Incident report analysis

Instructions

Summary	XYZ Financial Services, experienced a data breach attack. This breach comprised confedential information such as , client names, client addresses, client social security numbers, and financial transaction details. There was a vulnerability in the system allowing attackers to to bypass the web application firewall an dgian access to an internal database server.
Identify	This incident is a result of a data breach. A breach resulting in unauthorized subjects gaining access to confidential information. This confidential information contained highly personal information regarding the institution's clients.
Protect	Main course of action will be to patch zero day vulnerability in the web application framework.0 day patch will be deployed. Once a risk/vulnerability is disclosed , a patch is released, and the vulnerability is very small.
Detect	Other ways to monitor network traffic for security breaches continuously will be keeping the zero day patch updates as well as regularly monitoring.
Respond	Response team will be assigned and activated. All security vulnerabilities will be contained. Law enforcement will be contacted to investigate the findings legally.
Recover	Normal operation will continue as before. Restoring the operation will be conducted to allow business functions to resume. Improvements and

	continuing operation will be done as additional security measures are implemented. All lost data will be restored.

Reflections/Notes:

XYZ Financial Services experienced a data breach, exposing client names, addresses, social security numbers, and financial details due to a vulnerability in the web application framework. The primary response involves promptly patching the zero-day vulnerability, deploying continuous network monitoring, and activating an incident response team. Law enforcement will be engaged for legal investigation. Normal operations will resume swiftly, and ongoing improvements in security measures will be implemented. Lost data will be restored, and communication strategies will address affected parties, emphasizing legal and regulatory compliance. The incident underscores the need for proactive security measures to protect sensitive client information.