



# cs50 cybersecurity Project Harvard University Presentation

by Oladebo Ayanniyi

<https://github.com/oladebo?tab=repositories>

edX Account: oladeboayanniyi



# ❖ Case Study: University of Phoenix Data Breach (Dec 2025)

# ❖Content:

## Project Overview

- Situation and background purpose

## Objectives:

- Identification Problem(s) or Opportunities

## Faliure & Consequence

- State Hypothesis

## Answer

- Purpose Solution & discuss impact
- Lesson learn & Recommendation

## Executive Summary

- Conclusion

## ➤ Overview Business Objective

In December 2025, the University of Phoenix confirmed a **major data breach** after the Cl0p ransomware group exploited a *zero-day vulnerability* in Oracle's E-Business Suite. The breach impacted **3.5 million individuals** exposing:

- Names
- Contact details
- Dates of birth
- Social Security numbers
- Bank account information [TechRadar](#)

## ➤ Business Objectives

- **1. Enterprise software vulnerability:** The attackers exploited a previously unknown (zero-day) flaw in widely used enterprise software.
- **Insufficient patching & hardening:** This highlights **failure in vulnerability management**, patch application, and risk assessment for critical systems.
- **Data security controls missing or inadequate:** The exposure of highly sensitive personal and financial data shows that encryption and access controls weren't sufficiently protecting stored data. [TechRadar](#)

### Consequences

- Exposure of millions of people's private data.
- Regulatory and legal implications (privacy laws, credit monitoring obligations).
- Significant reputational damage for the

## ➤ Purpose Solution & discuss impact

### 2. Real-World Impact: Princeton University Phishing Data Breach

#### ✓ What Happened

A **class-action lawsuit** claims Princeton University failed to protect sensitive personal data in a phishing attack. The breach exposed data from students, parents, alumni, donors, and staff. [The Jersey Vindicator](#)

#### ✓ Technology & Failure

- . Phishing succeeded due to inadequate user education and email security controls.
- . Once attackers gained access, lack of **segmentation and monitoring** allowed broader data exposure.

# ➤ Purpose Solution & discuss impact

## 3. Regulatory Action: Change Healthcare Cyberattack Lawsuit

### ✓ What Happened

The Nebraska Attorney General's lawsuit against Change Healthcare survived a motion to dismiss, alleging violations of data privacy and security laws from a 2024 cyberattack. [The HIPAA Journal](#)

### ✓ Failure Highlights

- . Insufficient security controls in a healthcare tech environment.
- . Legal accountability when companies fail to protect consumer data under privacy laws.

# ➤ Purpose Solution & discuss impact

## ❖ 4. Bug Bounty Dynamics & Ethical Hacker Involvement (Industry Context)

### ✓ Bug Bounty Model Challenges

Recent industry coverage discusses how automation/AI may be “**breaking the bug bounty model**,” as more vulnerabilities are found and reported, complicating how organizations respond. [Cybernews](#)

Another report critiques that bug bounty schemes *by themselves* don’t guarantee secure software and that governments should hold developers liable for insecure code. [computerweekly.com](#)

### ✓ Why This Matters

- . Bug bounty programs are critical **prevention tools** — they help find vulnerabilities *before attackers do*.
- . But they are **not complete security solutions**; companies must integrate these discoveries into a full security program.

# ➤ Purpose Solution & discuss impact

## 5. Broader Threat Landscape (Context)

Cybersecurity news bulletins show ongoing threats like zero-day vulnerabilities (e.g., Cisco and other exploits), ransomware, and emerging AI-enhanced attacks that continue to challenge enterprise defenses. [The Hacker News](#)

# ➤ Key Lesson Learn & Recommendation

## 1. Key Lessons

- . **Regular and proactive patching** for known and emerging vulnerabilities across software stacks.
- . **Zero-trust and least privilege access models** for sensitive data.
- . **Encryption at rest and in transit** for personal information.
- . **Continuous risk assessments** for third-party/enterprise software.

## 2. Lessons

- . Implement **multi-factor authentication (MFA)** and strong email filtering.
- . Train users regularly to recognize phishing attempts.
- . Use **network segmentation** to limit access

# ➤ **Key Lesson Learn & Recommendation**

## **3. Lessons**

- . Healthcare data demands stringent protection due to sensitivity.**
- . Compliance alone isn't enough must be backed by solid risk management.**

## ❖ **Concluding Recommendations: Avoiding Similar Failures**

### **Technical Security Measures**

- ✓ Apply **timely patches and updates** across all software.
- ✓ Use **multi-factor authentication (MFA)** everywhere especially for admin and remote access.
- ✓ Encrypt **sensitive personal data at rest and in transit.**

### **Organizational Practices**

- ✓ Conduct **regular risk assessments and penetration testing** with both internal teams and **ethical hackers.**
- ✓ Integrate **bug bounty/VDP programs** to detect vulnerabilities early.
- ✓ Train employees on **phishing defense and secure practices.**

### **Governance & Compliance**

- ✓ Build cybersecurity into procurement (especially third-party software).
- ✓ Maintain incident response plans with drills.
- ✓ Monitor compliance with both privacy laws and internal security policies.

# ❖ Summary for our Presentation

Element	Details
Incident	University of Phoenix breach via zero-day (3.5M records)
Failure Type	Poor vulnerability and patch management
Technology	Enterprise software (Oracle E-Business Suite)
Impact	Massive privacy exposure & regulatory fallout
Prevention	MFA, encryption, patches, risk scanning
Supportive Press Examples	Princeton phishing lawsuit, Change Healthcare privacy case
Protective Mechanisms	Bug bounties & ethical hackers (improve proactive security)

The background is a dark blue gradient. On the left side, there are several overlapping, semi-transparent blue geometric shapes, including rectangles and parallelograms, some of which are tilted. On the right side, there is a pattern of small, light blue dots arranged in a grid, which fades out towards the center.

Thank You