Cybercrime in the Corporate Sector

Savitha Kesav Jagadeesan
Kochhar & Co
Chennai, India

Introduction

> "It stands to the everlasting credit of science that by acting on the human mind it has overcome man's insecurity before himself and before nature."
>
> — Albert Einstein

Unprecedented growth in computer science and technology has enabled many remarkable discoveries. These new developments have equipped the human race to overcome many earlier impediments and become remarkably more proficient in conducting its numerous activities. At the same time, this new technology and its many innovative uses have been used to perpetrate crimes, some of which are as ingenious as the new discoveries. This chapter examines criminal acts in light of business transactions that are routinely undertaken in today's highly networked environment and the need to address such network crimes.

This chapter begins with a discussion on the paradoxical nature of the Internet as a medium that enables unprecedented business opportunities while also being the largest potential threat to business. After a brief introduction to the concept of cybercrime and its prime targets, this chapter provides an analysis of the insurmountable impact of cybercrime meeting organized crime.

It also explains why the Internet is so attractive to criminals. It identifies discernible trends in the many ways cybercrime exploits businesses — and the heavy negative impact on the business sector — and the measures necessary for business to respond effectively to the growing exploitation of the Internet by organized criminals. The focus of this discussion is on how businesses, big or small, are affected by cybercrime and why regulatory measures are the need of the hour.

The chapter also discusses the response of the international community to this new form of crime, the many national and international challenges to effective policing of cybercrime, and analyses the extent to which the existing laws and organizations are sufficient to address Internet-specific unlawful conduct.

Overview of Cybercrime

Evolution of Internet

The term "networked environment" pertains to the human race being witness to and being part of one of the greatest scientific discoveries of this age: networked computers and the Internet. The first electronic general-purpose computer, the Electronic Numerical Integrator and Computer (ENIC), was built in 1946. This was bound into a network of computers that led to the early origins of the Internet in 1969.

The public was first introduced to the concepts of the Internet when a message was sent over the Advanced Research Projects Agency Network (ARPANET) from computer science Professor Leonard Kleinrock's laboratory at the University of California, Los Angeles, after the second piece of network equipment was installed at Stanford Research Institute in 1969. The ARPANET, in particular, led to the development of protocols for internetworking, in which multiple separate networks could be joined together into a "network of networks".

In 1982, the Internet protocol suite (TCP/IP)[1] was standardized, and, consequently, the concept of a worldwide network of interconnected TCP/IP networks, called the Internet, was introduced.[2] By the 1990s, millions of people were using their computers to "surf the web",[3] and this space came to be referred to as "cyberspace".

"Cyberspace" is a word that began in science-fiction literature in the 1980s, was quickly and widely adopted by computer professionals as well as hobbyists, and became a household term in the 1990s.

1 The Internet protocol suite is the networking model and a set of communications protocols used for the Internet and similar networks. It provides end-to-end connectivity, specifying how data should be formatted, addressed, transmitted, routed, and received at the destination. Additional information available on *Wikipedia* at http://en.wikipedia.org/wiki/Internet_protocol_suite.

2 Additional information available on *Wikipedia* at http://en.wikipedia.org/wiki/History_of_the_Internet.

3 The term "surf", used in this context, refers to the practice of browsing through websites: jumping from one link to another, following items of interest, watching videos, and viewing a range of content across different websites.

During this period, the uses of the Internet, networking, and digital communication were all growing dramatically, and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging.[4]

Cyberspace has become an important asset for economic growth. In 2012, approximately 2,100,000,000 people worldwide accessed the Internet, which meant that nearly thirty per cent of the global population was active online.[5] Statistics indicate that an average worker spends two-and-a-half hours each day composing emails.[6]

With the advent of mobile telephony, this proliferation of cyberspace has extended to cell phones, and subsequently to smart phones, making the expanse of cyberspace seamless and far-reaching. Within a span of approximately fifty years, computers have created a new space and transformed the way people work, play, and communicate.

Characteristics of Cyberspace

Two of the key characteristics of cyberspace are the vast number of users and the borderless nature of the Internet, where an act in one continent permeates to other distant continents, sometimes within minutes. These characteristics also indicate that business can be conducted faster without physical travel or a physical presence, with quicker responses across vast distances, and possibly have an impact on a global audience.

While this technological advance introduced plentiful benefits to society, the downside was not far behind. The changes created by computing and networking have manifested a new environment in which people increasingly gather in cyberspace to interact socially and commercially,[7] but these interactions also have provided an ideal

4 The origin of the term "cyberspace" is "cybernetics", derived from the Greek *kybernetes* (steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener in his pioneering work in electronic communication and control science; Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation", 63/3 *Western Journal of Communication* (1999), at pp. 382–383.

5 "Pingdom reports in to let us know there are 2.1 billion active web users worldwide", *Inquisitr* (21 January 2012), at http://www.inquisitr.com/184569/pingdom-reports-in-to-let-us-know-there-are-2-1-billion-active-web-users-worldwide/#1feXDwkg8RXyWJIF.99.

6 McKinsey Global Institute Report, "The social economy: Unlocking value and productivity through social technologies" (July 2012), at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy.

7 Decker, "Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime", 81/5 *Southern California Law Review* (2008) 959, at p. 961.

opportune platform for the perpetration of crimes. The characteristics of cyberspace have not only provided a whole new class of targets for crime, but also have led to an increase in the number of cyber-savvy individuals with a ready means to commit crimes that have widespread impact. As one commentator observes:

> "Growth of cyber criminals is occurring on two axes: first, the number of people who are technologically savvy enough to commit cybercrimes is growing exponentially; second, a derivative market in cybercrime appears to be growing as 'enablers' — 'persons who use their technical expertise to create and then sell to others easy-to-use tools' — make it possible for non-technologically savvy people to engage in cybercrime."[8]

The Internet has been compared to an "unsafe highway".[9] This analogy "is an apt reminder of the inherent decentralized and open architecture of the Internet".[10] The omnipresent nature of the Internet makes it an ideal platform for business and social interactions, but also makes it highly vulnerable to those seeking to commit mischief or indulge in gross misuse of web technologies.[11]

Troublemakers in cyberspace seek systems to infiltrate and misuse. Just for the heck of it, or as an intellectual challenge, there are some who try to hack into a computer to launch a worm or virus that could cripple a business organization or even disrupt an entire nation's business for the day.

The need of the hour is for all Internet users — individuals and businesses alike — to gear up to the potential dangers of cyberspace and its ability to cause major security incidents. Developing measures to combat this threat is vitally important, because one thing is for sure: a poorly developed security system is a hopelessly inadequate safeguard against cyber-attacks, while lack of security measures

---

8 Decker, "Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime", 81/5 *Southern California Law Review* (2008) 959, at p. 961, n. 15.

9 Lessig, *The Future of Ideas: the Fate of the Commons in a Connected World* (2002).

10 Broadhurst, "Developments in the global law enforcement of cyber-crime", 29/2 *Policing: An International Journal of Police Strategies and Management* (2006) 408, at p. 14. The article is available at http://eprints.qut.edu.au/3769/1/3769_1.pdf.

11 Yang and Hoffstadt, "Countering the Cyber-Crime Threat", 43 *Am. Crim. L. Rev.* (2006) 201, at p. 203.

poses a severe threat to the survivability and the profitability of the company's business operations.

Definitions of Cybercrime

The ability to cause harm to systems, networks, and users is only a manner of reworking traditional crimes and misdemeanors by using Internet technologies and the setting of today's digital age. Actions that perpetrate crimes in cyberspace are termed cybercrime.

Cybercrime is no longer confined to sporadic incidents of unauthorized access or hacking events. It has continually redefined itself to manifest itself in newer forms. In 1983, a group of experts of the Organization for Economic Cooperation and Development (OECD) defined the term "cybercrime" (or "computer-related crime") as "any illegal, unethical, or unauthorized behavior involving automatic data processing and/or transmission of data".[12]

Later studies went even further in developing broader concepts on "data and/or information crime".[13] As increasing incidents of cybercrime took center stage, so did the need to define it in order to regulate it. Hence, many definitions of cybercrime have been coined.

