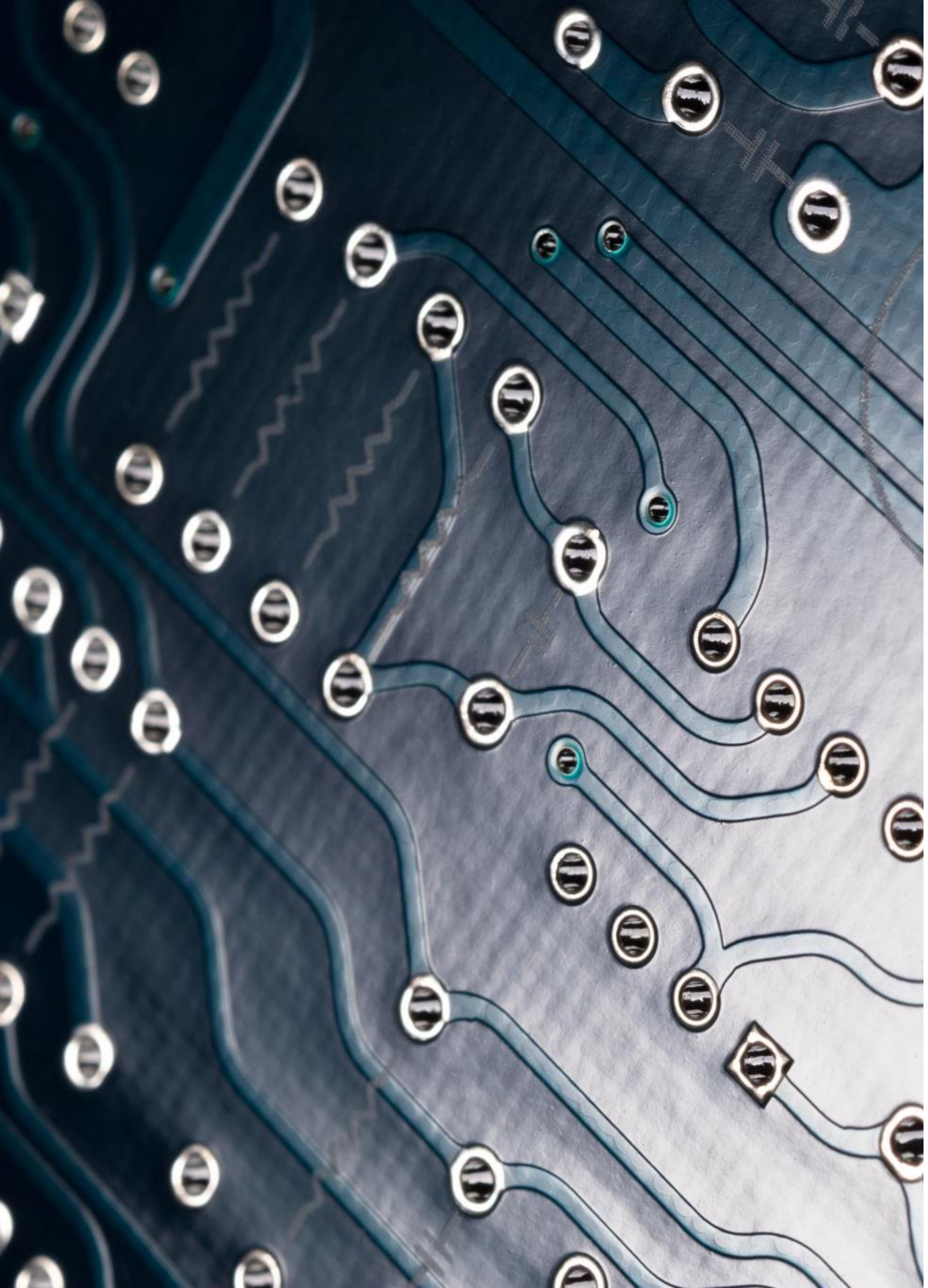
The Social Impact of Cybercrime

By: Myla, Jason, Tracy,
Mark, and Devin



INTRODUCTION TO CYBERCRIME

- What exactly is cybercrime?

