1.1. Introduction to Traditional Computer Crime

Computer crime is any criminal offense, activity or issue that involves computers. Computer misuse tends to fall into two categories. Computer is used to commit a crime. Computer itself is a target of a crime. Computer is the victim. Computer Security Incident. Computer Incident Response.

- **Computer Forensics** involves the preservation, identification, extraction, documentation and interpretation of computer data
- **Computer Forensics** is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law.
- **Computer forensics,** still a rather new discipline in computer security, focuses on finding digital evidence after a computer security incident has occurred.

The goal of **computer forensics** is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it.

Introduction

- The introduction of the **Internet** has created unparalleled opportunities for commerce, research, education, entertainment, and public discourse. A global marketplace has emerged, in which fresh ideas and increased appreciation for multiculturalism have flourished.
- The introduction of computerized encyclopedias, international consortia, worldwide connectivity, and communications has greatly enhanced quality of life for many individuals.
- Indeed, the Internet can be utilized as a window to the world, allowing individuals to satiate their curiosity and develop global consciousness. It allows individuals to experience those things that they have only dreamed about.
- Interested parties can visit the Louvre, devouring priceless artifacts at their leisure or take an African safari without the heat or mosquitoes. They can find answers to the most complex legal or medical questions or search for their soul mates.

- They can download coupons for their favorite restaurants or search for recipes to their favorite dishes.
- In addition, individuals, corporations, public organizations, and institutions can more effectively advertise their products or services, using graphically highlighted information and providing links to supplemental information or support.
- In fact, computerized access to unprecedented information has cut across traditional boundaries of communication.

Cyberspace and Criminal Behavior

- ✓ Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.
- ✓ Telephonic conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the **physicality** of the virtual world, outpaced only by the exponential growth in the number of users.
- ✓ No other method of communication converges audio, video, and data entities so effectively.
- ✓ Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone.
- ✓ In fact, the two created the **Electronic Frontier Foundation** (EFF) offering to —fund, conduct, and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional.
- ✓ While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through suburbanization. Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the

concentration of the urban population, the **Information** or **Digital Revolution** has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyberprotection even as they add additional doorlocks and alarm systems to insulate themselves from physical attacks.

Clarification of Terms

- ✓ Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon.
- ✓ For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. **Computer crime** has been traditionally defined as any criminal act committed via computer. **Computer-related crime** has been defined as any criminal act in which a computer is involved, even peripherally.
- ✓ **Cybercrime** has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, **digital crime,** a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, *digital crime* may be characterized as any of the three depending on case characteristics.
- ✓ C*ybercrime* will only be used to describe that criminal activity which has been facilitated via the Internet.
- ✓ Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality.

- ✓ For clarification purposes, **computer forensic science, computer forensics, and digital forensics** may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.