In Australia, for instance, cybercrime has a narrow statutory meaning as used in the Cybercrime Act 2001 (Cwlth), which details offenses against computer data and systems.[14] However, a broad meaning is given to cybercrime at an international level. At the European Council's Convention on Cybercrime,[15] "cybercrime" is used as an umbrella term to refer to an array of criminal activities, including offenses against computer data and systems, computer-related offenses, content offenses, and copyright offenses. Also used are a number of inter-related terms such as "computer crime", "internet crime", "e-crime", and "computer-related crime".

However, the scope of this chapter is to examine cybercrime as simply a new-age crime, a crime that only requires basic technical knowledge and two readily available weapons: a computer and the Internet. Cybercrime includes traditional crimes such as theft

12 Sieber, *The International Handbook on Cyber Crime* (1986), at pp. 1 *et seq*.
13 The problems of definition are discussed in Bloombecker, *Spectacular Computer Crimes* (1990), at pp. 69 *et seq*.
14 Definitions and general information are provided on the website of the Australian Institute of Criminology at http://www.aic.gov.au/crime_types/cybercrime/definitions.html.
15 ETS Number 185 (2001).

("upgraded" for the digital age) or newer crimes such as data diddling, as long as the means used include a computer connected to the Internet.

Recent Statistics on Cybercrime

Numerous individuals and businesses that carry out their activities in cyberspace have been targets of cybercrime. In 2012 alone, 2.1-billion people worldwide accessed the Internet, i.e., 30 per cent of the earth's population. Statistics indicate an average worker spends half of his time on the Internet, two-and-a-half hours spent sending emails. In 2011–2012, an estimated 556,000,000 adults across the world were victims of cybercrime,[16] which indicates a forty-two per cent increase in attacks since 2011.

This makes cybercrime costly. A Poneman Institute study found the average annualized cost of cybercrime for 56 organizations in their study is US $8.9-million per year, with a range of US $1.4-million to US $46-million.[17]

Of these targeted attacks, thirty-one per cent were aimed at businesses. Cyber attacks are becoming commonplace. The Poneman Study found that the subject companies experienced 102 successful attacks per week and 1.8 successful attacks per company per week.[18]

What is even more alarming is the way cybercrime perpetuates itself. Each year, new forms of cybercrime emerge. In 2012, 5,291 new cybercrime vulnerabilities were discovered, and 415 of them were on mobile operating systems.[19] Back in 2005, cybercrimes cost US $14,200,000,000 in damage to businesses worldwide.[20]

---

16 Symantec, *Internet Security Threat Report*, Volume 18, at p. 41 (the report is available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf); Symantec Press Release, "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually" (5 September 2012), at http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02.

17 Ponemon Institute Research Report, *2012 Cost of Cyber Crime Study: United States*.

18 Ponemon Institute Research Report, *2012 Cost of Cyber Crime Study: United States*.

19 Symantec, *Internet Security Threat Report* 2013, Volume 18, at p. 25; Symantec Press Release, "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually" (5 September 2012).

20 Decker, "Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime", 81/5 *Southern California Law Review* (2008) 959, at p. 961, n. 16.

In 2012, the varied forms of cybercrime cost the global economy US $110,000,000,000.[21]

The most costly cyber crimes are those caused by denial of service, malicious insiders, and web-based attacks. Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, application security testing and enterprise governance, and risk management and compliance (GRC) solutions.[22]

Risk Factors and Preventive Measures

Given the alarming rise in incidents of cybercrime and the huge amounts at stake, many have considered doing business over the Internet to be risky. However, this notion has not deterred a vast number of e-businesses from emerging, nor has it put the brakes on the dot-com boom. A host of companies have embraced this new technology to do business in one form or another. In fact, the Internet has become the efficient way to do business in the twenty-first century and is widely used for both business-to-business (B2B) transactions and business-to-consumer (B2C) transactions. The B2B market is predicted to exceed US $5,000,000,000,000 in the early twenty-first century.[23]

Despite this surge in B2B and B2C markets, the vulnerabilities of doing business over the Internet cannot be ignored, as there are risks attached not only to e-businesses, but also to businesses that use the Internet to carry out day-to-day activities. These companies are potentially exposed to serious technological as well as financial risks.

The reasons for this are certain characteristics of cybercrime, such as the ease of access to powerful technology, the anonymity of the criminal, and the fleeting nature of the evidence. These elements,

---

21 Norton, "2012 Cybercrime Report", available at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf. This annual report is based on self-reported experiences of more than 13,000 adults across twenty-four countries, and calculates the direct costs associated with global consumer cybercrime.

22 Ponemon Institute Research Report, *2012 Cost of Cyber Crime Study: United States*.

23 Kratchman, Smith, and Smith, "Perpetration and Prevention of Cyber Crimes", 23/2 *Internal Auditing* (March–April 2008), at pp. 3–12; Kratchman, Smith, and Smith, "Case Studies of Cybercrime and their Impact on Marketing Activity and Shareholder Value", 15/2 *Academy of Marketing Studies Journal* (2011), at pp. 67–81; El Gawady, "The Impact of E-Commerce on Developed and Developing Countries — Case Study: Egypt and United States", at http://www.must.edu.eg/Publications/Businees_Res5.pdf.

which provide armor for a perfect crime, are available to the cybercriminal and ensure that the cybercriminal escapes unharmed.[24]

Given that the use of technology in today's business environment brings new risks to the fore, using old solutions might not be the answer. New risks require new measures. There are unique problems related to digital information and transactions, such as storage and intellectual property issues, that must be considered.[25]

Therefore, although the new technology allows individuals to engage in international business activity as never before, it also expands the scale and scope of the associated risks. Technology tools mean that computing power, connectivity, and speed can spread viruses, compromise systems, and compound errors in seconds, potentially affecting interconnected parties, increasing business costs to rectify such mishaps, and hitting a larger target than even envisaged. Cybercriminals never stop devising new techniques. New tools mean new vulnerabilities, and the preventive measures to overcome these vulnerabilities fail to keep pace with cybercriminals' ability to devise new techniques.

The reporting of this type of crime is often inadequate. This is partly because some crimes go unnoticed and partly because the victims (economic operators and companies) are wary about reporting cybercrimes for fear of getting a bad reputation and of their future business prospects being affected by public exposure of their vulnerabilities.

Companies must factor these risks into their business risk margins and take abundant precautions to fight against these vulnerabilities.[26] Any form of crime is socially harmful; combating cybercrime is not just a matter of creating security measures through the medium itself, but also requires the establishment of preventive measures in the legal sphere to address the situation.

Business Impact of Cybercrime

International Character of Cybercrime

Cybercrime is a global phenomenon. The international character of cybercrime compounds the difficulty of predicting and safeguarding

24 Kratchman, Smith, and Smith, "Case Studies of Cybercrime and their Impact on Marketing Activity and Shareholder Value" (2011), at pp. 67–81.

25 Kratchman, Smith, and Smith, "Case Studies of Cybercrime and their Impact on Marketing Activity and Shareholder Value" (2011), at pp. 67–81.

26 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002).

against it. Emerging countries such as India are especially at risk, as cyber-security is still relatively less advanced, allowing cyber-criminals located anywhere in the world to easily access confidential government information.

In a recent report titled "India Risk Survey 2012", released by the Federation of Indian Chambers of Commerce and Industry (FICCI),[27] "Information and Cyber Insecurity" was listed as a top risk to the government and to business establishments alike, ahead of traditional risks such as terrorism and natural hazards. The same findings may well be applicable to many developed countries as well.

This risk is mainly because of the characteristic features of cybercrime, such as its transnational nature. As cybercrimes make geographical boundaries insignificant, combating cybercrime calls for international harmonization of laws and crossborder regulation, along with mandatory global prosecution procedures;[28] however, such is not the case, nor is it feasible in the near future. Regulation is usually fragmented, and countries differ on definitions of cybercrime, leave alone the types of crime and punishment.

