BITS Pilani

Dr Sashank Dara

WILP-CSIS

BITSPilani

Pilani Campus

SS ZG588- Cyber Crimes, Forensics and Incident Handling

Contact Session- 9

Module 8 -Organizations and Cyber Crime, Criminology and Organized Crime

8.1 Organizations and Cyber Crime

8.2 Criminology and Theories

8.3 Organized Crime and Technology

Organizations and cyber crimes

- Data breaches, denial-of-service attacks, malware, and corporate espionage are just some of the threats organizations have had to deal with these past several years.
- With the threat of a cyberattack looming on the horizon, businesses need to re-assess how they collect, store, and protect sensitive information. Many organizations have stopped the practice of storing their customers' personal and financial information on their servers.
- There's no data breach if there's nothing to steal.
- Some companies have even shut down their online storefronts due to growing concerns that they can't protect against an attack. Sixty percent of organizations that suffer a breach go out of business after six months.

Organizations and cyber crimes

- Because the recent attacks have been mainstream, customers are now demanding to know how firms handle their data.
- Even if cybercriminals can't break into a company's network, they can still cause problems by way of identity theft and fraud. Stolen personal information from one source can be the point of entry for another.
- Businesses need to have a good identity monitoring service in place to watch out for leaks and breaches that can affect their staff and clients.
- Companies that suffer a breach not only lose a treasure trove of sensitive data, they also lose business and face stiff fines or even lawsuits. As mentioned earlier, more than half of small businesses that get attacked aren't able to recover.

Organizations and cyber crimes

- If they pull through, there will always be a stigma that they're not taking their customer's information seriously.
- Another favorite of cybercriminals is disrupting operations by using a denial-ofservice (DoS) attack.
- A DoS attack will make websites or online stores unavailable to its users.
- Customers that can't log in or use a company's services are a significant revenue loss that can go viral.
- People who report on the issue and rant on social media can permanently damage the reputation of the affected company.

- The attack that forced Code Spaces out of business – what went wrong? - IT Governance UK Blog

Criminology and Theories

- Criminology is the study of why individuals commit crimes and why they behave in certain situations.
- Understanding why a person commits a crime, one can develop ways to control crime or rehabilitate the criminal. There are many theories in criminology.
- Some attribute crime to the individual; they believe that an individual weights the pros and cons and makes a conscious choice whether or not to commit a crime.
- Others believe it is the community's responsibility to ensure that their citizens do not commit crime by offering them a safe and secure place in which to live.
- Some ascertain that some individuals have latent traits that will determine how they will react when put in certain negative conditions.

Criminology and Theories

- By studying these theories and applying them to individuals, perhaps psychologists can deter criminals from repeating crimes and help in their rehabilitation.
- **Choice Theory:** The belief that individuals choose to commit a crime, looking at the opportunities before them, weighing the benefit versus the punishment, and deciding whether to proceed or not.
- **Classical Theory:** Similar to the choice theory, this theory ascertains that people think before they proceed with criminal actions; that when one commits a crime, it is because the individual decided that it was advantageous to commit the crime.
- **Conflict Theory:** The conflict theory holds that crime results from the conflicts in society among the different social classes, and that laws actually arise from necessity as a result of conflict, rather than a general consensus.

Criminology and Theories

- **Critical Theory:** Critical theory upholds the belief that a small few, the elite of the society, decide laws and the definition of crime; those who commit crimes disagree with the laws that were created to keep control of them.
- **Labelling Theory:** Those who follow the labelling theory of criminology ascribe to the fact that an individual will become what he is labelled or what others expect him to become; the danger comes from calling a crime a crime and a criminal a criminal.
- **Life Course Theory:** The theory that a person's "course" in life is determined by short (transitory) and long (trajectory) events in his life, and crime can result when a transitory event causes stress in a person's life causing him to commit a crime against society.

Criminology and Theories

- **Positivist Theory:** The positivist rejects the idea that each individual makes a conscious, rational choice to commit a crime; rather, some individuals are abnormal in intelligence, social acceptance, or some other way, and that causes them to commit crime.
- **Rational Choice Theory:** Reasons that an individual thinks through each action, deciding on whether it would be worth the risk of committing a crime to reap the benefits of that crime, whether the goal be financial, pleasure, or some other beneficial result.
- **Routine activity theory:** Followers of the routine activity theory believe that crime is inevitable, and that if the target is attractive enough, crime will happen; effective measures must be in place to deter crime from happening.

Criminology and Theories

- **Social Control Theory:** Theorists believe it is society's responsibility to maintain a certain degree of stability and certainly in an individual's life, to make the rules and responsibilities clear, and to create other activities to thwart criminal activity.
- **Social disorganization theory:** Suggests that crime occurs in communities that experience breakdown in social mores and opportunities, such as in highly populated, lower income, urban communities.
- **Social Learning Theory:** Social learning indicates that individuals learn from those around them; they base their morals and activities on what they see others in their social environment doing.

