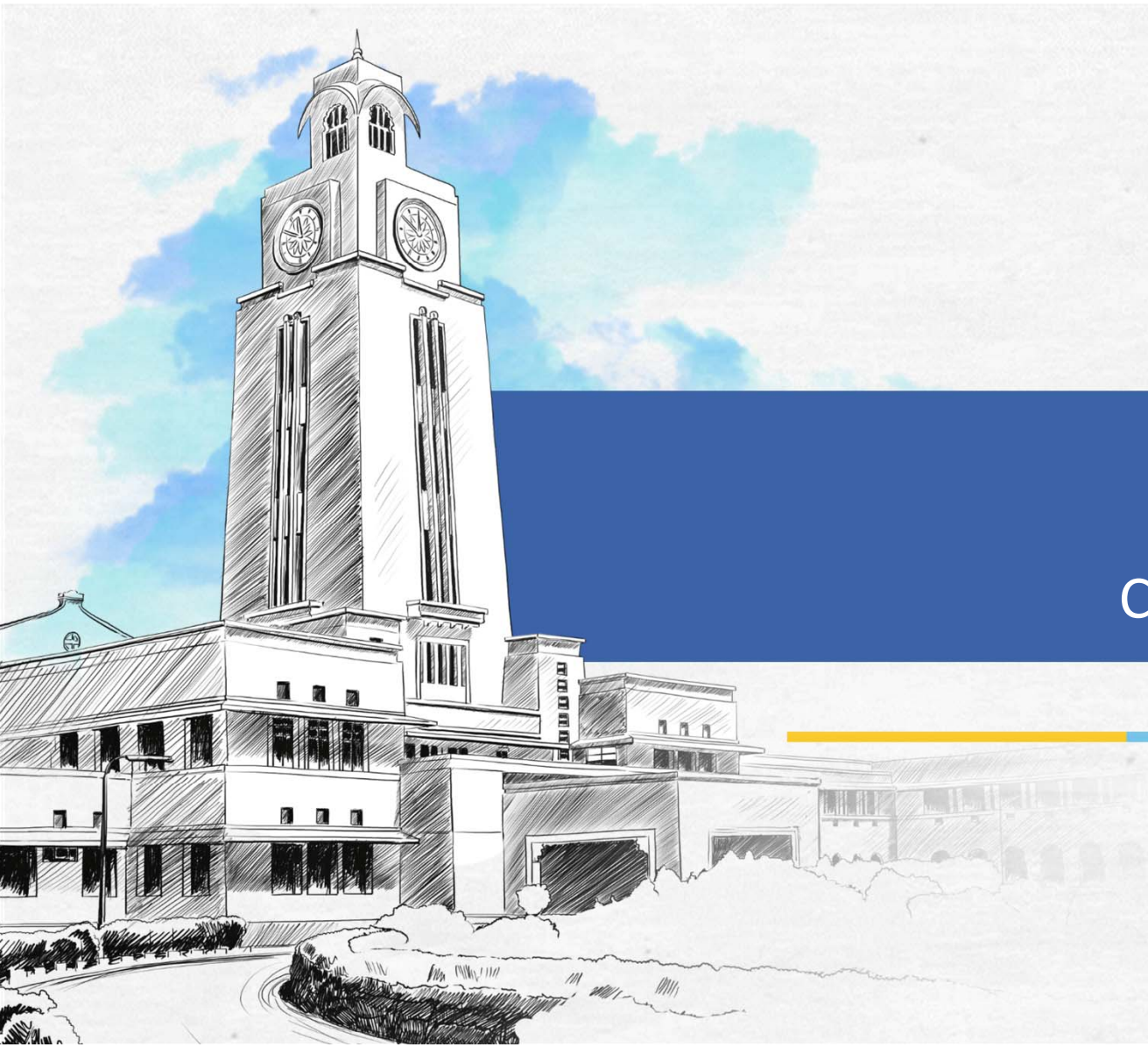


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Crimes and Offenses

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks

innovate achieve lead

Agenda

- Cyber Crimes and Offenses:
  - Introduction to Cyber Crimes
  - Motives
  - Classification of crimes and criminals
  - Types, frequency and amount of Cyber Crime
  - Organized Cyber Crime
  - Cyber terrorism
  - Cyber war
  - Cyber Crime Modus-Operandi and Social Engineering
  - Cybercrimes against individuals, organizations, and nations
  - Cyber Crime Techniques
  - Cyber Crime Monitoring and Prevention
  - Domestic and International Response