Cybercriminals exploit this situation by coming up with new tools and discovering new vulnerabilities to attack targets. Moreover, the targets of cybercrime have evolved from personal targets to financially sound targets such as business enterprises that can be held to ransom and made to pay big monies. As a recent report observes, this is primarily because:

> ". . . many business organizations are leaving themselves vulnerable to cybercrime based on a false sense of security — perhaps even complacency — driven by non-agile security tools and processes. Many are failing to recognize cybercrimes in their [information technology] environments and misallocating limited resources to lesser threats. For example, many organizations focus heavily on foiling hackers and blocking pornography, leaving major cybercrimes undetected and unaddressed. This has generated significant risk exposure, including exposure to financial losses, regulatory

27 The report is available on the FICCI website at http://www.ficci.com/SEDocument/20186/IndiaRiskSurvey2012.pdf.

28 Talwar, "Computer-Related Crime", Inaugural address by the Deputy Governor of the Reserve Bank of India at the National Seminar on Computer-Related Crime (New Delhi, 24 February 1999), *CBI Bulletin* (February 1999), at p. 6-6.

issues, data breach liabilities, damage to brand, and loss of client and public confidence."[29]

Most Common Threats to Businesses

A recent collective analysis distributed at the initiative of the French National Gendarmerie has identified the forms of cybercrime that are most likely to target businesses.[30] These threats are:

(1) Denial of service/blocked access/paralysis/unavailability;
(2) Loss or theft of strategic data/unfair competition;
(3) Misinformation/defamation/damaged image;
(4) Intrusions/economic fraud/embezzlement;
(5) Cyber-extortion/demand for ransom;
(6) Theft of personal data managed by a business;
(7) Threats to vital infrastructures;
(8) Propagation of malware through social networks/web navigation;
(9) Misuse; and
(10) Falsification of documents.

In a denial-of-service attack, a computer or network resource is made unavailable to its intended users. Most often, it involves flooding a computer or a server with more requests than it can handle, causing the server to crash.[31] This form of cybercrime usually targets high-traffic websites such as banks and credit card payment gateways.

Apart from denial-of-service attacks, which have led to widespread panic in companies, there are the pervasive virus/worm attacks, such as the notorious ILoveYou virus (popularly referred to as the Love Bug virus) that spread widespread mayhem in the 1990s. Computer viruses and malware are here to stay and are often used more for mischief and disruption rather than for financial gain.

These small malicious software programs are designed to quickly spread from one computer to another and to interfere with computer operations, and subsequently corrupt or delete data on the victim's

29 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat" (January 2010), at p. 3. The report is available at http://www.deloitte.com/assets/dcom-unitedstates/local%20assets/documents/aers/us_aers_deloitte%20cyber%20crime%20pov%20jan252010.pdf.

30 *Prospective Analysis on Trends in Cybercrime from 2011 to 2020* (2011), at p. 14. The analysis is available on the McAffee website at http://www.mcafee.com/in/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf.

31 India Forensic, *Full Guide on Cyber Crimes in India*, at http://www.indiaforensic.com/compcrime1.htm.

computer. They not only cause mayhem, but also render systems ineffective. Restoring systems to their former state has heavy financial consequences.[32] A targeted company's productivity also is negatively impacted, as this form of cybercrime seriously impairs users' productive time. Slower computers, inaccessible servers, and jammed networks affect the overall productivity of individual users and companies.

Typical cyber-exhortion schemes include hacking into a computer network, locking out the company and its customers from accessing the company's information system, and gaining access to sensitive data. The cybercriminal may hold the company's data ransom, may threaten to release sensitive protected data (such as credit card numbers and medical histories), or may threaten to sell a company's corporate secrets if his demands are not met.

Misuse refers to misuse of information technology and digital devices to gain unauthorized access to a computer program or computer data with the intention of committing or facilitating the commission of an offense or the unauthorized modification of computer data with criminal intent.

Other Cybercrimes

The most common forms of cybercrimes are essentially traditional in nature; the only difference is that the medium to commit the crimes has changed. Apart from the most common threats to business, there are certain new forms of cybercrime that require attention, especially considering that the public sector is as exposed as the private sector.

One such example is the Ukrainian cybercriminals who stole US $415,000 from the United States by means of unauthorized wire transfers from a Kentucky county bank.[33] The criminals were aided by more than two dozen fellow conspirators in the United States. The act was carried out by a customized version of a "keystroke logging Trojan" that promptly sent stolen credentials to the attackers by instant messenger. This malware also enabled the attackers to log into the victim's bank account by using the victim's own Internet connection. This incident clearly exposed the vulnerability of the systems in use.

---

32 India Forensic, *Full Guide on Cyber Crimes in India*.

33 Krebs, "PC Invader Costs KY County $415,000", *The Washington Post* (2 July 2009), at http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

Data diddling is another form of cybercrime, which involves changing data prior or during input into a computer and then changing it back after the processing has been completed. By using this technique, cybercriminals can manipulate data without either the crime or the criminal being identified. Information is changed from the way it should be entered by a person keying in the data, by a virus that changes data or the application, or by any other person involved in the process of having information stored in a computer file.

The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data. "Botnets" (a term derived from the words "robot" and "network") consist of a network of interconnected, remote-controlled computers generally infected with malicious software that turns the infected systems into so-called "bots", "robots", or "zombies".

The cyber infection is difficult to detect. It can be used for a number of actions, including DDoS attacks, sending spam, stealing personal information, hosting malicious sites, and delivering "payloads" of other malicious software; thus, they are effective cybercrime tool.

The NDMC Electricity Billing Fraud case that took place in 1996 is a typical example of data diddling. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council (NDMC). Collection of money, computerized accounting, record maintenance, and remittance in the bank were exclusively left to a private contractor who was a computer professional. The contractor misappropriated a huge amount of funds by manipulating data files to show fewer receipts and bank remittances.[34]

Yet another form of cybercrime that has the potential to exploit its targets financially is the salami attack, where small attacks that can go undetected but add up to a major attack. For instance, a bank employee inserts a program into the bank's servers that deducts negligible amounts of money (say, INR 2 a month) from the account of every customer. Account holders will probably fail to notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month. Salami attacks have been covered under Section 66 of the Indian Information Technology Act and Section 477A of the Indian Penal Code in relation to falsification of accounts.

These forms of cybercrime are leading to new emerging forms that seem to be designed to beat the very system that seeks to regulate such

34 India Forensic, *Full Guide on Cyber Crimes in India*.

crimes. One such example has been the recent Advanced Persistent Threat (APT) phenomenon, which hit the headlines when it was perceived that the Chinese government was training and funding hackers to attack businesses and foreign governments.

> "The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence-gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target."[35]

Economic Implications

Both the typical forms of cybercrime and other cybercrimes have a major impact on businesses. Take the example of the famous worm that was launched by Robert Morris in 1988. The Internet was still at its nascent stage when this worm affected thousands of computers, and it took a team of experts almost three days to get rid of the worm, during which time many of the computers had to be disconnected from the network. Today, one such attack can render several companies defenseless, facing huge financial losses and loss of reputation.

Loss of reputation can even result from fraudulent e-mail. This occurred in the Bank NSP case, where a management trainee of the bank was engaged to be married to a young man who worked at another company. She exchanged several e-mails with her fiancé, using the bank's computers. However, when the engagement was called off, the trainee created fraudulent email IDs, such as "Indianbarassociations", and sent e-mails to her ex-fiancé's foreign clients through the bank's computers. The young man's company lost a large number of clients and took the bank to court. The bank was held liable for the e-mails sent using the bank's system.

From a corporate perspective, the most critical area expected to be addressed is that of confidential information, particularly in crossborder communications. The protection of privacy and data can be derived from various laws pertaining to information technology,

35 Wikipedia at http://en.wikipedia.org/wiki/Advanced_persistent_threat.

intellectual property, and contractual obligations. The paramount legislative act in India relating to information technology and cyber crime is the Information Technology Act of 2000. The Information Technology Act provides for safeguard against breaches in relation to data from computer systems.

