International Cybersecurity and Digital Forensics Academy

Course: GRC104 - Compliance Frameworks and Legal Requirements
Assignment title: Comparative Incident & Security Breach Analysis
Due date: [08/11/2025]
Format: PDF (report) + optional slide deck (10 slides)

Assignment brief

Select two (2) recent security incidents or breaches (within the last 3 years). For each incident, prepare a comparative report that examines:

- The affected organization (industry, size, and geographic location)
- The type of incident (data breach, ransomware, insider misuse, supply-chain compromise, etc.)
- The security requirements and regulations relevant to that organization (examples: GDPR, HIPAA, PCI-DSS, SOX, local financial regulations, data localization laws)
- The root causes and control failures that enabled the incident (technical, process, and human factors)
- The detection and disclosure timeline (who discovered the incident and how; self-reported vs discovered by regulator/third-party)
- The organizational and regulatory response (notifications, remediation, fines, litigation, executive consequences)
- Impact assessment (data exposure, financial, reputational, operational, customer trust)
- Lessons learned & prioritized remediation roadmap (short, medium, long-term controls; policy and governance changes)
- Individual accountability and criminal exposure considerations, including the role of whistleblowers and protections where relevant

Deliverables

Incident Analysis Report (PDF)

- Title page (student name, student ID, course, instructor, date)
- Executive summary
- Detailed analysis for Incident A (structured subsections)
- Detailed analysis for Incident B (structured subsections)
- Comparative analysis
- Recommendations & prioritized remediation roadmap (with owners & timelines)
- References & appendices (timelines, supporting documents, source links)