Introduction to Cyber Crimes

Introduction to Cyber Crimes

innovate achieve lead

Target Security Breach

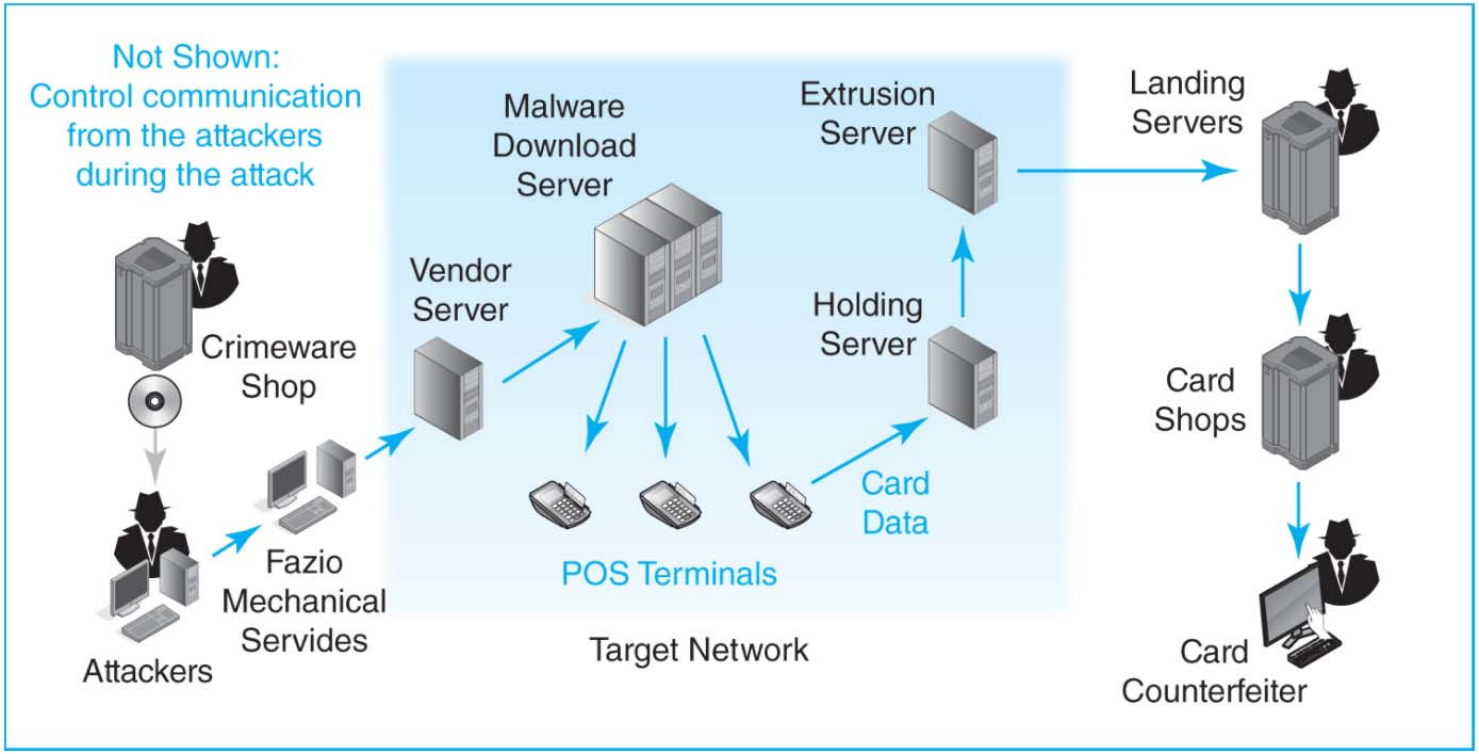
https://www.youtube.com/watch?v=M5tl4Yf92Nk&ab_channel=BloombergQuicktake
https://www.youtube.com/watch?v=w1o52wMzjFw&ab_channel=CNN
https://www.npr.org/2014/01/13/262185937/how-the-hackers-did-it-a-dicussion-about-targets-data-breach

Source: Internet

Introduction to Cyber Crimes

innovate achieve lead

Target Security Breach



Source: Business Data Networks and Security – Raymond R Pranko, Julia L. Pranko

Introduction to Cyber Crimes

innovate achieve lead

Target Security Breach

- Christmas Season 2013
- BlackPOS malware "scrapes" transaction data
- Data from 40 million credit card transactions stolen
- In separate attack, personal information on 70 million Target customers stolen
- Sales fell 5.3%, profits fell 46% (by $500 million)
- Several hundred million dollars due to lawsuits
- Chief Technology Officer and CEO fired

Source: Internet

Introduction to Cyber Crimes

innovate achieve lead

IT Security Breach Statistics

- Information is Beautiful
  - https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Data Breach Statistics
  - https://phoenixnap.com/blog/data-breach-statistics

Source: Internet

Introduction to Cyber Crimes

innovate achieve lead

Introduction

- Today, the Internet is an essential part of everyday life for most people
  - Businesses, Governments, and Individuals rely on the Internet for their daily routine
- Almost everything happens on the Internet these days:
  - conducting business,
  - performing research,
  - gathering information,
  - shopping,
  - entertainment,
  - payment for goods and services,
  - banking and financial tasks,
  - sending files and data to others, and
  - communicating with friends and family around the world
- It is estimated that about 31 percent of the Earth's population uses the Internet regularly