The Act contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein. The Act provides for personal liability for illegal or unauthorized use of computers, computer systems and data stored therein. For example, Section 43A provides penalties for negligent handling of sensitive personal data resulting in wrongful loss or gain. Section 72A of the Information Technology Act provides for penalty for breach of confidentiality and privacy under a lawful contract by any person who, while performing services under a lawful contract, has secured access to any record or document containing personal information about another person and knowingly causes such information to be disclosed to any other person.

The Information Technology Data Rules are an extension of Section 43A of the Information Technology Act. The Information Technology Data Rules provide for the security practices to be adhered to by body corporate while dealing with sensitive personal data. "Personal Information" includes passwords, financial information, physical, physiological and mental health condition, sexual orientation, and "other information available or likely to be available with a body corporate, capable of identifying a person".

The Information Technology Data Rules also specify that a body corporate handling such sensitive data should provide a privacy policy for handling or dealing in personal information. In addition, a body corporate handling sensitive information should adhere to reasonable security practices and procedures. One example mentioned under the Information Technology Data Rules is the International Standard IS/ISO/IEC 27001 on Information Technology — Security Techniques — Information Security Management System — Requirements.

Under Indian law, there is no defined law for confidentiality. The mention of confidentiality under any law in India comes in the Information Technology Act under two Sections that deal more with providing the punishment for such disclosure than defining the principles of confidentiality. Interestingly, the first Section, being Section 72, is limited in scope as regards its applicability. Section 72 of the Information Technology Act provides for penalty for breach of

confidentiality and privacy with regard to securing access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned; however, the application of this Section is restricted to a person who has sought access to the information by the powers vested in him under the Information Technology Act.

This basically means that Section 72 is more applicable to the inspector in charge of the investigation who has sought access to information. The punishment is for a maximum term of two years or fine up to 1 lakh of rupees. Therefore, under Indian law as confidentiality principles are enunciated, these are protected and taken care of under contract law. Stringent principles of confidentiality are provided under contract law and disruption of the same or disclosure of information when bound by confidentiality may lead to termination of the contract and/or damages for breach of contract.

However, it is Section 72A of the Information Technology Act that states that a person, including an intermediary (as already-defined BPOs also are intermediaries), who, while performing services under a lawful contract, has personal information about another person and disclosure happens through a breach of contract or wilfully, can be prosecuted and punished under the Information Technology Act. In Section 72A, the punishment is more stringent and can lead to imprisonment of three years, or with fine that may extend to 5 lakh of rupees, or both.

Of course, the confidentiality clauses are made subject to the condition that in the event the information is sort due to a legal investigation or as required by law such disclosure of information is permissible.

If the legal authority, such as the Central Government of India or any State Government in India, believes the information with a person is of the nature required by them, irrespective of confidentiality principles, such information would required to be disclosed. However, a lawful process would have to be followed as indicated above.

The remedy at this point is incorporating data protection terms under letters of engagement, seeking enforcement on breach, or seeking action under the Trade Marks Act or the Indian Penal Code, which are inadequate substitutes for a justifiable statutory regime. The protection of confidential data falls distressingly short of expectations, and the damages are hopelessly inadequate, particularly as these breaches often occur in crossborder situations, and require lengthy strong-arm tactics to be combated effectively.

According to the UNDOP interviews of law enforcement agencies, the confidentiality, integrity, and accessibility of computer systems, such as "illegal access to a computer system", make up between one-third and 10 per cent of acts, depending upon the region. Such actions are integral to a range of cybercrimes, and it may be that differing capacities of countries to identify and to prosecute these (more technical) offenses affects their perceived prevalence across regions.[36]

The many forms of cyber-attacks and security breaches only reflect that cybercrimes are increasing in frequency and sophistication, with discovery usually occurring only after the fact, if at all. These trends are aptly summarized by Deloitte in a white paper on cybercrime:

> "Cyber criminals are targeting organizations and individuals with malware and anonymization techniques that can evade current security controls.
>
> Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense and are rapidly becoming obsolete — for instance, cyber criminals now use encryption technology to avoid detection.
>
> Cyber criminals are leveraging innovation at a pace which many target organizations and security vendors cannot possibly match.
>
> Effective deterrents to cybercrime are not known, available, or accessible to many practitioners, many of whom underestimate the scope and severity of the problem."[37]

What is even more disturbing is that the ground-breaking technologies painstakingly discovered by dedicated innovators are being ruthlessly exploited by astute cybercriminals to commit serious and malicious crimes. As the Deloitte white paper observes:

> "Cyber criminals now operate undetected within the very 'walls' erected to keep hackers out. Their technologies include rogue devices plugged into corporate networks, polymorphic malware, and key-loggers that capture credentials and give

36 United Nations Office On Drugs And Crime Vienna, *Comprehensive Study on Cybercrime*, February 2013.

37 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat" (January 2010), at p. 5.

> criminals privileged access while evading detection. These technologies are a reason why so many breaches are detected only after significant exposure has occurred."[38]

One such segment of criminals that has used this new form of crime in a systematic and organized manner is, of course, organized crime syndicates. The next section takes a look at the potential impact on businesses when cybercrime is used as the new tool of organized crime.

Business Impact of Organized Cybercrime

The capabilities and opportunities provided by the Internet have transformed the way people do business; at the same time, the Internet provides the ideal medium and ample scope for criminal exploitation. The dark side of the Internet involves not only fraud and theft, but has extended its scope to organized crime "that has pervaded cyberspace, adding cybercrime to its portfolio of 'businesses'".[39] As one commentator observes:

> "In the virtual world, as in the real world, most criminal activities are initiated by individuals or small groups, which can be termed 'disorganized crime'. Yet, there is growing evidence that organized crime groups or mafias are exploiting the new opportunities offered by the Internet."[40]

Although cybercrime is largely initiated by individuals, it also is increasingly likely to be perpetrated in organized crime circles, until there is ultimately an overlap. In fact, individual criminals are likely to morph into organized criminals. The skills of individual criminals are used by traditional organized crime entities specifically for committing cybercrimes. This new phenomenon raises concerns that urgently need to be recognized by businesses and governments "as an emerging and very serious threat to cyber security".[41]

38 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat" (January 2010), at p. 6.
39 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat" (January 2010), at p. 6.
40 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 1.
41 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 1.

According to a United Nations Office on Drugs and Crime study on cybercrime, upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity. This is established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and "cashing out" of financial information.

An interesting observation is that they also found during the course of their study that cybercrime perpetrators no longer require complex skills or techniques.[42]

Take the example of a Russian group that attacked one of the best known banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer more than US $10,000,000 to foreign accounts.[43] A number of the perpetrators were arrested, and some of them possessed fake Greek and Israeli passports. The high quality of the forging could have been produced only in Russia, by members of the former Russian secret service, the KGB.

A recent example is the cyber-heist on a fuel distribution firm in North Carolina, where the firm lost more than US $800,000. Had the victim company or its bank detected the unauthorized activity sooner, the loss would have been significantly lower.

However, both the company and its bank failed to notice the attackers' comings and goings for five days. Organized cyberthieves began siphoning cash in sub-US $5,000 and sub-US $10,000 chunks to approximately a dozen "money mules" — people hired through work-at-home job scams to help the crooks launder the stolen money.[44]

These examples clearly reflect how cybercrime has now evolved into "organized cybercrime", with far-reaching effects and insurmountable costs. Today's cyber criminals have evolved to make their crimes more profitable, they have specialities, they are masters in their chosen field, they have networks, and they organize their crimes. In this scenario, it is imperative that businesses recognize this very serious threat.

---

42 United Nations Office on Drugs and Crime Vienna, *Comprehensive Study on Cybercrime,* February 2013.

43 *Datenschutz-Berater*, Volume 10 (1995), at p. 23; Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 6.

44 Krebs, "NC Fuel Distributor Hit by $800,000 Cyberheist", *Krebs on Security* (23 May 2013), at http://krebsonsecurity.com/category/smallbizvictims/.

Given that organized crime has traditionally selected particular industries as targets for infiltration, it is essential that the corporate sector consider both general cybercrime and large-scale organized cybercrime when formulating its policies on risk management and risk margins.

