BAKER COLLEGE
STUDENT LEARNING OUTCOMES

CRJ 3350 Cybercrimes
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Analyze the concept of cybercrimes.
    a. Distinguish between various types of cybercrimes, such as hacking, identity theft, phishing, malware, cyber stalking, ransomware, bullying, denial-of-service attacks and cyber fraud.
    b. Discuss the motivations between various types of cybercrimes, the effects of the crime, and the range of punishments if caught and convicted.
    c. Examine real-world cybercrime case studies to understand the tactics, techniques, and procedures employed by cybercriminals.
    d. Explain the pros and cons of the Internet of Things (IoT).

2. Examine the legal and ethical issues surrounding cybercrimes, including laws, regulations, and international agreements.
    a. Compare the ethical dilemmas faced by real-world individuals and organizations as it relates to data collections and individual privacy rights.
    b. Discuss the risks associated with the capture and storage of personal data by IoTs, organizations, businesses and large corporations.

3. Identify the monetary, professional, and personal losses associated with various cybercrimes.
    a. Discuss the impact of cybercrimes on individuals, organizations, and society using real-world cases.
    b. Discuss the predatory impact of cybercrimes on senior citizens, the poor, and disadvantaged.
    c. Discuss growing trends in cybercrime in the U.S. and globally and the future effects to people and business if they escalate.

4. Analyze basic cybercrime prevention strategies and the roles of the people who prevent cybercrimes.
    a. Explore basic strategies and techniques to prevent and mitigate cybercrimes for all individuals, including strong passwords and Multi-Factor Authentication

(MFA), regular software and security patch updates, firewalls and anti-virus software,

b. Explain the strategies and techniques to prevent and mitigate cybercrimes, including intrusion detection, incident response, and risk management.
c. Investigate best practices and strategies for enhancing cybersecurity within a personal context.
d. Explore the roles and differences between entry-level jobs in cybersecurity.

Big Ideas and Essential Questions

Big Ideas

- Types of cybercrimes
- Legal and Ethical Issues
- Losses due to Cybercrime
- Prevention Strategies

Essential Questions

1. Who commits the various types of cybercrimes and what are their motivations?
2. How do the legal and ethical issues that surround privacy and data collection impact cybercrime risk?
3. How extensive is the damage done by hackers and how can it be prevented?
4. How are the growing and ever-changing cyber threats here and abroad changing the way individuals and organizations prepare for, deal with and mitigate cybercrime?

These SLOs are approved for experiential credit.

Effective: Fall 2024