**CASE STUDY**

You have been appointed as the Information Security Officer for XY Limited, a telecommunications company with operations in the European Union and Africa.

Your immediate manager is the Chief Information Officer (CIO). The CIO is part of the company’s executive management team that includes the Chief Executive Officer, Chief Financial Officer, Chief Sales & Marketing Officer, Chief Technical Officer and Chief Human Resources Officer.

In your second week on the job, you get a call at midday from the IT Operations Manager reporting that suspicious activities have been observed on several XY Limited IT systems.

Preliminary investigations indicate the following:

1. Attackers have uploaded a web shell, giving them greater access on one of the web sites. The attackers extracted the contents of the database and uploaded tools including password extraction tools and privilege escalation tools to the web server from which to attack the internal network. Additionally, the attackers have gained access to a number of credit card details, as well as sensitive details of 80% of XY Limited’s clients.
2. A copy of password stealing malware had been found on three of XY Limited’s domain controllers. A regular user had opened a phishing email that contained a link to a malicious site. Examination of the payload found that it hosted an exploit for what was, at the time, a novel remote code execution vulnerability (0-day) in Adobe Flash. The payload dropped by the exploit had gained high privileges on the regular user’s machine and disabled antivirus.

The administrator had then logged into the regular user’s machine to understand why the antivirus was not functioning whereby their domain credentials were stolen.

The attacker had then attacked the internal network, including the domain controllers using the stolen credentials. As part of their attacks they had installed credential stealing malware on the domain controllers and gained large numbers of plaintext credentials.

Note that XY limited has no incident response team or processes.

**You have been allocated 45 minutes to present at the Exco meeting in the next one hour 30 minutes. For the scenario above and additional questions below, prepare a presentation for XY Limited’s executive management team addressing the following points and questions:**

* What steps would you take to contain and address this cybersecurity incident?
* Identify the specific vulnerabilities or failures that possibly led to the attacks in [1] and [2] above?
* What controls would you recommend to address each of the specific vulnerabilities or failures identified?
* Explain the following concepts or terms to the executive management team. Give examples as well.
* Threat
* Vulnerability
* Zero-day vulnerability
* Risk
* Control
* Provide a high-level summary of the Equifax data breach and lessons learned for improving cybersecurity.

Explain the following concepts to XY Limited’s executive management team. Remember to give examples and indicate how you would embed these concepts within an environment.

* Security by design
* Privacy by design
* Defense in depth – what are the typical layers? In your opinion, which layer is the most critical and why?

What are the key benefits of implementing of an information security management system (ISMS)?

What elements or sections would you include in a business case for implementing an information security management system (ISMS)? Indicate what each element or section covers