The primary objective of organized crime is to generate a profit; as such, it is a business that is operated by criminal means. Criminal organizations are always on the lookout for new means and opportunities to perpetrate criminal exploitation. The Internet and the ever-increasing growth of electronic commerce provide organized crime groups with tremendous new opportunities.[45] The FBI has noted three primary categories of cyber threat actors:

> "[1] Organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks; [2] state sponsors-foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defence contractors; and [3] increasingly there are terrorist groups who want to impact this country the same way they did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life."[46]

Another reason why cyberspace is a potentially welcome area for organized criminals is because organized crime groups often operate out of safe havens. The transnational nature of the Internet therefore perfectly fits their *modus operandi*. There are no borders defining the commitment of cybercrimes, which makes policing problematic and makes "large-scale investigations slow and tedious at best, and impossible at worst".[47]

This was one of the lessons of the Love Bug virus. Although the virus spread worldwide and cost businesses billions of dollars, when FBI agents succeeded in identifying the perpetrator, a student in the

---

45 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 1.

46 Federal Bureau of Investigation, *The Cyber Threat: Part 1: On the Front Lines With Shawn Henry*, 27 March 2012, http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712

47 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 2.

Philippines, they also found that there were no laws under which he could be prosecuted.

Although a growing number of countries have been enacting legal and regulatory measures to combat cybercrime, there are bound to be "jurisdictional voids from which criminals and intruders can operate with impunity".[48] Cyberspace provides ample scope for exploitation by criminals precisely because it provides them with the best possible escape tool — anonymity.

Today, organized crime groups use the Internet for communications (usually encrypted) and for any other nefarious purposes that they identify as gainful and profitable for their "business". Indeed, organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as for its many other opportunities for illegal activity. The implications are far-reaching and require a response not only from governments, but also from businesses, which can all too easily become the targets of organized cybercrime.

Measures to Combat Cybercrime

Addressing Major Vulnerabilities

Business Losses

Cybercrime and cybercrimes committed by organized crime groups have far-reaching implications for business. They forebode grim consequences, such as business disruption and loss of sensitive information, including intellectual property and trade secrets. This is followed by loss of reputation and brand name, along with losses caused due to damaged equipment.

The primary goal for cybercriminals is financial fraud and/or access to the company's financial records. Only a miniscule percentage of attacks is "motivated by political or ideological agendas".[49] As a recent report observes:

> "Organizations in Germany and the US experience the highest average rate of weekly attacks, 82 and 79, respectively. Brazil

48 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 4.

49 Ponemon Institute, "The Impact of Cybercrime on Business — Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong, and Brazil" (May 2012), at p. 2. The report is available at http://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf.

> and Hong Kong have the lowest frequency, on average 47 and 54 per week, respectively. On average, respondents believe 17 per cent of machines and mobile devices within their organizations have been infected by an act of cybercrime.[50]
>
> In the aftermath of one cybercrime attack, the cost to investigate, recover brand and reputation, and invest in technologies ranges from an average high of [US] $298,359 . . . for German organizations to an average low of [US] $106,904 . . . for Brazilian organizations."[51]

Insider Vulnerability

Insider vulnerability is a serious issue. In most cases, the attackers are disgruntled ex-employees or employees of the company. There are often very few controls imposed by companies, the most common deterrents being a non-disclosure agreement and a letter of engagement that binds the employees. This does little to stop a disgruntled employee from retaliating by exposing the cyber vulnerabilities of their company. In the event that this does happen, the damage is already done by the time an investigation takes place.

In one of the first prosecutions of its type, the former Chief Network Administrator of Omega Engineering Corporation was convicted in the New Jersey Federal District Court in May 2000 for planting a computer "time bomb" that cost the company more than US $10,000,000. Demoted prior to being fired in 1996, the disgruntled employee stayed after regular business hours, programming and testing commands that eventually would permanently wipe out all the design and production programs vital to Omega's New Jersey manufacturing operations. The "bomb" had been designed to activate automatically if a countermanding command was not received.[52]

Traditionally, internal attacks account for approximately eighty-five per cent of all attempted intrusions, while the remaining fifteen per cent come from external sources. According to survey results

---

50 Ponemon Institute, "The Impact of Cybercrime on Business — Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong, and Brazil" (May 2012), at p. 1.

51 Ponemon Institute, "The Impact of Cybercrime on Business — Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong, and Brazil" (May 2012), at p. 2.

52 Gaudin, "The Omega files: A true story", *CNN.com* (27 June 2000), at http://edition.cnn.com/2000/TECH/computing/06/27/omega.files.idg/.

released in July 1998 by Internet Security Systems, sixty-one per cent of corporate respondents suffered computer system attacks originating from inside the organization, and forty-five per cent of those attacks resulted in losses of more than US $200,000. According to a global economic crime survey conducted by PricewaterhouseCoopers (PWC) in 2011,[53] fifty-six per cent of the participants identified "internal fraudsters" as the largest perpetrators of cybercrime across all business sectors surveyed.[54]

Between 2009 and 2012, insider attacks resulted in losses that had increased by US $60,000 over three years.[55] It is therefore imperative that before employees are hired, they are thoroughly screened and their references carefully checked. Equal attention should be paid to the each employee's authorized levels of security use and any unauthorized use should immediately be investigated.

Escalating Impact of Small Events

Whether it be the "Melissa" virus or the "I love you" virus, a single strike makes a global impact costing companies and governments millions of dollars.

The simple prank of putting up a pornographic website along with a corporate site might seem a minor event, but has a large-scale impact, considering the vast global reach of the Internet. Within seconds, the reputation of the affected company becomes questionable, especially if it is a company in the information technology sector.

According to a recent survey, the average time it takes to recover from a cyber-attack is twenty-four days, at an average cost of US $24,475 per day, amounting to an overall cost of US $591,780 over the twenty-four-day period.[56]

Increasingly, small to medium-sized businesses are finding themselves on the frontline of these targeted attacks, as they have fewer resources to combat the threat. A successful attack on this business segment may initiate attacks against a larger organization, such as an

53 The survey, which included 3,877 respondents from organizations in seventy-eight countries, is available at https://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf.

54 PWC, "Cybercrime: Protecting against the growing threat — Global Economic Crime Survey" (November 2011), at p. 22.

55 Ponemon Institute, "2012 Cost of Cyber Crime Study: United States" (October 2012), at p. 12.

56 Ponemon Institute, "2012 Cost of Cyber Crime Study: United States" (October 2012), at p. 13.

attack on a supplier leading to a more serious attack on the supplier's corporate clients.

Malware such as Stuxnet in 2010, Duqu in 2011, Flamer and DistTrack in 2012, and FBI and Firefox Redirect in 2013 show increasing levels of sophistication and danger, with the potential for severe damage being correspondingly higher. For example, the malware used in the Shamoon attacks on a Saudi oil firm had the ability to erase hard drives.[57]

Therefore, cybercrime cannot have a minimal impact. One of the key combative measures is for companies to recognize the far-reaching effects and acknowledge that they may well be targets, and then establishing the necessary combative measures. Symantec has recommended:

> ". . . multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network. Endpoints must be secured by more than signature based antivirus technology."[58]

Jurisdictional Differences in Legislative and Punitive Measures

There are divergences in national cybercrime laws, due to legal and constitutional differences. The area of penalties highlights this issue as seen in the I-love-you case. The Philippines student who released the Love Bug virus could not be prosecuted because the Philippines did not have a law in place for the crime he committed.

In India, cybercrime is punished with minimum imprisonment of three months and paltry fines and maximum imprisonment of up to seven years. The United States imposes sanctions with imprisonment even amounting to thirty-five years; many consider that the punishment far surpasses the crime.

The jurisdictional differences in punitive measures make it possible for a cybercriminal to visualize the consequences of his crime according to jurisdiction and use a country with the lowest levels of security,

---

57 "The Shamoon Attacks", *Symantec Official Blog* (16 August 2012), at http://www.symantec.com/connect/blogs/shamoon-attacks.

