Business Continuity & Risk Management

Assignment 2

Incident Response Planning

Name: John Ehab

ID: 100-2096

Part a

Attack scenario 1

Attack name	Ransomware
Threat / Threat Agents	• Theft • Experienced hacker
Vulnerabilities	• Weakness in filtering the incoming files • Weakness in the antivirus systems running on our database
Indicators of attack	High rate of files modifications
Damage or loss to information assets likely from this attack	All the valuable information that is saved on our servers
Immediate actions taken when this attack is underway	• Take the devices offline, disconnect from any network • Stop any malicious encryption software that may still be running • Isolate critical systems to prevent further spread of the malware • Collect and retain logs
Follow-up actions	• Determining the state of storage systems and status of online and offline backups • Prioritizing applications and info for recovery • Creating an inventory of sensitive or high-risk data that could have been stolen

Attack scenario 2

Attack name	**DOS**
Threat / Threat Agents	• Script kiddies • Business competitors
Vulnerabilities	Weakness in filtering the incoming packets or our firewalls
Indicators of attack	Unusual consumption of the servers' resources
Damage or loss to information assets likely from this attack	Denial of service for some clients
Immediate actions taken when this attack is underway	Overprovision the server's bandwidth Alert key stakeholders Call any other 3rd parties that may be responsible for service delivery
Follow-up actions	• Check all critical systems and databases • Modify your security systems and IDPSs • Add a part as a proof of work (e.g captcha) on your website to prevent bots from flooding my server with illegitimate packets

Part b

Stakeholder	Reason of choice	Vision
General management	Gives the upper management support for the team and providing the needed materials and budget.	Ensures that the IR team is achieving the overall business mission, vison, and policy.
IT management	The technical team that has the knowledge and expertise across the company's different systems and online services.	Gives the needed information about how our systems work and the probable vulnerabilities that may be exploited.
InfoSec management	The core of the IRPT, include security analysts and engineers who keep our systems secure and have the experience of different cyber attacks and how to defend against them and how to respond to any cyber attack.	How to increase the security quality of our business by applying the defensive countermeasures, and also how to be able to differentiate what a real incident is and what is not.
Legal department	They give information about the legalities and law enforcement rules that should take place if any cyber crime happened.	Ensures that the incident response activities taken line up with laws and regulations to protect the organization.

Part c

a) Team Model Structure

Central team. First, because my business is relatively small, so I won't have a lot of staff to work in multiple teams. Second, to keep all the plans and experts in one area for better communication and managing the whole process in case a big incident happens, and they can train employees in every department to let them know if an incident is undergoing and they can take the control to handle it.

b) Staff Model

Partially outsourced. The business has its own team of incident handling, but may need help from more professional 3rd parties in some cases of attacks that could cause severe damages or that cannot be handled by our team or by our resources.

c) CSIRT Services

It should provide the 3 kinds of services (reactive, proactive and security quality management services). It should detect the incidents and handle them. And should manage the IDSs and the configurations of the systems, and do the assessment activities preparing for any incident that may happen. And it also should ensure the good security quality of the business's systems and tools, analyze risks, and provide the education and training for the employees.