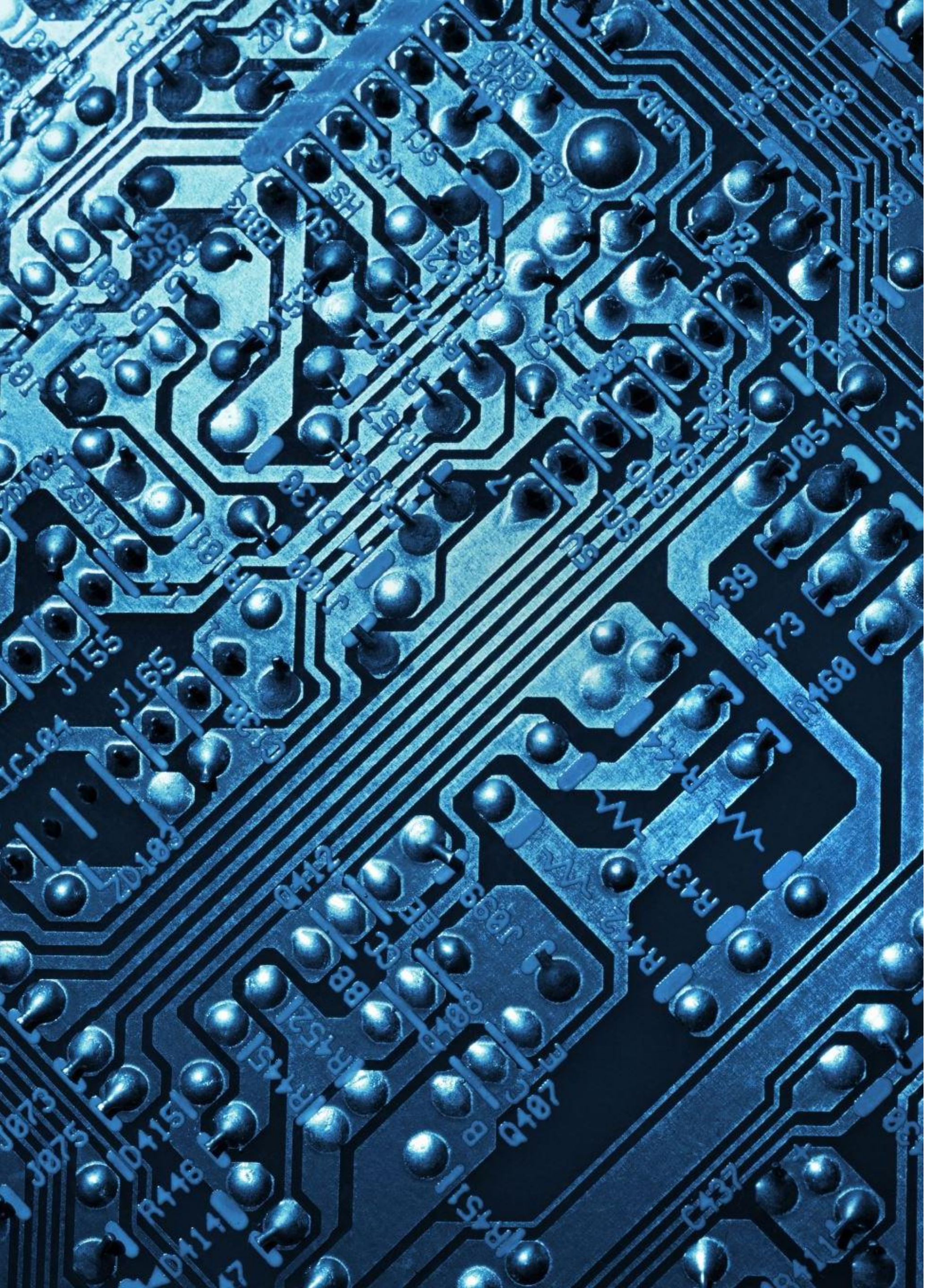
  - Cybercrime is the criminal activity using digital technologies

  - As our society digitizes, the number of threats increases and creates greater vulnerability in society