58 Symantec, *Internet Security Threat Report 2013*, Volume 18, at p. 22.

in terms of legal reprisal, as the domain to launch a cyber-attack. This major challenge to successful prosecution brings to the fore the whole argument on jurisdiction and the boundaryless nature of crime. The harmonization of cybercrime laws is hence essential for elimination of safe havens and swift prosecution as well as evidence collection.

Unethical Hacking

The corporate sector needs to recognize that the problem threatening it is cybercrime, not merely hacking.[59] As one commentator explains:

> "Disruption, denial of service, and website defacements will continue to be problems, but exploitation of access to information systems for profit is likely to become more pervasive. The trend toward accessing business systems, highlighting security holes, and offering these services for a significant fee, for example, is a thinly veiled form of extortion."[60]

Organized groups, such as the team behind the Elderwood attacks that target high-profile companies, have worked to discover new weaknesses in everyday software such as web browsers and browser plug-ins. When one vulnerability becomes public, they are able to immediately deploy a new one, which highlights the sophistication of the groups exploiting such vulnerabilities. There is an arms race between cybercriminals and legitimate software developers.

Unfortunately, the criminals' ability to quickly find and exploit new vulnerabilities outpaces the software vendors' abilities to fix and release patches. Some software companies update security patches once a quarter; others are slow to acknowledge vulnerabilities. Even companies that carry out security updates methodically and regularly are often slow to deploy them throughout the organization.

Any lapse in security protocols leaves corporate systems wide open to unethical hacking. It is vital for companies to acknowledge that there are always potential threats. While amateur hacking may be considered mischief, security holes that allow hackers to break into corporate systems results in cybercrime with very serious consequences.

---

59 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002).

60 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 5.

Small-Business Targets

Small businesses are an easy target for cyber-attacks, as these companies usually fail to recognize the impact of cybercrime on their business. According to a recent report by Symantec:

> ". . . small businesses believe they are immune to attacks targeted at them. However, money stolen from a small business is as easy to spend as money stolen from a large business. And while small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank. While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, they are potentially easy targets as they are typically less careful in their cyber-defenses. Criminal activity is mainly driven by crimes of opportunity. With cybercrimes, that opportunity appears to be with small businesses."[61]

A notable impact is the use of small businesses to reach the cybercriminals' ultimate targets — the large company that the smaller company works with. As the Symantec report states:

> "Additionally, small businesses and organizations can become pawns in more sophisticated attacks. Driven by attack toolkits, in 2012 the number of web-based attacks increased by one third and many of these attacks originated from the compromised websites of small businesses. These massive attacks increase the risk of infection for all of us. . . . Supplementing their phishing attacks, cyber-espionage gangs now hijack these websites, lying in wait for their targets to visit so that they can infect them. This type of attack, called a watering hole, is another way attackers leverage weak security of one entity to defeat the strong security of another."[62]

Small businesses need to recognize cybercrime as a business risk and apportion the budget to combat it. They must realize that small is not invisible, but only makes them easy targets for cyber-attacks. They must ensure that all the necessary protection measures are in place,

---

61 Symantec, *Internet Security Threat Report 2013*, Volume 18, at p. 4.
62 Symantec, *Internet Security Threat Report 2013*, Volume 18, at p. 4.

including updated software and security patches and a procedure for authorized IT use for all employees.

Infiltration

Cybercrime is perpetuated by ingenious minds, which now include the organizational skills of crime syndicates.[63] This scenario makes the corporate sector, particularly the high-tech industry, highly vulnerable to infiltration, as organized crime groups usually seek foreign accomplices. Organized cybercrime is an international phenomenon and is often characterized by the systematic infiltration (and, in some cases, domination) of particular business sectors, often through legitimate front companies. As one writer recommends:

> "Consequently, the kind of due diligence exercise that has long been common in the banking sector needs to be extended to other industries. For bankers, 'know your customer' has become standard practice. For the hi-tech business, it is perhaps even more important to know your partners, especially when they are from another country. Questions need to be asked about their financing, their clients, and their associates — as well as the extent to which there are laws against cyber-crimes. Thorough background checks are essential prior to allowing any joint use of data and communication systems, or to bringing in their representatives to work with one's own employees. When there is overseas expansion, these background checks need to be extended to new employees and consultants. Although this might appear to be an exaggerated concern, it is not."[64]

Combative Measures

Awareness and Education

It is common knowledge that hackers break into computers, but there is a persistent misconception that a cybercriminal is the same as a hacker. A cybercriminal is not merely a mischief-maker, but a person

63 Organized crime groups are discussed in the section "Business Impact of Organized Cybercrime", above.

64 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at p. 6.

with a keen and intelligent mind who launches a successful cyber-attack only after first understanding how to cover his tracks. As an investigative report states:

> "Hackers employ techniques, such as 'onion skin' technology, to make their presence on the Internet or e-mail anonymous. They may penetrate multiple systems and 'daisy chain' their attacks (sometimes called 'connection laundering') to increase the difficulty of tracing them back from their victims. They may work in tandem with other hackers and store their hacking 'tools' at remote secondary sites in different states or countries. Interpol, the international police agency, estimates there are more than 30,000 hacker-oriented Web sites."[65]

Business enterprises must be educated and also must educate their employees to understand and be aware of the potential dangers of a cyber-attack perpetrated through social engineering. In the context of cybercrime, social engineering refers to practices that are used to deceive people into divulging confidential information or unknowingly commit acts that enable a cybercriminal to get access to information that can be used to commit fraud or gain unauthorized access to computer systems and networks.

With the proper training, employees can safeguard company information, ensuring that it is not downloaded or given away for free to somebody that either asks for it over the telephone or logs onto a web page.[66]

Similarly, good training and procedures can reduce the risk of accidental data loss and other insider risks. Employees must be trained to recognize the value of data and the measures they must adopt to protect it.[67] Deloitte suggests that most organizations should consider a continued risk-based approach to cyber-security, along with a renewed focus on a more in-depth analysis of their inbound and outbound network traffic. "Such an approach incorporates the potential vulnerability to and impact of cybercrime, along

---

65 State of New Jersey Commission of Investigation and the Attorney General of New Jersey, "Computer Crime: A Joint Report" (June 2000), at p. 53. The report is available at http://csrc.nist.gov/publications/secpubs/computer.pdf.

66 State of New Jersey Commission of Investigation and the Attorney General of New Jersey, "Computer Crime: A Joint Report" (June 2000), at p. 53.

67 Symantec, *Internet Security Threat Report 2013*, Volume 18, at pp. 20–21; Symantec Press Release, "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually" (5 September 2012).

with other, perhaps more familiar and measurable risks, such as unauthorized trades and foreign currency risk."[68]

Security Plan

Despite reports on heavy costs resulting from cybercrime, Internet security has not become a boardroom priority in many organizations. Many businesses would rate the risk of cyber-attacks as low. Relatively few organizations have recognized the very serious threat of cybercrime and even fewer have addressed it. As found in recent studies, many of the surveyed businesses, especially small businesses, did not have a well-defined security plan in place.[69]

Many businesses do not apportion amounts for internet security or the budget allocation is marginal compared to the risk. Of course, higher spending does not necessarily yield greater security. Organizations may "allocate significant resources to technological security measures, but neglect simple, inexpensive measures such as patch management, log analysis, privilege restrictions, password expiration, and termination of former employees' access through a robust deprovisioning process".[70]

This suggests that there is a need for a major shift in thinking about cyber security and in planning and implementing security measures. Such measures are particularly important if e-commerce is to reach its full potential and if individual companies are to avoid significant losses as a result of criminal activities. Perhaps the most important changes are needed in the corporate conception of cyber security.

This has two distinct but overlapping dimensions: security has to be understood in broad rather than narrow terms, and security can no longer be an after-thought, but needs to be part of a company's intelligence, planning, and business strategy. In this context, there are several specific recommendations that need to be considered carefully by firms, particularly those in the high-tech sector.

---

68 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat" (January 2010), at p. 7.

69 Varon, "FBI: Cybercrime Still a Priority", CIO (15 October 2001); Symantec, *Internet Security Threat Report 2013*, Volume 18, at p. 4; Symantec Press Release, "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually" (5 September 2012).