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Introduction to Cyber Crimes

innovate achieve lead

Introduction

- While advances in technology have benefited society, they have also created new opportunities for cybercriminals
- And as the computer technology becomes more advanced, so do the illegal activities
  - New criminal offenses are constantly being developed in the realm of cyberspace.
- Traditional crimes are also done online with the advancement of technology
  - E.g., fraud, theft, stalking, and bullying, Illegal drugs, and child pornography
- These new forms of crimes are occurring because they are comparatively easy to commit online
- Cybercriminals can…
  - easily hack into computer systems anywhere in the world with little cost and little risk of being caught
  - alter records and information, steal money, or steal the identities of innocent victims
  - offer goods and products for sale that cannot be purchased elsewhere
  - post with the intent of harming a person's reputation
- The software needed to carry out all of these malicious attacks can be purchased online for a small fee

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Introduction to Cyber Crimes

innovate achieve lead

Definitions

- Cyber crime has been defined differently by different researchers
  - *"A crime conducted in which a computer was directly and significantly instrumental"*
  - *"Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution"*
  - *"Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers"*
  - *"Any financial dishonesty that takes place in a computer environment"*
  - *"Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom"*

Source: Cyber Security by Nina Godbole and Sunit Belapure

Introduction to Cyber Crimes

innovate achieve lead

Types of Computer Crime

- *"Computer crime or cybercrime is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity"*

  --- New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

- The U.S. Department of Justice categories computer crime based on the role that the computer plays in the criminal activity
  - Computers as targets
  - Computers as storage devices
  - Computers as communication tools

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Introduction to Cyber Crimes

innovate achieve lead

Types of Computer Crime

- Computer systems as targets
  - In this category, a computer systems becomes a target
  - The crime involves:
    - Acquiring information stored on that computer system
    - Controlling the target system without authorization
    - Theft of service
    - Altering the integrity of data
    - Interfering with the availability of the computer or server
  - This form of crime involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Introduction to Cyber Crimes

innovate achieve lead

Types of Computer Crime

- Computers as storage devices
  - In this category of computer crime, computer or a computer device is used as a passive storage medium. For example:
    - Storing stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software)
- Computers as communication tools
  - In this category, computer crimes are simply traditional crimes that are committed online. For example:
    - Illegal sale of prescription drugs, controlled substances, alcohol, and guns
    - Fraud
    - Gambling, and
    - Child pornography

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Introduction to Cyber Crimes

innovate achieve lead

Types of Computer Crime

- The Council of Europe (EU) describes cybercrime as applied to three categories of criminal activities:
  - First, covers traditional forms of crime
    - E.g., fraud or forgery committed over electronic communication networks and information systems
  - Second, concerns with the publication of illegal content
    - over electronic media (i.e., child sexual abuse material or incitement to racial hatred)
  - Third, includes crimes unique to electronic networks
    - E.g., attacks against information systems, denial of service, hacking
    - These types of attacks can also be directed against crucial infrastructures such as power grids, nuclear plants, etc., with potentially disastrous consequences for the whole society

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Introduction to Cyber Crimes

innovate achieve lead

Types of Computer Crime

- Convention on Cybercrime, 2001
  - First international treaty that sought to address Internet crimes by harmonizing
    - national laws
    - improving investigative techniques, and
    - increasing cooperation among nations
  - It was developed by the Council of Europe and has been ratified by 43 nations, including the United States.
  - The Convention includes a list of crimes (see next slide) that each signatory state must transpose into its own law
    - This list represents an international consensus on what constitutes computer crime, or cybercrime, and what crimes are considered important

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Introduction to Cyber Crimes

innovate achieve lead

Cybercrimes Cited in the Convention on Cybercrime

Cybercrime	Description
Article 2: Illegal access	The access to the whole or any part of a computer system without right
Article 3: Illegal interception	The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data
Article 4: Data interference	The damaging, deletion, deterioration, alteration or suppression of computer data without right
Article 5: System interference	The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Article 6: Misuse of devices	a) The production, sale, procurement for use, import, distribution or otherwise making available of: i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and b) The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Source: Computer Security Principles & Practice by William Stallings & Lawrie Brown

Introduction to Cyber Crimes

innovate achieve lead

Cybercrimes Cited in the Convention on Cybercrime

Cybercrime	Description
Article 7: Computer-related forgery	The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible
Article 8: Computer-related fraud	The causing of a loss of property to another person by: a) Any input, alteration, deletion or suppression of computer data; b) Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Article 9: Offenses related to child pornography	a) Producing child pornography for the purpose of its distribution through a computer system; b) Offering or making available child pornography through a computer system; c) Distributing or transmitting child pornography through a computer system; d) Procuring child pornography through a computer system for oneself or for another person; e) Possessing child pornography in a computer system or on a computer-data storage medium.
Article 10: Infringements of copyright and related rights	No description
Article 11: Attempt and aiding or abetting	Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Source: Computer Security Principles & Practice by William Stallings & Lawrie Brown