Criminology and Theories

- **Strain Theory:** The theory holds that individuals will turn to a life of crime when they are strained, or when they are unable to achieve the goals of the society, whether power, finance, or some other desirable goal.
- **Trait Theory:** Those who follow the trait theory believe that individuals have certain traits that will contribute to whether or not they are capable of committing a crime when pushed in a certain direction, or when they are in duress.

Organized Crime & Technology

- Cyber organized crime can include organized criminal groups engaging in cybercrime and cybercriminals or other groups that do not meet the criteria established by the Organized Crime Convention, that engage in activities typically associated with organized crime.

- Organized cyber crime groups may be small or large, loosely affiliated or welldefined; some groups are almost corporate in nature, with established leadership and various members filling specific functional roles.
- **Hacktivists:** Some groups of cyber criminals are driven by a particular political or social agenda. “Hacktivists” tend to be more interested in embarrassing companies or

publicizing damning evidence of some sort and are usually not interested in robbing their targets of money or assets.

- What is hacktivism? (techtarget.com)
- **Terrorists:** The threat of terrorism increased significantly in the aftermath of the September 11 attacks. Thankfully, most terror organizations lack the technical savvy and resources to pull off major cyber attacks. In fact, according to The International Cyber Terrorism Regulation Project, terrorist cyber crime tends to involve mostly the publication of propaganda, psychological campaigns (such as beheading videos), intelligence, information sharing and other communication.

Organized Crime & Technology

- **State-backed hackers:** Espionage continues to be prevalent in the modern world. Recent history is replete with examples of alleged state-backed hacking campaigns. The Stuxnet worm hack of the 2000s was allegedly developed by the U.S. and its allies to disrupt Iran's nuclear program. China has been accused of digital espionage involving U.S.

industrial secrets. In 2020, hackers allegedly backed by the Russian government accessed U.S. government and corporate networks by exploiting software made by SolarWinds.

- **Insider threats:** Criminal organizations can also target insiders with blackmail. The goal is to obtain corporate secrets, sensitive data, passwords and other types of access to secure networks that could result in the theft of money or information.

Blurred lines: As with most things, the real world is rarely neatly divided into precise categories. Many organized cyber crime groups participate in hacking "all of the above." A terrorist organization, for example, could employ tech-savvy individuals to recruit new members, run hacktivism campaigns and deploy a phishing campaign or

Organized Crime & Technology

ransomware attack to obtain sensitive cyber security information and finance terror operations.

Examples of Organized crimes –

- **Botnets**—a botnet is a network of computers that attackers infected with malware, compromised and connected them to a central command & control center. The attackers enlist more and more devices into their botnet, and use them to send spam emails, conduct DDoS attacks, click fraud, and cryptomining. Users are often unaware their computer is being used as a platform for cyber crime.

Organized Crime & Technology

- **Ransomware and other malware**—Ransomware is malware that encrypts data on a local machine and demands a ransom to unlock it. There are hundreds of millions of other types of malware that can cause damage to end-user devices and result in data exfiltration.

Examples of Organized crimes –

- **Phishing and other social engineering attacks**—phishing involves sending misleading messages via email or other channels, that cause internet users to provide personal information, access malicious websites or download malicious payloads.

Organized Crime & Technology

- **Fraud and identity theft**—fraud is the theft of funds by an attacker pretending to be the owner of an account, or using stolen cards or credentials. Identity theft is a related concept, and involves compromising a user's online accounts to enable an attacker to perform actions in their name.

Examples of Organized crimes –

- **Flood attacks**—most modern flood attacks are DDoS attacks, which leverage a botnet to hit a website or organization with massive amounts of fake traffic. Flood attacks can be targeted at the network layer, choking an organization's bandwidth and server resources, or at the application layer, bringing down a database or email server for example.
- **Browser hijacking**—attacks like cross site scripting (XSS) can cause malicious code to run in a user's browser. This can result in session hijacking, drive-by downloads and other illicit activity carried out in the user's browser without their consent.

Case study examples

- **In 2013-2016**, Yahoo experienced a data breach which resulted in the theft of 3 billion user accounts. For some of these accounts, the attackers got hold of private information and passwords, which could be used to access user accounts in other online services. Much of this data is available today, either free or for a price, on the dark web.
- **In 2014**, US retailer Home Depot's point of sale systems were breached. Attackers stole 50 million personal credit cards, and for some time any credit card swiped at Home Depot stores was captured and its details compromised by the attackers.

Case study examples

- **In 2016**, the largest ever distributed denial of service (DDoS) attack took place, which used over 1 million connected devices in the Internet of Things, which were compromised by the attackers due to software vulnerabilities. The attack caused outages in the global domain name system (DNS) and popular services including Twitter, Netflix and PayPal.
- **In 2017**, the WannaCry attack, allegedly launched by North Korea, unleashed a type of ransomware which not only locks down content on user devices, but also rapidly spreads itself. WannaCry infected 300,000 computers around the world, and users were asked to pay hundreds of dollars to decrypt and restore their data.

Air Force Network - Wikipedia

Thank you.