70 Deloitte, "Cyber crime: a clear and present danger — Combating the fastest growing cyber security threat", at p. 9.

Business enterprises are trying to establish their presence on the Internet and through online communications. The idea is to show potential clients that the newest technology is being deployed to create an efficient business environment, which is considered a cornerstone to business growth and change. However, this rush to establish a strong web presence and adopt online communications tends to discount the security preparedness of these companies.

Very often, data exchange for information sharing takes place in an unsafe Internet environment, where scant regard has been paid to security issues. Business enterprises must understand the implications this can have on their business and address the situation in-house before it is too late. One of the first steps in this direction is the establishment of sound preventive measures.

Reporting and Control Mechanisms

Most businesses are afraid to complain to law enforcement agencies for fear of exposing security vulnerabilities. Companies want to avoid public relations disasters that may adversely impact their business reputation. Despite the government's ability to gather evidence through a mandatory process not available to the private sector, companies are concerned that their ability to gather the information they need to stop the intrusions and to find the perpetrators may be restricted once the government becomes involved.

Corporations also fear that making it known to law enforcement agencies that intruders penetrated their defenses may invite government regulation. They would rather institute their own system to ward off attacks than comply with government-dictated controls. For there to be an effective partnership between law enforcement and the business community, the corporate sector must have confidence that any security breaches referred to law enforcement agencies will be handled as swiftly, competently, and confidentially as possible.

Corporate victims will be more likely to report intrusions to law enforcement agencies if law enforcement agencies' technical proficiency and reaction time improves and if the investigation and discovery phases of cases adequately preserve confidentiality. Law enforcement expertise and resources must be available to handle a high volume of routine cases as well as high-profile matters. It would be a good measure to designate a singular reporting point for cybercrime that would then pursue and investigate the crime. Police

are ill equipped especially in developing countries to combat this form of cybercrime. A recent study reports:

> "While the majority of companies have the important security building blocks . . . needed for their security infrastructure, less than half of organizations in this study have advanced protections to fight botnets and APTs.
>
> The majority of organizations in the United States and Germany are deploying solutions and training that are more specific to addressing cyber risk such as anti-bot, application controls, and security intelligence systems. Whereas, other countries represented in this study are lagging behind in their cyber security readiness.
>
> Senior executives are more concerned about cyber-attacks and see a greater need to take steps to reduce the risk. In all organizations represented in this study, respondents who hold leadership positions are more likely than respondents in lower-level information technology and information technology security positions to say their organizations are very concerned and have fully implemented and applied security precautions, technology, and training."[71]

Criminal Intelligence Analysis

A company's business intelligence analysis is not complete until it contains a criminal intelligence analysis in the form of comprehensive information that is compiled, analyzed, and disseminated to all concerned parties as a means to prevent and monitor cybercrime.

> "Indeed, criminal intelligence analysis needs to be integrated fully into business intelligence; risk assessment needs to incorporate criminal threats; and cyber-security needs to be conceptualized as part of a broader security problem that cannot be understood or dealt with in strictly technical terms. Defending against such contingencies requires that high-tech firms develop broad security programs that incorporate cyber security into a much broader program. Cyber security needs

71 Ponemon Institute, "The Impact of Cybercrime on Business — Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong, and Brazil" (May 2012), at p. 2.

> to be one component of a broader security program that includes personnel, physical assets, the provision of services, and financial assets. An arrangement in which the security officer is responsible for cyber security as part of a comprehensive mandate is likely to be more effective and appropriate than one in which cyber security is seen as a distinct portfolio separate from other components of security."[72]

Partnerships and Information-Sharing Arrangements

Another strategy to combat rising cybercrime is be to develop a working partnership with government and law enforcement agencies. There are precedents for such arrangements in other sectors. In recent years, the major oil companies, although very competitive with one another, have established information-sharing arrangements and worked very closely with law enforcement to minimize infiltration by organized crime figures and criminal companies.

One such initiative is the European Network and Information Security Agency (ENISA), which functions as a networking center for sharing information security expertise in the European Union (EU), among its Member States, the private sector, and European citizens. ENISA works with these groups to develop advice and recommendations on good practices in information security.

It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU.[73]

A recent initiative has been the launch of the International Cyber Security Protection Alliance (ICSPA) in October 2012. The ICSPA is supported by a group of Canada's most reputable businesses: CGI Canada, McAfee, Research in Motion, Lockheed Martin, and Above Security. In May 2013, the ICSPA conducted a study to determine the

---

72 Williams, "Organized Crime and Cyber-Crime: Implications for Business", CERT Coordination Center (2002), at pp. 5–6.

73 Additional information about ENISA and its work can be found on the ENISA website at http://www.enisa.europa.eu. ENISA is further discussed in the subsection "The European Response", below.

impact of cybercrime on businesses in Canada[74] and has been hailed as a useful tool to determine awareness of cybercrime and its associated dangers.

Deterrents to Effective Regulation

Reporting Concerns

Initiatives such as ENISA and the ICSPA are warranted and should be encouraged. However, cooperative initiatives are not easy to implement. The key concern has always been the jurisdictional differences and policy differences in the information technology sectors of different countries, where some believe regulation is not mandated or others tend to over-regulate. Another key concern that works against such initiatives is the issue of reporting cyber-attacks.

There is broad agreement that cybercrime is under-reported. One of the most important (and also most understandable) reasons is concern on the part of financial institutions and businesses regarding reputational damage. Reporting concerns are even more relevant for e-commerce businesses where business expansion hinges on secure and speedy transactions. In these cases, there is the justifiable desire to avoid any disclosures that might undermine customer confidence and place a company at a competitive disadvantage.

Unfortunately, this reticence to report cyber-attacks works in favor of cybercriminals. There are three levels at which the disclosure issue can be understood: within the business sector, in the relationship between business and law enforcement, and full public disclosure. Indeed, the more the first two options are developed and refined, the less need there will be for full public disclosure.

One useful approach, therefore, would be for companies within a particular sector to agree to share information about cybercrimes among themselves, on the assumption that similar methods and techniques that are used against one business entity also are likely to be used against others. Even more important is the development of mutual trust between businesses and law enforcement agencies.

There are several instances of companies working closely with law enforcement agencies in responding to cyber-threats. For such cooperation to be effective, however, law enforcement agencies have to

74 The study is available on the ICSPA website at https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.pdf.

synthesize and exercise considerable care and discretion not to expose company vulnerabilities, while the companies themselves have to be willing to report any criminal activities directed against their information and communication systems.

Transborder Nature of Cyberspace

Cybercrime mimics traditional criminal exploitation, but can be executed with unprecedented ease, speed, and with the potential to hit across jurisdictions. Consequently, the tasks of detecting, investigating, and prosecuting cybercriminals pose formidable challenges to law enforcement agencies across the globe.

Combatting cybercrime effectively requires a clear mandate on complete cooperation with inter-country investigations in order to facilitate the timely and efficient sharing of information. However, in the context of cybercrime, such information exchange is extremely difficult, if not impossible.

Forensic computing and evidence preservation protocols are indispensable for effective investigation and prosecution of cybercrime, particularly in light of the transborder nature of evidence collection.[75] It is likely that many jurisdictions do not follow these techniques and protocols and may lack the trained personnel to implement these procedures. These impediments to effective policing are all related to the essential nature of cyberspace, which leads to its greatest advantage for the cybercriminal: anonymity without boundaries. As one commentator explains:

> ". . . at least six factors make the ex post criminalization computer network abuse problematic: (A) the presence of arbitrary spatial distinctions in cyberspace; (B) the difficulty of detecting criminal activity in cyberspace; (C) the difficulty of determining criminal identity in cyberspace; (D) the difficulty of proving criminal culpability in cyberspace; (E) the absence of incentives to report computer crime; and (F) the absence of deterrence in present criminal law provisions."[76]

---

75 Broadhurst, "Developments in the global law enforcement of cyber-crime", 29/2 *Policing: An International Journal of Police Strategies and Management* (2006) 408, at p. 416.