- The purpose of our presentation today is to examine the impact cybercrime has on victims, explore societal effects, and discuss the real-world cases and prevention strategies

Consequences for victims (1): Financial and privacy loss

- Victims can suffer from financial harm which could be identity theft, online fraud, or even ransomware.
- They can also suffer privacy breaches which is the exposure of personal data, medical records, and private communications.
- Individuals lose control over their own identities and finances
- A case study that we found was the *WannaCry Ransomware attack* that happened in May of 2017
    - This case affected 200,000+ systems worldwide
    - The UK National Health Services were disrupted, and many surgeries had to be cancelled
    - The estimated losses were around more than $4 billion



Consequences for victims (2): Psychological Impacts

- Cybercrime can have psychological impacts on their victims and bring them emotional distress, anxiety, and even trauma.
- Victims of cyberbullying or even sextortion can suffer long-term effects, which then can lead to them not trusting the internet or online platforms
- EXAMPLE: The movie *Cyberbully* which is based off a true story. A 17-year-old got a laptop for her birthday; she then gets on all these online platforms and sees that all these people from school are making fun of her and even experiences sextortion. This leads to her to attempt in suicide.
- https://www.youtube.com/watch?v=c1ilW2Areil

Broader Societal impacts : Economic, institutional, trust and national security

ECONOMIC AND INSTITUTIONAL

- The amount of global cybercrime damages are around $10.5 trillion/year by 2025 (Cybersecurity Ventures)
- Business disruptions lead to job losses and reduced consumer trust.
- Public institutions like healthcare and finances face rising costs for cybersecurity

TRUST AND NATIONAL SECURITY

- Can have a loss of public trust in technology, online banking, and governments as well
- Cyberattacks often threaten critical infrastructure and national defenses
- **Example: The solar winds attack (2020)**

- Compromised the U.S. government agencies and major corporations
- Exposed all the vulnerabilities in software supply chains
- Highlighted geopolitical dimensions of cybercrimes

Broader social effects

- Decline in broader trust

    - When people lack trust in digital services, individuals become less willing to use online healthcare, online banking, or even cloud services

- Social inequality and digital vulnerability

    - Recovery from cybercrimes are harder for the elderlies, low-income households, and people with limited digital literacy because they are more likely to experience phishing scams, have weak passwords, and lack access to cybersecurity tools

- Community disruptions

    -Cyberattacks targeting's your local infrastructures can affect the entire communities

- Increased fear and behavioral change

    - This digital withdrawal can slow a community progress apart of the digital world and can also slow down digital innovation

- Strain on public resources

    - Can reduce fundings for education, community programs, and local services

Social Inequality & Ethical Concerns/ Prevention Strategies: Individuals & Organizations

Social Inequality & Ethical Concerns

- Vulnerable groups (elderly, digitally unskilled) targeted more often
- Cybercrime deepens social divides and digital inequality
- Ethical challenges: misinformation, surveillance, data misuse

Prevention Strategies: Individuals & Organizations

For individuals:

- Strong passwords, multi-factor authentication
- Awareness and digital literacy
- Safe online behavior (avoid phishing/scams)
- **For organizations:**
- Security frameworks (ISO 27001, NIST)
- Employee training & incident response plans
- Data backup and encryption