Motives Behind Cybercrimes

Introduction to Cyber Crimes

innovate achieve lead

Motives

- Why do people commit cybercrime?
  - That is a tough question to answer
  - Every cybercriminal is different and has a different reason for his or her illicit behavior
- Cybercriminals commit crimes on the Internet to achieve many goals:
  - Financial Reasons
  - Disrupt Business
  - Terrorism
  - Theft (Nonfinancial)
  - Political Reasons
  - Amusement/Curiosity/Challenge
  - Organized Crime
  - Locating Victims

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Introduction to Cyber Crimes

innovate achieve lead

Motives

- Typical motives behind cybercrime are:
  - Greed
  - Desire to gain power and/or publicity
  - Desire for revenge
  - A sense of adventure
  - looking for thrill to access forbidden information
  - Destructive mindset
  - Desire to sell network security services

Source: Cyber Security by Nina Godbole and Sunit Belapure

innovate achieve lead

Classification of Crimes and Criminals

Classification of Crimes and Criminals

Classification of Cybercrimes

- Cybercrimes are classified as follows:
  - Cybercrimes against individual
  - Cybercrimes against property
  - Cybercrimes against organization
  - Cybercrimes against society

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Classification of Cybercrimes

- Cybercrimes against individual
  - E-Mail Spoofing and other online frauds
  - Phishing, Spear Phishing and its various other forms such as Vishing and Smishing
  - Spamming
  - Cyberdefamation
  - Cyberstalking and harassment
  - Computer sabotage
  - Pornographic offenses
  - Password sniffing

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Classification of Cybercrimes

- Cybercrimes against organization
  - Unauthorized accessing of computer
  - Password sniffing
  - Denial-of-service
  - Virus attack/dissemination of viruses
  - E-Mail bombing/mail bombs
  - Salami attack/Salami technique
  - Logic bomb
  - Trojan Horse
  - Data diddling
  - Newsgroup Spam
  - Industrial spying/Industrial espionage
  - Computer network intrusions
  - Software piracy

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

Classification of Cybercrimes

- Cybercrimes against property
  - Credit card frauds
  - Intellectual property (IP) crimes
- Cybercrimes against society
  - Forgery
  - Cyberterrorism
  - Web jacking
    - Web application improperly redirects a user's browser from a page on a trusted domain to a bogus domain without the user's consent

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Selected Crimes

- Cyberdefamation
  - According to Indian Penal Code (IPC), defamation is
    - *"Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person"*
  - Cyberdefamation happens when the above takes place with the help of computers and/or the Internet
  - E.g., someone publishes defamatory matter about someone on a website or sends E-mail containing defamatory information to all friends of that person
  - *Libel* is written defamation
  - *Slander* is oral defamation

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Selected Crimes

- Salami Attack/Salami Technique
  - These attacks are used for committing financial crimes
  - The core idea is to make the alteration so insignificant that in a single case, it would go unnoticed
  - For Example:
    - A bank employee inserts a program that deducts a small amount of money (Say Rs.0.10/-) in a month from the account of every customer
    - Account holders probably won't notice such a small unauthorized debit
    - However, the bank employee makes a sizeable amount every month

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

Selected Crimes

- Data Diddling
  - Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system
  - It involves altering raw data just before it is processed by a computer and then changing it back after the process is complete
  - The original data is changed, either by a person typing in the data, a virus, or a programmer during recording, encoding, examining, checking, converting or transmitting data
  - Using this technique, the attacker may modify the expected output and is difficult to track
  - For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full
  - Other examples include:
    - Forging or counterfeiting documents
    - Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

Selected Crimes

- Industrial Spying/Espionage
  - Industrial Spying involves getting secret information about
    - product finances,
    - product designs,
    - research and development,
    - marketing strategies,
    - etc.,.
  - With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now generating profits out of industrial spying
  - Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Cybercriminals

- Cybercriminals are those who use mobile phones, laptop computers, or network servers to commit a cybercrime
- For example:
  - a cybercriminal may hack into a computer network to disseminate a computer virus
  - an offender may use a computer to send child pornography to another user or steal another person's identity
- An offender commits a computer crime when he or she uses a computer as the tool to commit a crime
- A cybercriminal usually needs to have more than a basic level of computer knowledge to commit a computer crime
- Because of the nature of technology, it is sometimes difficult to identify the person who is responsible for a virus, attack, or other cybercrime

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Classification of Crimes and Criminals

Classification of Cybercriminals

- Cybercriminals are categorized into three groups that reflects their motivation
  - Type I: Those who are hungry for recognition
  - Type II: Those who are not interested in recognition
  - Type III: Those who are insiders

Source: Cyber Security by Nina Godbole and Sunit Belapure

Classification of Crimes and Criminals

innovate achieve lead

Classification of Cybercriminals

- Type I: Those who are hungry for recognition
  - Hobby hackers
  - IT professionals
  - Politically motivated hackers
  - Terrorist organizations
- Type II: Those who are not interested in recognition
  - Psychological perverts
  - Financially motivated hackers (corporate espionage)
  - State-sponsored hacking (national espionage, sabotage)
  - Organized criminals
- Type III: Those who are insiders
  - Disgruntled or former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and/or theft

