of Date Code*
Indicators of attack	• *A typically slow network performance such as long load times for files or websites* • *The inability to load a particular website such as your web property* • *A sudden loss of connectivity across devices on the same network*
Damage or loss to information assets likely from this attack	*Clients can't proceed with payment service and some orders maybe confirmed without payment being confirmed*
Immediate actions taken when this attack is underway	• *Recognize that there is a problem* • *Inform stakeholders* • *Inform the Mitigation Service Providers (MSP)* • *Trying to fix the source problem* • *Changing the organization's filtering strategy* • *Eliminating or relocating the target system* • *may have to go through a trial-and-error process until we find a solution that eliminates the issues associated with the attack without disrupting normal operations*
Follow-up actions	• *Identify which resources have been affected and forecast which resources will be affected* • *Estimate the current and potential technical effect of the incident* • *Report the incident to the appropriate internal personnel and external organizations.*

	• *Create a follow-up report.* • *Hold a "lessons learned" meeting.*

Attack scenario 2

Attack name	*Unauthorized Access*
Threat / Threat Agents	*Attackers (Hackers)*
Vulnerabilities	• *Network vulnerabilities are weaknesses within an organization's hardware or software infrastructure that allow cyberattacks to gain access and cause harm. These areas of exposure can range from poorly-protected wireless access all the way to misconfigured firewalls that don't guard the network at large.* • *Operating system (OS) vulnerabilities are exposures within an OS that allow cyberattacks to cause damage on any device where the OS is installed. An example of an attack that takes advantage of OS vulnerabilities is a Denial of Service (DoS) attack, where repeated fake requests clog a system so it becomes overloaded. Unpatched and outdated software also creates OS vulnerabilities, because the system running the application is exposed, sometimes endangering the entire network* • *Process vulnerabilities are created when procedures that are supposed to act as security measures are insufficient. One of the most common process vulnerabilities is an authentication weakness, where users, and even IT administrators, use weak passwords* • *Human vulnerabilities are created by user errors that can expose networks, hardware, and sensitive data to malicious actors. They arguably pose the most significant threat, particularly because of the increase in remote and mobile workers. Examples of human vulnerability in security are opening an email attachment infected with malware, or not installing software updates on mobile devics*

Indicators of attack	*Alerts from network intrusion detection software and network behavior analysis software* *• Unusual traffic to and from the host* *• New process/software installed and running on a host* *• New files or directories with unusual or nonstandard names*
Damage or loss to information assets likely from this attack	• *Client’s data could be leaked or stolen*
Immediate actions taken when this attack is underway	○ *Isolate* ○ *Disable network port* ○ *Block* ○ *Disable user account* ○ *Lock down*
Follow-up actions	● *After the UA has been contained, the task of identifying the avenue of attack and closing any still-open repeat mechanisms begins.* ● *At the same time, we must identify the extent of the damage done by the UA and look for any residual effects, such as rootkits or back doors.* ● *all accounts reset of all passwords, including those for administrator accounts*

Part b

Stakeholder	Reason of choice	Vision
InfoSec management	• *In case of DOS Attack/UA he/she will have enough experience to react and respond* ● *Also, will always be available to secure our system as it’s their job*	*Enough experience to defend against any attack*

PR Department	• *Will always need them in case an attack occurred to keep business reputations*	*Keeps good business reputation*
legal department	• *Always need them for legal actions*	*They will use all legal laws to help company and also to help us from breaking the law without being aware*
General management	• *To report which services were affected and inform employees how to react* ● *Also, to motivate employees*	*They will have more time to spend with employees so they know how they feel what they need to do to motivate them*

Part c

a) Team Model Structure

Centralized as we are still a small organization

b) Staff Model

Partially outsource to gather as many experiences as we can from a well experienced company,
Disadvantage that our data can be exposed to an external company but it can be controlled with the contract made with them regarding their limit of interference

c) CSIRT Services

Pro-active to try to prevent the attack before it even happens.