Social Cybercrime Example

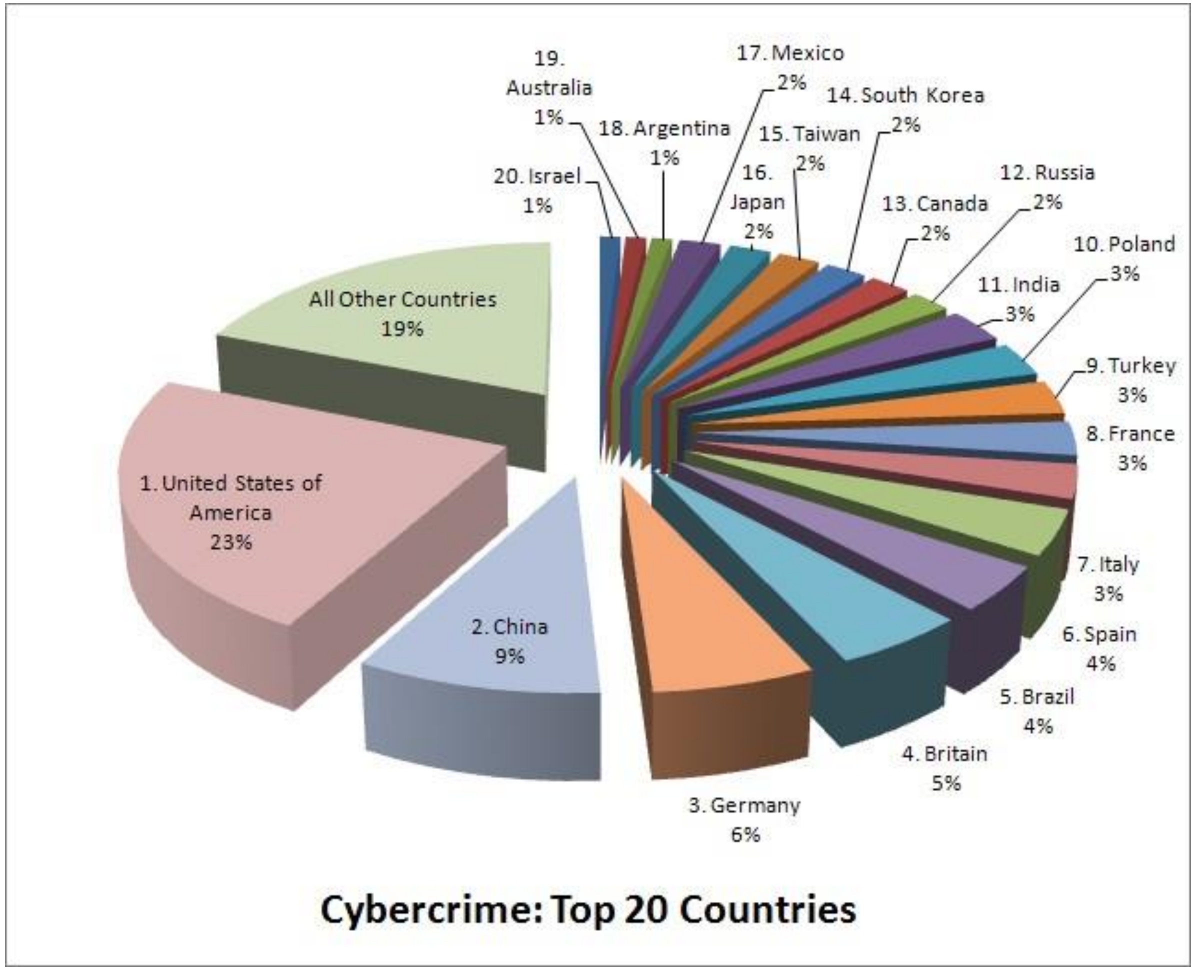
- Epsilon Data Breach (2011)
  - Best Buy
  - Target
  - JPMorgan
  - Chase

- Hacked into over 250 million emails
- Resold their information/data to people via document sharing websites and download
- Ended up costing entirely $4billion to recover

Prevention Strategies: Government & Global Cooperation

- **Stronger Cybersecurity Polices**
  - Governments need to enforce updated cybersecurity laws and data protection regulations.
- **National Cybersecurity Agencies**
  - More specialized agencies (e.g. CISA) are needed for threat detection and emergency responses.
- **International Collaboration**
  - Countries need to work together to share intelligence on threats and track cybercriminals.

List of Top 20 Countries with the highest rate of Cybercrime (source: BusinessWeek/Symantec)



REFERENCES

Greenberg, A. (2017). *The WannaCry ransomware attack explained*. Wired.

National Health Service (NHS). (2018). *Lessons learned from the WannaCry ransomware attack*.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Analysis of the SolarWinds Orion supply-chain compromise*.

Microsoft Security Response Center. (2020). *Deep dive into the SolarWinds attack*.

U.S. Government Accountability Office (GAO). (2021). *Federal response to the SolarWinds cyber incident*.