Source: Cyber Security by Nina Godbole and Sunit Belapure

Types and Frequency of Cybercrime

Types and Frequency of Cybercrime

innovate achieve lead

Types of Cybercrime

- There are many types of cybercrimes and therefore many ways to categorize them
- For example, the U.S. Department of Justice categorizes types of computer crime in three ways:
  1) the computer as the target
     - involves attacking other computer systems
       - E.g., by spreading viruses or a denial-of-service [DoS] attack
  2) the computer as the weapon
     - using a computer to commit traditional crimes
       - E.g., fraud, illegal gambling, or online pornography
  3) the computer as an accessory or a device that contains data incidental to the crime
     - using a computer as a method to maintain records on illegal or stolen information

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

Types of Cybercrime

- The United Nations lists five categories of cybercrime:
  1) financial
     - crimes that disrupt a business's ability to conduct e-commerce
       - E.g., viruses, cyberattacks or DoS attacks, or e-forgery
  2) piracy
     - making illegal copies of copyrighted material
  3) hacking
     - the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access
  4) cyberterrorism
  5) online pornography

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Types of Cybercrime

- Another categorization is based on the intended victim of the crime:
  1) cybercrimes committed against people
     - e.g., the transmission of child pornography or stalking or harassment using a computer
  2) cybercrimes against property (asset), most likely the computer
     - e.g., a virus
  3) cybercrimes against government
     - e.g., cyberterrorism

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Types of Cybercrime

- Cybercrimes committed against people
  - Sex Offenses:
    - Sexting, Child Pornography, and Sexual Predators
  - Identify theft
  - Hacking
  - Session hijacking
  - Password cracking
  - Vice crimes
  - Harassment
    - Cyberstalking and Cyberbullying
  - Cybertheft
  - Computer-based Fraud
  - Auto Auction Fraud
  - Dating Scams
  - FBI/Government Official Scam
  - File Sharing/Internet Piracy
  - Phishing
  - Social Engineering

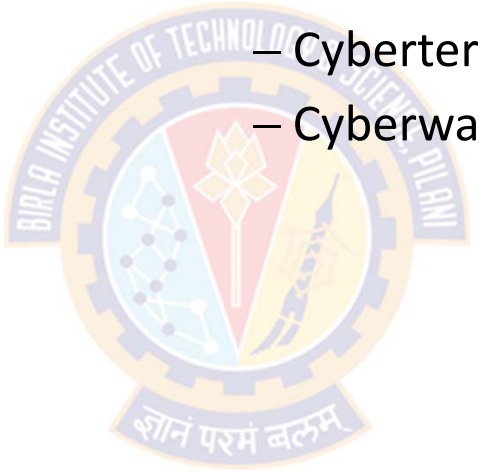
Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Types of Cybercrime

- Cybercrimes against Property (Computer Vandalism)
  - Viruses
  - Bots
  - Trojan Horses
  - Worms
  - Spyware
  - Logic Bomb
  - Rootkit
  - Spam
  - Denial-of-Service
  - Ransomware
- Cybercrimes against Governments
  - Cyberterrorism
  - Cyberwarfare



Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Sex Offenses
  - Research found that nearly 1 of 10 people consume online child pornography regularly
  - New technologies and the Internet makes it easier to trade and distribute images and videos in the global market
    - E.g., digital cameras, personal computers, software, and remote storage drives
  - Deep fakes make is even worse
  - Social media sites (E.g., online dating)
    - Sexual predators fake their identity and prowl the Internet
  - The prevalence of child pornography has increased by 82.2 percent since 1994
    - --- Center for Missing and Exploited Children
  - Between 2004 and 2008 there has been an increase of over 200 percent in online enticement of minors
    - --- Crimes Against Children Task Force
  - Through the Child Victim Identification Program, over 1.3 million images of children online have been documented

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Identity Theft
  - Identity theft refers to
    - "all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."
  - Involves stealing of personal information from a victim
    - E.g., Social Security number, date of birth, home address, passwords, or driver's license number, and then using that information to access a victim's bank accounts and/or make charges on the victim's credit cards
  - Can be subdivided into four categories:
    - Financial identity theft
      - Criminal uses another person's personal information to steal funds from an account or otherwise obtain goods and services
    - Criminal identity theft
      - Person poses as another person when accused of a crime or apprehended for a crime
    - Identity cloning
      - Criminal uses another person's identifying information to assume that identity in daily life.
    - Business/commercial identity theft
      - Involves using another's business name as a means to obtain credit

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Identity Theft
  - Different ways of stealing personal information
    - Fake emails and websites (Phishing)
    - Dumpster diving
    - Skimming
      - Stealing credit/debit card numbers by use of a special storage device when processing a card
    - Diverting billing statements by completing a change of address form
    - Using traditional methods such as stealing wallets, purses, or preapproved credit cards
    - Using spyware, Trojan horses, or hacking
    - Shoulder surfing
      - By looking over someone's shoulder as they type in information at an ATM or a store checkout

