

Instructional Scenario

Data Breach Crisis: Protecting Customer Information



Course/Duty Area: Cybersecurity Fundamentals/Exploring Cybersecurity Fundamentals

Estimated Time Required: 5–7 hours

Scenario:

TechStart Solutions, a local e-commerce company, has just experienced a significant data breach affecting 50,000 customer accounts. Your first week as a cybersecurity intern, you arrive Monday morning to find the IT department in crisis mode. The breach occurred over the weekend when an employee clicked on a phishing email that appeared to be from the company's shipping partner. Hackers gained access to customer names, addresses, email addresses, and encrypted payment information. The company's reputation is at stake, customers are angry, and local media is requesting interviews.

Your supervisor tasks you with joining the incident response team. The CEO wants to understand exactly what happened, how it could have been prevented, and what steps need to be taken immediately. The legal team needs documentation for potential regulatory compliance issues. The marketing department needs to draft customer communications. Meanwhile, IT must secure the network, investigate the extent of the breach, and implement safeguards to prevent future incidents.

You must work with cross-functional teams to analyze the breach using cybersecurity fundamentals including the CIA Triad (Confidentiality, Integrity, Availability), defense-in-depth strategies, and incident response protocols. Your recommendations will directly impact the company's recovery efforts and future security posture. Time is critical and every hour of delay increases customer risk and potential legal liability.

Big Question:

How can organizations implement comprehensive cybersecurity measures to prevent data breaches while maintaining effective incident response capabilities when breaches occur?

Focused Questions:

- What cybersecurity fundamentals (CIA Triad principles) were violated in this breach, and how?
- What technical controls (firewalls, encryption, access controls) might have prevented or limited this attack?
- How should the incident response team prioritize their actions in the first 24 hours, first week, and first month?
- What role does security awareness training play in preventing social engineering attacks like phishing?
- How do legal requirements (such as breach notification laws) impact the company's response timeline and actions?
- What security policies and procedures should TechStart implement to prevent similar incidents?
- How can the organization balance security measures with business operations and user experience?

Student Project or Outcome:

Students will develop a comprehensive Incident Response and Prevention Plan that includes

- a timeline of the breach with technical analysis of vulnerabilities exploited
- immediate response actions with prioritization and rationale
- communication templates for customers, employees, and media
- recommended technical security controls with cost-benefit analysis
- an employee security awareness training program outline
- updated security policies and procedures
- a long-term security improvement roadmap.

Project-Based Assessment:

Students will present their Incident Response and Prevention Plan to a panel (teacher and potentially industry professionals) acting as TechStart's executive team. Presentations should include:

- Executive summary with key findings and recommendations
- Technical analysis demonstrating understanding of cybersecurity fundamentals
- Implementation timeline with resource requirements
- Risk assessment matrix
- Professional slide deck or digital presentation
- Written report (5–7 pages)

Evaluation will use a rubric assessing technical accuracy, practical feasibility, communication clarity, critical thinking, and professionalism. Students will be evaluated on both their presentation skills and depth of cybersecurity knowledge applied to a realistic workplace scenario.

Teacher Resources:

- [NIST Cybersecurity Framework](#)
- [CISA Stop Ransomware Guide](#)
- [SANS Incident Handler's Handbook](#)
- [SANS Incident Response Forms](#)
- Sample data breach case studies (e.g., Target, 2013; Equifax, 2017; Capital One, 2019)
- Phishing email examples and identification training materials
- CIA Triad and Defense-in-Depth instructional materials
- Guest speaker opportunity: Local cybersecurity professional or incident response team member
- State data breach notification law resources
- Rubric for technical accuracy, critical thinking, and professional presentation

Scenario submitted by Dr. Sophia George, Granby High School, Norfolk Public Schools

Claude AI (Anthropic) helped ensure proper formatting, comprehensive coverage of topics, and alignment with the Virginia CTE instructional scenario template and guidelines.