

Instructional Scenario

Vulnerability Dilemma:

Ethical Hacking and Disclosure



Course/Duty Area: Cybersecurity Fundamentals/ Exploring Ethics as It Relates to Cybersecurity

Estimated Time Required: 4–6 hours

Scenario:

You are a junior security analyst at CyberGuard Consulting, a cybersecurity firm that conducts penetration testing for clients. During a routine security assessment of a regional hospital's patient portal, you discover a critical zero-day vulnerability that could allow unauthorized access to thousands of patient medical records, including sensitive information about diagnoses, medications, and treatment plans. The hospital is not currently a client, and you found this vulnerability while conducting research on common healthcare system architectures.

Your discovery presents several ethical dilemmas. The vulnerability affects not just this hospital, but potentially dozens of other healthcare facilities using the same software platform. The software vendor is a major healthcare technology company. You could: (1) report it directly to the hospital, (2) contact the software vendor through their responsible disclosure program, (3) report it to government agencies like CISA, (4) post it publicly to force immediate action, or (5) try to sell the information. Each option has different ethical implications, legal considerations, and potential consequences for patient safety.

Adding complexity to your decision, you learn that your supervisor has a professional rivalry with the hospital's Chief Information Security Officer. Your company is also competing for a lucrative contract with the software vendor. A colleague suggests that "finding" this vulnerability during a sales pitch to the hospital could help win their business. Meanwhile, every day the vulnerability remains unpatched puts real patients at risk. You must navigate professional ethics codes, legal obligations, business pressures, and moral responsibility for patient safety.

Big Question:

How do cybersecurity professionals balance ethical obligations to protect the public with legal requirements, business interests, and professional responsibilities when discovering critical security vulnerabilities?

Focused Questions:

- What ethical frameworks (utilitarianism, deontology, virtue ethics) can guide decision-making in cybersecurity dilemmas?
- What are the key principles in professional codes of ethics for cybersecurity (ISC² Code of Ethics, EC-Council Code of Ethics)?
- What is responsible disclosure, and how does it balance security researcher rights with public safety?
- How do business pressures and conflicts of interest challenge ethical decision-making in cybersecurity?
- What legal protections exist for security researchers, and what are the risks of different disclosure approaches?
- How does the urgency and severity of a vulnerability impact ethical obligations?
- What role do cybersecurity professionals have in protecting vulnerable populations (patients, children, elderly)?

- How can organizations create cultures that support ethical decision-making even when it conflicts with business goals?

Student Project or Outcome:

Students will create a comprehensive Ethical Decision-Making Framework and Case Analysis that includes

- an analysis of the scenario, using multiple ethical frameworks
- a stakeholder impact assessment (e.g., patients, hospital, vendor, employer, public)
- a recommended course of action with detailed ethical justification
- a step-by-step action plan with timeline and rationale
- analysis of potential consequences for each possible decision
- a comparison with relevant professional ethics codes
- policy recommendations for the consulting firm
- reflection on personal values and how they influence professional decisions.

Project-Based Assessment:

Students will participate in a Socratic seminar or panel discussion where they

- present their recommended decision with ethical justification (5–7 minutes)
- defend their position through Q&A from peers and teacher
- respond to counterarguments and alternative perspectives
- demonstrate understanding of ethical frameworks and professional codes
- submit a written ethics analysis paper (4–6 pages)
- complete a self-reflection on how their personal values influenced their decision.

Evaluation will use a rubric assessing ethical reasoning, knowledge of professional codes, consideration of consequences, ability to defend position, understanding of legal issues, and quality of written analysis. Emphasis on critical thinking, not "right" answers.

Teacher Resources:

- [ISC2 Code of Ethics](#)
- [EC-Council Code of Ethics](#)
- [CERT Guide to Coordinated Vulnerability Disclosure](#)
- Computer Fraud and Abuse Act (CFAA) overview and legal considerations
- Case studies (e.g., Google Project Zero disclosure practices, Marcus Hutchins case, white hat vs. black hat hacking)
- Ethical frameworks in cybersecurity (e.g., utilitarianism, deontology, virtue ethics)
- Guest speaker opportunity: Security researcher, ethical hacker, or healthcare CISO
- Rubric emphasizing ethical reasoning and professional judgment
- Debate/discussion facilitation guide
- HIPAA overview for healthcare security context
- Responsible disclosure timeline examples
- Assessment rubric focusing on critical thinking and ethical analysis rather than predetermined "correct" answers

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

Claude AI (Anthropic) was used in the development of this instructional scenario to ensure proper formatting, comprehensive coverage of topics, and alignment with the Virginia CTE instructional scenario template and guidelines.