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

Cybercrimes committed against people

- Hacking
  - Hacking is unauthorized or illegal access to a computer system
  - Hackers look for vulnerabilities or for systems that are poorly protected to get inside the system
  - Once in the system, hackers can do anything:
    - Change information to cause confusion or harm
    - Steal a person's identity
    - Change the appearance of a website
    - Steal copyrighted software
    - Access classified information
    - Install malware
    - Launch a DoS attack

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Types of Hackers
  - Black hat hacker
    - Also known as cracker
    - Refers to a person who attempts to exploit flaws in a system for malicious purposes
  - White hat hacker
    - Also called as "sneakers" or "tiger teams"
    - A person who does not have any criminal intent and does not intend to commit any crimes
    - Looks for potential gaps in security and, thus, learn how to protect systems better
    - Companies hire white hat hackers to hack into their systems and recommend ways to improve the security systems
  - Grey hat hackers
    - These individuals are somewhere in between black hat and white hat hackers
    - Sometimes they hack into computers to commit crime and other times do so with no intent of harm
    - They may search for weaknesses but only disclose those vulnerabilities to the system administrator under certain circumstances, often for monetary reward

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Motivation behind hacking
  - Entertainment
    - Hackers who are curious or bored, see hacking as entertainment
  - Challenge
    - Some see hacking as a challenge or may seek to point out possible security risks
  - Feel the power or peer recognition
  - Ideals
    - For example, believing that all information should be free and accessible to everyone and that there should be no secrets
  - Political reasons
    - Cyberterrorism
    - They may seek to infiltrate the websites of competing political organizations
  - Helping others
    - Hackers want to help those living under totalitarian regimes exchange information more freely

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Categories of Hackers
  - Casual hackers (also referred as "script kiddies")
    - Tend to be less skilled and usually only commit nuisance crimes
    - Use tools purchased from the Internet
    - Usually motivated by curiosity or by the thrill of breaking into a system
  - Political hackers (also called as "cyberactivists.")
    - These hackers have specific targets and are pursuing a specific cause
    - The knowledge and skill of political hackers can vary, but they generally tend to deface websites
  - Organized crime hackers who seek a profit
    - They focus on breaking into bank accounts, stealing credit card numbers, or stealing confidential information
    - They focus on business computer systems that are likely to have data on many people
  - Phreakers
    - Consists of those who hack telephone systems
    - They were more prevalent prior to the advent of cell phones

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

Cybercrimes committed against people

- Vice crimes
  - A vice is a practice, behavior, or habit generally considered immoral, sinful, criminal, rude, taboo, depraved, or degrading ,deviant or perverted in the associated society
  - Many vice crimes are now committed online
    - E.g., sale of illicit or prescription drugs
      - The sale of these drugs via the Internet is illegal except to a customer through a state-licensed pharmacy based in the United States
    - E.g., online gambling
      - It is illegal in the United States
      - Gambling service providers require electronic payment via credit cards, debit cards, or electronic fund transfers
    - E.g., online prostitution
      - This is against the law
      - Involves accessing the Internet crosses state and national borders

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Computer-based Fraud
  - Fraud is a lie
  - If someone leads you to believe something that is false to benefit them, they are lying and committing fraud
  - A fraud can result when a victim voluntarily gives money or property to another person who has misrepresented himself/herself or the service they are offering
  - For example:
    - investment offers
    - auction fraud
    - failure to send merchandise
    - sending a buyer a product that is less valuable than what was originally advertised
    - failure to deliver a purchased good in a timely manner or at all
    - failure to disclose all relevant information about a product or terms of the sale

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Computer-based Fraud
  - "Internet fraud"
    - Refers to any type of fraud scheme that uses one or more online services:
      - E.g., chat rooms, email, message boards, or websites
    - Involves
      - presenting fraudulent solicitations to prospective victims
      - conducting fraudulent transactions
      - transmitting the proceeds of fraud to financial institutions or to others connected with the scheme
  - Some common types of Internet fraud
    - identity theft
    - purchase scams
    - counterfeit money orders
    - phishing for sensitive information
    - click fraud, whereby false hits are generated for websites to gain advertising money

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Auto Auction Fraud
  - Cybercrime that involves the sale of automobiles
  - Someone will try to sell a car that they do not own or is not in their possession
  - They will place the car for sale at a price far below the car's true value, explaining that they must sell it because they are moving and cannot take the car with them, or are facing an emergency and need the money
  - Because of the urgency, the seller asks that the car be sold quickly
  - They ask the buyer to send a full or partial payment immediately, and once the payment is received, the offender takes the money and disappears
  - According to the Internet Crime Complaint Center (IC3), there were 16,861 reports of vehicle scams in 2014 (https://www.ic3.gov/)
    - Total reported losses were $56,222,655.26

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- Dating Scams
  - These cyber scams are related to people who seek a romantic partner online through a dating website or a social media outlet
  - Often, the pair never physically meet but will converse online for many weeks or even months
  - The offender will ask for money, claiming to be in some emergency or suffering a tragedy, or maybe sick and need financial help
  - A victim may be willing to send money, because they have met their soulmate and are sure that eventually there will be a future relationship
  - Once the offender receives the money, they disappear

