1.2. Traditional problems associated with Computer Crime

The physical environment that breeds computer crime is far different from traditional venues. In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents. The lack of physical boundaries and the removal of traditional jurisdictional demarcations allow perpetrators to commit multinational crime with little fear (or potential) of judicial sanctions. For the first time, criminals can cross international boundaries without the use of passports or official documentation. Whereas traditional criminal activity required the physical presence of the perpetrators, cybercrime is facilitated by international connections that enable individuals to commit criminal activity in England while sitting in their offices in Alabama. In addition, electronic crime does not require an extensive array of equipment or tools.

Perceived Insignificance, Stereotypes, and Incompetence

- Investigators and administrators have displayed great reluctance to pursue computer criminals.
- A lack of knowledge coupled with general apathy toward cyber criminality has resulted in an atmosphere of indifference.
- Many stereotype computer criminals as nonthreatening, socially challenged individuals (i.e., nerds or geeks) and fail to see the insidious nature of computer crime;
- In addition, those administrators and investigators who grudgingly admit the presence and danger of electronic crime tend to concentrate exclusively on child pornography, overlooking motivations and criminal behaviors apart from sexual gratification.
- Even in situations where law enforcement authorities recognize the insidious nature of computer or cybercrime, many do not perceive themselves or others in their department to be competent to investigate such criminal activity.

Prosecutorial Reluctance

- As media focus has increasingly highlighted the dangers of cyberspace, including those involving cyber bullying and child exploitation, public awareness has heightened an urgency to protect children's virtual playgrounds.
- In response, federal and state resources have often been allocated to fund specialized units to investigate and prosecute those offenses which affect the safety of American children.
- For example, the Federal Bureau of Investigation maintains a partnership with the Child Exploitation and Obscenity Section of the Department of Justice.
- This organization is composed of attorneys and computer forensic specialists who provide expertise to U.S. Attorney's Offices on crimes against children cases.

Lack of Reporting

- The number of reported incidents handled by Carnegie-Mellon University's Computer Emergency Response Team (CERT) has increased threefold, from 24,097 in 2006 to 72,065 in 2008.13 In their annual survey, *CSO Magazine* (in conjunction with the U.S. Secret Service; CERT, and Deloitte) reported that 58 percent of the organizations surveyed perceived themselves to be more prepared to prevent, detect, respond to, or recover from a cybercrime incident compared to the previous year.
- However, only 56 percent of respondents actually had a plan for reporting and responding to a crime.14 In 2011, it was reported that over 75 percent of all insider intrusions were handled internally without notification of authorities.
- Underreporting on the part of businesses and corporations may be attributed to a variety of reasons, but perhaps the most common are exposure to financial losses, data breach liabilities, damage to brand, regulatory issues, and loss of consumer confidence.
- Contemporary society, characterized by increased reliance on paperless transactions, demands assurances that the company's infrastructure is invulnerable and that confidential information remains inviolate.

Lack of Resources

- Computer intrusions have proven to be problematic within the corporate world, such institutions' unwillingness or inability to effectively communicate with judicial authorities has led to an increase in computer crime.
- Unfortunately, law enforcement and corporate entities desperately need to cooperate with one another.
- Unlike their civil service counterparts, the business communities have the resources (both financial and legal) necessary to effectively combat computer crimes.
- First, these companies, through their system administrators, have far more leeway in monitoring communications and system activities, and they have the ability to establish policies which enable wide-scale oversight.

Jurisprudential Inconsistency

- Unfortunately, the Supreme Court has remained resolutely averse to deciding matters of law in the newly emerging sphere of cyberspace.
- They have virtually denied cert on every computer privacy case to which individuals have appealed and have refused to determine appropriate levels of Fourth Amendment protections of individuals and computer equipment.
- This hesitation has become even more pronounced with the emergence of wireless communications, social networking sites, and smart phones.
- As such, obvious demarcations of perception, application, and enforcement of computer crime laws vary widely across the country, and a standard of behavior in one jurisdiction may supersede or even negate legal standards in another.
- Traditionally, trial and appellate courts evaluated the constitutionality of computer crime statutes, searches, and investigations through the lens of the First and Fourth Amendment.
- Evaluating appropriate boundaries for free speech and establishing standards of reasonableness have varied across state and federal rulings, and an inconsistent patchwork of guidelines has resulted.