MGS 650 - Information Assurance - Guest Lecture
Akhilesh Anand Undralla
11/17/2021

Breaches:

Breaches are a type of security incident that involves the release of personally identifiable information. Security incidents/events are events such as impersonation, denial of service and website defacement that don't involve the theft of personal information. Breach is a triggering event that involves unauthorized access to or acquire of PII, compromising security, confidentiality and integrity of PII. PII constitutes information that involves first name and last name in combination with SSN, State ID, Drivers ID, Medical information, financial information, biometrics. Username or email address is considered PII with a combination of a password or security question and answer. Organizations are not required to report many security incidents/events but required by law to issue 'breach' notification to impacted individuals within stipulated time period and follow documented procedures in the case of breaches. All the states within the USA maintain various rules that adhere to breach notification statuses. After the event of breach, evaluate whether breached data is legally PII or not by investigating the breach. It is determined whether the PII breach is not a legal issue if data is not used for business purposes, when the data is encrypted and when the investigation team marks the breach as low risk or zero likelihood of harm due to the breach.

Security Incident Lifecycle:

A security incident lifecycle starts with 'Initial Response' (72 hours) stage, Insurer is brought in and all the engagements during investigation are informed concurrently. A brief (usually ambiguous) notice must be sent to customers and partners to maintain company reputation. If an outside counsel is involved, vendor bias is verified. The Forensics department begins investigation by collecting evidence and IT contains the risk by corrective measures. This can also involve a 'breach coach' who works to isolate the data, notify customers/partners, retain required forensics professionals and manage risk crisis communications. During the next stage, "Investigation and Remediation" (1-2 months) organization investigates the data breach and determines the extent of the breach. Remediation actions involve securing network perimeter, securing tamper-proof evidence and restoration paths/methods. 'Wrap up and Recovery' (2-3 months) involves outside counsel reviews and submission of an approved and confidential forensic report to the management. Wrap up report can be considered as a 'post-mortem' report. At this stage, all the restoration plans are set up and a long term remediation plan (a contingency plan) is put in place. Next stage i.e., Breach notification stage (4-6 months) involves teams of security, IT, legal working together to reduce the company's risk as low as possible by working with consultants and finalizing breach notification requirements. After impacted servers are analyzed for breach data, a data mining report is generated by the vendor. An outside counsel determines applicable laws to send out notifications to individuals under legal terms. State attorneys must be notified if a threshold of a breach meets a certain risk criteria. A substitute notice is open notice to the public to announce breach news and their

response efforts. A notification vendor utilizes data mining report to a reduced version of spreadsheets and produces a mailing list. During the 'Fallout' stage (1-3 years) aspects such as legal liabilities, cost to business, scale of penalties, customer/business litigation proposals are finalized.

Legal Risks:

Legal risks surrounding breach notification statuses involve scrutiny into aspects like right of action for breach, security incident penalties, delaying notifications approved by attorney general, injunctions. Legal risk surrounding litigation involves settlements, lawyers suing other lawyers for living which can turn out to be time consuming and expensive. In conclusion, Legal, business and security/IT teams must work together to mitigate risks wherein legal teams should work with security/IT to conduct table top exercises, in-house training and work audit team to improve security posture and formulate change management policies. Cybersecurity lawyer, part of the legal team in an organization enforces policies related to breach notification statuses, security incident lifecycle and legal risks. In the perspective of the law and regulatory compliance, a breach and a security incident/event are not the same.