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes committed against people

- FBI/Government Official Scam
  - Victims will receive an email that seems to be from a high-ranking government official such as the director of the FBI
  - In some cases, the official's name is included to make the email appear more authentic
  - The letter will demand payment for an outstanding bill or some other purpose
  - Because it seems official and threatening, many people who receive the note actually send money, which ends up in the hands of a criminal, not the FBI or other agency
  - In 2013, the IC3 (https://www.ic3.gov/) reports that there were 9,169 complaints of this scam, with a loss of $6,348,881.28
  - Another version of this scam has been termed the "grandparent scam," in which an elderly person gets a message that a grandchild needs financial assistance
    - In some cases, the email may appear to be from the grandchild
  - The grandchild pleads for money because he or she has been the victim of a crime, often in a foreign country, and needs money to get medical help or to travel home

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

innovate achieve lead

Cybercrimes against Governments

- Cyberterrorism
  - According to the FBI, cyberterrorism is any
    - "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents."
  - Cyberterrorism occurs when an individual or group hacks into a government website with the intent of causing terror, violence against persons or property, or enough harm to generate fear
  - These acts are usually planned, are premeditated, and use computer technology to commit politically motivated violence against civilians
  - These are criminal acts that target national security data and top secret information or that disrupt the provision of services
  - They are designed to cause physical violence or extreme financial harm
  - Possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

Cybercrimes against Governments

- Cyberterrorism
  - Terrorist groups also use the Internet to
    - communicate with each other, spread information about their activities, and plan future attacks
    - attack a particular target to spread panic and alarm, recruit new members, or seek donations
  - In 2007, Michael Curtis Reynolds from Montana was part of a plot to blow up the Trans-Continental gas pipeline with help from Al Qaeda
  - He also had similar plots against an oil refinery in Wyoming and the Trans-Alaska oil pipeline
  - He was arrested in 2005 as he was picking up a bag that contained $40,000 from an Al Qaeda contact
  - He was tried and convicted of charges related to cyberterrorist activities
  - He defended his actions by explaining that he was trying to catch terrorists
  - The court did not believe his story, and he was sentenced to 30 years in prison

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Types and Frequency of Cybercrime

Cybercrimes against Governments

- Cyberwarfare
  - Also known as cyberwar
  - Cyberwarfare is an attack on technology
  - It is the ability to carry out large-scale attacks on computers, websites, and networks
  - Criminals do things like:
    - hijacking a satellite or phone network
    - hijacking computers and turning them into zombies that spread malicious code
    - paralyzing a website by repeatedly trying to gain access through a DoS attack
  - For example:
    - One side could start a DoS attack so that armies will not be able to keep in touch with each other
    - The other side, can hack into a system and track what the enemy is doing or planning
  - They can also use the Internet to deface websites and post inaccurate or false information that embarrasses the other side

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

Amount of Cybercrime

innovate achieve lead

Introduction

- Information about the amount of cybercrime that exists helps in analyzing trends and patterns in cybercrime
- This information could be used to make predictions and mitigate or prevent further crime
- Unfortunately, accurate statistics on the number of cyber events and the revenue loss are simply not known
- Some agencies have attempted to estimate the number and patterns of cybercrime based on reported offenses
  - However, not all cybercrimes are reported
- Why Is the Amount of Cybercrime Unknown?

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported
  - Cybercrimes remain unrecognized
    - Most computer crimes remain unrecognized and therefore are not reported to officials
    - Sometimes a criminal hacks into a computer system but does no damage, or the damage is so small it is not identified
    - For Example:
      - pirated files may be shared among users without the knowledge of the original artist who thus cannot report the theft
  - Embarrassment
    - Even those who are aware that a crime occurred may not report it to authorities because
      - They may be embarrassed that they fell for a phishing scam
      - They may feel foolish that they believed someone who told an outlandish story on a dating website
      - The victims may suffer only embarrassment and no financial harm, so they assume nothing can be done

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported, Contd…
  - Lack of understanding
    - Some victims may not understand that what occurred was a crime that could be reported
      - For example, a victim of cyberbullying may think the offender is just mean but does not consider the act to be a criminal offense
  - Fear of negative publicity
    - Many companies may be hesitant to report cybercrime incidents because they wish to avoid the negative publicity and possible loss of confidence by customers
  - Lack of confidence in the legal system
    - Many victims of cybercrimes may think that even if they do report a crime, the criminal will probably not be caught and punished for the crime, so they opt to forgo filing a formal report
  - Cybercriminals remain undetected
    - Many cybercriminals are very technologically savvy and have many tools to help them remain undetected
      - Instruments such as encryption devices make it difficult for law enforcement to track down the offender

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported, Contd…
  - Lack of clear/standard definitions
    - In some cases, there is a lack of clarity regarding the definition of the concepts involved
      - E.g., the meaning of the term "cyberbullying" may vary from one jurisdiction to another
    - If a crime is a newly evolved offense, law enforcement may not know how to handle it
    - They may not know how to collect the required evidence needed to prosecute the offender
    - Thus, even if a victim attempts to report an offense, the confusion may prohibit an accurate reporting of events
  - Lack of clarity on the jurisdiction
    - In some cases, a victim may not know whom to report the crime to
    - Is a cybercrime an issue for local police or for a federal agency such as the FBI?
    - Who has jurisdiction over a crime when there are no boundaries per se?

