Chapter I
Cybercrime, Cybersecurity, and Financial Institutions Worldwide

Pauline C. Reich
Waseda University, Japan

ABSTRACT

While the benefits of the Internet and other forms of computer networks are streamlining financial institutions, the same institutions are often among the first institutions to be affected by Cybercrime and Cybersecurity issues due to the financial incentives as well as their strategic place in each nation’s infrastructure and economy. We must look not only at the efficiency, but also at the negative aspects of the use of technology by financial institutions. Consumers as well as businesses must be well informed about conducting transactions in the safest manner possible. The nature of the Internet is cross-border, and thus Cybercrime and Internet Security issues involving financial institutions should be made known by international organizations, regional organizations, and when there have been cross-border law enforcement collaborations in investigations, extraditions, and so forth. At present, due to the fact that law is generally written at the national (or even state level, as is the case of Identity Theft law in the U.S.), there is a need for reporting of cross-border cases in the literature if such data can be obtained from law enforcement officials by scholars.

INTRODUCTION

These days, financial institutions in developed and many developing countries worldwide have adopted use of the Internet and computers in their transactions. Unfortunately, criminal elements are often one step ahead of legitimate businesses and consumers in finding ways to commit cybercrimes.

According to a recent report from London:

There is an issue of under reporting across the UK. A U.S. survey identified the global cost of e-crime as £1 trillion annually. Lloyds of London estimated that the ‘I Love You’ virus cost the global economy $10 billion. A recent report by the DTI/PricewaterhouseCoopers (PWC) indicated that 84% of large UK businesses had...
Cybercrime, Cybersecurity, and Financial Institutions Worldwide

a malicious security incident last year and that 21% of respondents to a Government survey felt ‘at risk’ to e-crime whereas only 16% worried more about a burglary. It is widely recognized that e-crime is the most rapidly expanding form of criminality, encompassing both new criminal offences in relation to computers (viruses and hacking, etc.) and ‘old’ crimes (fraud, harassment, etc.), committed using digital or computer technology. The Met [London Metropolitan Police] is currently conducting a review of its approach to e-crime. A review of all MPS high-tech assets and external relationships has been conducted to identify areas for improvement or where gaps exist that require addressing. The report identified digital forensics as the area most in need of investment in the near future. With increasing utilisation of digital technology, the demand for associated forensic services is likely to increase by 30-40% over 2006/2007. There is a need to plan for future demand, in order to prioritize expenditure on the increasing costs of outsourcing. (OUT-LAW, 2007b)

Definitions of Cybercrime and Cybersecurity

There is no exact definition of “Cybercrime.” It varies from country to country. It may be called “computer crime” or be referred to by other titles in the legislation. Some countries are able to use existing laws to apply to crimes against computers and networks, for example, through the adoption of amendments to their Criminal Laws. Other countries have adopted completely new laws to address the acts we may consider cybercrimes, for example, the Republic of Korea, and also apply parts of traditional laws. Still other countries have no laws to address such acts that are considered crimes elsewhere.

Since there are no consistent definitions of the terms “Cybercrime” or “Cybersecurity,” the same actions may be characterized in various terms, for example, “computer crime,” “computer intrusion,” “Internet security,” “network intrusion,” and so forth, in laws and policies of various nations and international organizations.

Despite the lack of consistent definitions, here are a few definitions from various places:

Computer crimes—also called:

1. **Computer-related crime**: The use of a computer is integral to committing the offense; examples are offenses such as computer-related forgery (where false data are put forward as authentic) and computer-related fraud (the fraudulent interference with or manipulation of data to cause property loss)

2. **Computer crime**: A general label for offenses in which a computer is the object or the offense or the tool for its commission

3. **Internet crime**: Crimes in which the use of the Internet is a key feature and includes content-related offenses such as possession of child pornography, or in some countries, the dissemination of hate or racist material

4. **E-crime**: A general label for offenses committed using an electronic data storage or communications device (Australian Institute of Criminology, 2005)

Cybercrime is defined both in statutes adopted by countries and economies, and at times at state or commonwealth levels, but not in the Council of Europe Convention on Cybercrime, which, as has been pointed out by commentators, has a broader meaning at the international level. It is then:

an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses, and copyright offenses. This wide definition of Cybercrime overlaps in part with general offense categories that need not be ICT-dependent, such as white-collar crime and economic crime. (Australian Institute of Criminology, 2005).
Related Content

Regulating Mobile Services: An Institution-Based View
[www.igi-global.com/chapter/regulating-mobile-services/68553?camid=4v1a](www.igi-global.com/chapter/regulating-mobile-services/68553?camid=4v1a)

After Auction’s Complete: What Will Buyers Do Next? - A Case Study of Feedback Rating at eBay
[www.igi-global.com/article/after-auctions-complete/181748?camid=4v1a](www.igi-global.com/article/after-auctions-complete/181748?camid=4v1a)

Development of a Measurement Instrument for Website Design Utilizing Analytic Hierarchy Process (AHP) Multi-Attribute Decision Modeling
[www.igi-global.com/article/development-of-a-measurement-instrument-for-website-design-utilizing-analytic-hierarchy-process-ahp-multi-attribute-decision-modeling/132696?camid=4v1a](www.igi-global.com/article/development-of-a-measurement-instrument-for-website-design-utilizing-analytic-hierarchy-process-ahp-multi-attribute-decision-modeling/132696?camid=4v1a)

Social Media in Accelerating Mobile Apps
[www.igi-global.com/article/social-media-in-accelerating-mobile-apps/177162?camid=4v1a](www.igi-global.com/article/social-media-in-accelerating-mobile-apps/177162?camid=4v1a)