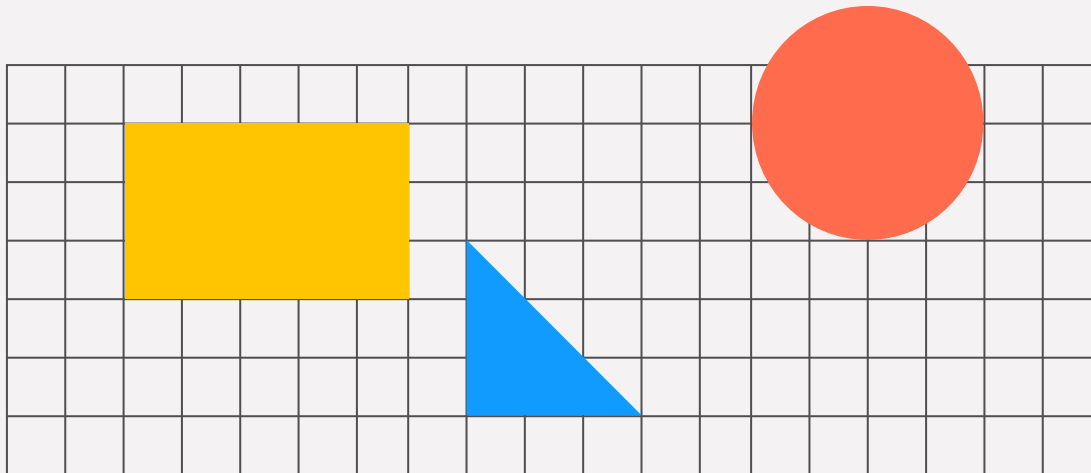


Final Presentation

Adelina Bowden, Justin Wilson, Ivan
Ofosu, Matthew Harris



Topics



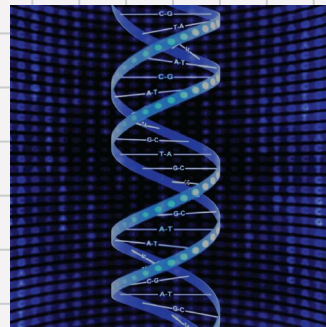
Bio-Cybersecurity

Cyber-Criminology

SCADA Systems

Cyber-Ethics

What is Bio-Cybersecurity?



- Bio-Cybersecurity focuses on protecting biological data (DNA sequences, medical records, biometrics) and systems from cyber threats.

Importance



- As we evolve technologically, we grow more reliant on bio-technology in healthcare, forensics, and other such fields. Without bio-cybersecurity these fields are vulnerable to cyber attacks.



Cyber attacks could include:

- DNA sequence tampering
- Medical device hacking (EX- insulin pumps and pacemakers)
- Privacy risks

Uses

- Bio-cybersecurity is used to protect:
 - Patient healthcare
 - Genetic records
 - Forensics in law enforcement
 - Prevent the remote hacking/manipulation of implantable bio technology such as pacemakers.

Real-World Examples



- In 2023, 23andMe, a popular genetic testing company, suffered a major data breach.
- Hackers exploited reused passwords from previous leaks to access customer profiles.
- ~6.9 million users affected.
- Stolen data included ancestry information, health-related genetic markers, and personal info.
- Data appeared on hacker forums and was sold in targeted batches (e.g., by ethnicity)

Long-Term Risk



- Are we too focused on short-term protection and not enough on the ethical, legal, and social consequences 5, 10, or 50 years from now?
- Are new biotech tools like CRISPR)advancing faster than our ability to predict their long-term effects?
 - CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats)

For a solution, we could build security by design and include ethical principles in our development of biotech.

CyberCrime in 2023

The IC3 is the Internet Crime Complaint Center run by the FBI and make annual reports.



- Complaints: 880,418 (a 10% increase from 2022)
- Losses: Over \$12.5 billion (a 22% increase from 2022)
- Top State Losses: California reported the highest, exceeding \$2 billion, with Texas, Florida, and New York following behind



In 2023, there was an increase in monetary losses from cyber crimes.

Key findings from the IC3 2023



Investment Fraud

- Losses rose from \$3.31 billion in 2022 to \$4.57 billion in 2023—a 38% increase
- Cryptocurrency investment fraud accounted for \$3.94 billion of these losses

Tech Support Scams

- Significant impact on older adults, with over half of the losses attributed to individuals over 60



Most common cyber crimes in the U.S:

1. Phishing
2. Personal Data Breach
3. Non-payment/ Non-Delivery
4. Extortion
5. Tech support Scams

Cyber Laws and Acts

State lawmakers target certain cyber crimes that are particularly impacting the people in their state.

Federal

- Computer Fraud and Abuse Act (CFAA) – 1986 - Main law for prosecuting cybercrime.
- Electronic Communications Privacy Act (ECPA) – 1986 - Includes the Stored Communications Act – applies to cloud services, ISPs.
- Digital Millennium Copyright Act (DMCA) – 1998 - Often used in cases involving piracy or illegal streaming tools


Federal laws are a baseline for cyber laws while state laws can be more specific when targeting certain cyber crimes.

Issues with the US legal system



- Many cybercriminals are not found or prosecuted with only 0.1% of cybercriminals are prosecuted in the US (over 880,000 complaints to IC3 and only 300-500 are federally prosecuted annually)
- Many cyber attacks come from people in foreign countries that do not extradite cybercriminals (China, Russia, and Iran)
- Cybercriminals using technologies (VPNS, proxies, encryption, and botnets) to stay hidden.
- Lack of resources in local police departments (Officers and Money)

What is Cyber-Ethics?

- 
- Ethics define what are right and wrong actions in situations.
 - In the cybersecurity, ethics serves as a beacon for cybersecurity professionals. It helps identify the type of online behavior and conduct that harms individuals and businesses.
 - Ethical doctrines separate CS professionals from hackers.

Why are Cyber-Ethics Important?




As cyber threats evolve, ethical considerations become crucial in guiding professionals to act responsibly and maintain trust. Ethical cybersecurity professionals use their skills to protect data, contrasting with malicious hackers who exploit it.

- Guides Responsible Behavior
- Builds Trust
- Prevents Abuse of Power
- Supports Legal Compliance

Ethics In Action

Trustworthiness:

- 
- Being entrusted with access to sensitive data and upholding integrity and confidentiality.


Adherence to Codes:

- Following established ethical frameworks ensures consistent and responsible behavior across the industry.

Continuous Vigilance:

- Staying informed about emerging threats and ethical dilemmas is vital for effective cybersecurity practice.

What are SCADA Systems?

- 
- Stands for: Supervisory Control and Data Acquisition
 - Electronic systems that control and monitor physical machines and systems
 - Used by nuclear power plants, power grids, and water utility systems

SCADA Vulnerabilities

- Default passwords
- Untrained personnel on cybersecurity concepts
- Not enough firewalls and physical security in place



Examples



- In 2021, Russian hackers infiltrated Colonial Pipeline, blocking oil transport to the East Coast of America.
- The hack cost \$4.4 million in ransomware payment with cryptocurrency
- In 2023, Volt Typhoon (Chinese hackers) infiltrated utility systems in the state of Massachusetts and had been left undetected for 10 months before being found

Long Term Risks



- The long term risks of vulnerability in SCADA systems is that as more things switch to being online, more things will be vulnerable to being hacked by other countries.

Short Arm of Predictive Knowledge

Due to the nature of technology, advancements happen much faster than the laws and policies can get ahead of.

This is why disaster recovery plans, backup plans and redundancy are extremely important.

- USCYBERCOM - the government's cyber force to respond to threats and attacks



Podcast