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

Why Is the Amount of Cybercrime Unknown?

- Because so many crimes go unreported
  - the true amount of cybercrime is unknown, and
  - the damages caused by cybercriminals have been underestimated
- Despite the difficulties, many agencies have attempted to track the number of crimes reported
  - this is likely not an accurate portrayal of actual crimes

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

Sample Surveys/Reports

- Cyber Security Breaches Survey 2021
  - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021
- The Internet Crime Reports by the IC3 – 2020
  - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- RSA Security
  - is an American computer and network security company with a focus on encryption and encryption standards
  - https://www.rsa.com/content/dam/en/white-paper/2019-current-state-of-cybercrime.pdf
- 2018 State of Cybercrime
  - https://www.secureworks.com/resources/rp-2018-state-of-cybercrime
- 2017 Cybercrime Report
  - https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
- 2017 Cost of Cybercrime Study
  - https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
- 2021 National Technology Security Coalition
  - https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

2010 – 2011 Computer Crime and Security Study

- Instead of relying on reported incidents of cybercrime, the Computer Security Institute surveyed the agencies and asked if they had ever experienced a cyberattack
- The goal was to determine a more accurate picture of the number of cyber offenses
- The Institute surveyed 5,412 security practitioners by traditional mail and email
- Questions were asked about cybercrimes committed from July 2009 through July 2010
- In total, 351 surveys (less than 7%) were completed and returned
  - 49.8% (almost half) had not experienced a security incident in the previous year,
  - 41.1% had experienced some type of cybersecurity incident, and
  - 9.1% did not know
- Just over 40% (of 351 security personnel) admitted to an attack, but about 9 percent did not know whether they had been attacked at all

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

2010 – 2011 Computer Crime and Security Study

- Of those who had experienced an attack (among the 41.1%)
  - 21.6% reported that they were the victim of a targeted attack
  - 54.5% percent were not targeted, and
  - 24% percent were unable to determine the type of attack
  - 67.1% reported malware attack
    - Malware seems to be most common type of attack
  - 8.7% reported financial fraud incidents
  - 59.1% did not believe their losses were because of malicious acts by insiders
  - 39.5% reported that none of their losses were because of non-malicious insider actions
- Few of the respondents were willing to share information about the financial losses the company had suffered as a result of the attack
  - However, they did report that their losses were not due to cybercrime perpetrated by insiders

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

2010 – 2011 Computer Crime and Security Study

Category	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots/zombies			21	20	23	29
Password sniffing			10	9	17	12
Financial fraud	7	9	12	12	20	9
Denial-of-service attack	32	25	25	21	29	19
Website defacement	5	6	19	6	14	7
Insider abuse of Internet access or email (e.g., pornography, pirated software)	48	42	59	44	30	25
Unauthorized access or privilege escalation by insider					15	13
System penetration by outsider					14	11
Theft of or unauthorized access to personally identifiable information due to mobile device theft/loss				8	6	5
Theft of or unauthorized access to intellectual property due to mobile device theft/loss				4	6	5
Theft of or unauthorized access to personally identifiable information or protected health information due to all other causes				8	10	11
Theft of or unauthorized access to intellectual property due to all other causes				5	8	5

*Blank boxes indicate that the data pertaining to that category was not gathered that year.

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

The 2012 Norton Cybercrime Report

- The Norton Cybercrime Report is based on an annual survey of officials in 24 countries about their experiences with cybercrime
- The 2012 survey included officials from 24 countries
- The agency conducted an online survey of 13,018 adults between the ages of 18 and 64 years
- The findings indicated that
  - there were 556 million victims of cybercrime each year, or 18 victims per second
  - there were 1.4 million cybercrime victims every day
  - the average loss per victim was $197 when measured globally ($290 in the United States)
  - the cost of consumer cybercrime is about $100 billion a year
    - this figure may be low because so much cybercrime is unreported
- Of the respondents, 15% had had their social network profiles hacked and said that another person had pretended to be them
- About 10% of social websites reported that they had fallen for a scam or fake link on a social network

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Amount of Cybercrime

innovate achieve lead

2013 European Network and Information Security Agency

- In 2013, the ENISA, the European Union agency published the report
  - *ENISA Threat Landscape: Responding to the Evolving Threat Environment*
- This was a meta-analysis of 120 separate reports published between 2011 and 2012 by different groups and agencies
- The report reviews potential threats and threat agents and lists the top threats and emerging trends in today's advancing technology
  - Drive-by exploits
  - Worms/Trojan horses
  - Code injection attacks
  - Exploit kits
  - Botnets
  - Denial-of-service attacks
  - Phishing
  - Compromising confidential information
  - Rogueware/scareware
  - Spam

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!