76 Dierks, "Electronic Communications and Legal Change: Computer Network Abuse", 6 *Harv. J. Law and Tech.* (Spring 1993) 307, at pp. 330–331.

These challenges makes the combating of cybercrime a global problem, a transborder issue that goes beyond any particular jurisdiction.

Enforcement and Regulation Issues

Countries across the globe agree that the key problem lies in the nature of the cyberspace and the perpetration of cybercrime. The scale of the offense and victimization is much larger in scope, commission of cybercrime is cheaper, and criminals can easily escape detection and apprehension. These factors are further compounded by the technical and legal complexities of investigating cybercrime; of collecting, analyzing, and presenting evidence; and of identifying, apprehending, and prosecuting offenders — all of which present enormous challenges to the regulation and enforcement of cybercrime.

Cybercrime is more difficult to detect and harder to prove than conventional crime, as cybercriminals find new ways to exploit the system. The anonymity of the web and the extraterritorial (non-jurisdictional) nature of such crimes work to the advantage of cybercriminals by facilitating the perpetration of crimes from remote locations, while posing an immense challenge for forensic scientists and criminal investigators.

Cybercrime is a low-risk and high-reward venture. Armed with just a few basic skills and a great deal of persistence, a cybercriminal can easily move large sums of money across countries or enter and destroy valuable data and cause enormous damage to the affected organizations. It also can turn out to be a "dark crime" because of the lack of information that law enforcers have on its incidence and spread. Detection of cybercrime is often difficult due to lack of mandatory reporting mechanisms and the necessary new-age skills to address, uncover, and prosecute it.[77]

The three primary factors that make the detection, investigation, and prosecution of cybercrime so challenging are anonymity, non-traceability, and lack of geographical boundaries. The current network system does not require a user to expose facial, vocal, or physical features, or even his true identity by name. Under this anonymity, is sometimes impossible to detect the crimes committed, leave alone the criminal.

---

77 Talwar, "Computer-Related Crime", Inaugural address by the Deputy Governor of the RBI, National Seminar on Computer-Related Crime (New Delhi, 24 February 1999), *CBI Bulletin* (February 1999), at p. 6-6.

All information over a network system is exchanged in the form of electronic data; once the data is erased, there is no physical trace of evidence left, without which prosecution is impossible. Cyberspace does not require a physical location or any geographical limitations. Information is easily and instantly communicated in real time, regardless of the distances between users, making borderless remote access significantly easy. This means that the concept of national borders ceases to apply in cyberspace.[78]

Extraterritorial Jurisdiction

Traditionally, the jurisdiction of courts is local. Courts hear prosecutions related to violations of local laws, provided that there is an adequate link between the offense and the jurisdiction in question. However, legislatures will often confer extraterritorial jurisdiction for certain crimes, such as crimes committed by members of the defense forces or on the high seas and counterfeiting offenses. In exceptional cases, national laws may even be applicable to offenses committed overseas by foreign nationals.[79] However, as one commentator remarks:

> "These circumstances [of extraterritorial jurisdiction] are, to say the least, most unusual. But in a shrinking world where the internet has surmounted borders, a key challenge is to define a law that encompasses not only local jurisdiction but also global [jurisdiction].
>
> To the extent that international computer-related crime is amenable to international enforcement, it will require concerted international cooperation. Past performance in the context of other forms of criminality would suggest that this cooperation is unlikely to be forthcoming except in the relatively infrequent types of illegality where there is widespread international consensus about the activity in question (such as child pornography or fraud on a scale likely to destabilize financial markets), and about the desirability of suppressing

78 Yasutomi, Address at the National Seminar on Computer-Related Crime (New Delhi, 24 February 1999), *CBI Bulletin* (February 1999), at p. 19.

79 Grabosky, "Computer Crime: A Criminological Overview", Presentation at the Workshop on Crimes Related to the Computer Network, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (Vienna, 15 April 2000), at p. 17.

> it. In many instances, extradition is likely to be more cumbersome, the greater the cultural and ideological distance between the two parties.
>
> Even so, this would assume a seamless world system of stable sovereign states; such a system does not exist today, nor is it likely to exist in our lifetime. Law enforcement and regulatory vacuums exist in some parts of the world, certainly in those settings where the state has effectively collapsed. Even where state power does exist in full force, the corruption of individual regimes can impede international cooperation.
>
> Issues of transborder criminality aside, many law enforcement agencies as we know them lack the capacity on their own to control computer-related crime which occurs entirely within their own jurisdiction."[80]

Thus, the global nature of cybercrime poses great challenges for the detection, investigation, and prosecution of cybercriminals. In a crossborder crime, prosecution of the offense requires the authorities to determine where the crime has occurred, followed by the collection of evidence and the offender being brought to trial. Cybercrime, however, poses serious and complex legal problems concerning both jurisdiction and extradition. As one commentator states:

> "If an online financial newsletter originating in the Bahamas contains fraudulent speculation about the prospects of a company whose shares are traded on the Australian Stock Exchange, where has the offense occurred? Even if one is able to decide which law is applicable, further difficulties may arise in applying that law.
>
> In a unitary jurisdiction, such as New Zealand, where there is one law and one law enforcement agency, determining and applying the applicable law is difficult enough. Criminal activities committed from across the globe, however, pose even greater problems. Sovereign governments are finding it difficult to exercise control over online behavior at home, not to mention abroad. A resident of Chicago who falls victim to a

80 Grabosky, "Computer Crime: A Criminological Overview", Presentation at the Workshop on Crimes Related to the Computer Network, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (Vienna, 15 April 2000), at pp. 17–18.

> tele-marketing scam originating in Albania, for example, can expect little assistance from law enforcement agencies in either jurisdiction. As a result, regulation by territorially based rules may prove to be inappropriate for these types of offenses . . . .
>
> Extraterritorial law enforcement costs are also often prohibitive. The time, money, and uncertainty required by international investigations, and if successful, extradition proceedings, can be so high as to preclude attention to all but the most serious offending. Moreover, the cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities which, despite prevailing trends towards globalization, exists only infrequently.
>
> Other issues which may complicate investigation entail the logistics of search and seizure during real time, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology."[81]

Lack of Trained Investigators

Another major challenge to combating cybercrime, at least at the present moment, is the lack of trained computer-crime investigators. Police forces find such experts difficult to retain. As one commentator observes:

> "Much like the priesthood, policing was formerly a lifetime vocation. In many police services today, trained computer crime investigators must battle for the equipment which they regard as necessary to do their job. The development of expertise in forensic computing, moreover, may require a concentration and specialization that precludes the development of the more general expertise required for advancement through the ranks. With the traditional high-status areas of policing such as homicide investigation now joined by those

81 Grabosky, "Computer Crime: A Criminological Overview", Presentation at the Workshop on Crimes Related to the Computer Network, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (Vienna, 15 April 2000), at pp. 16–17.

> of general management as the most prestigious areas of policing, prospects for upward mobility on the part of the computer crime investigator are thus limited."[82]

In India, police inspectors handle cases and are inept in following the leads or collecting evidence. The medium of crime requires attention in proportion. However, this crucial factor has been missing.

Problems with International Cooperation

The strategic challenges discussed so far when scaled up to the international scene only magnify the problems and inadequacies of successfully tracking down and prosecuting individuals involved in cybercrime. The seamless nature of the Internet has long been a global concern that needs to be addressed. Some of the major problems related to international cooperation in the area of cybercrime and criminal law are:

(1) The lack of global consensus on definitions of cybercrime;
(2) Jurisdictional variations in expertise (and sometimes the lack of expertise) on the part of the police, prosecutors, and the courts in relation to this criminal sector;
(3) The inadequacy of existing laws for investigation and access to computer systems and networks, including the inapplicability of seizure powers for intangibles such as computerized data;
(4) The lack of harmonization between the various national procedural laws concerning the investigation of cybercrime; and
(5) The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, and the inability of existing treaties to take into account the dynamics and special requirements of cyber security.

This situation is aptly summarized by one of the participants at an international conference of the International Society for the Reform of Criminal Law:

> "It is a matter of great concern and dismay that there are still jurisdictions, such as Europe, where assistance is not as

82 Grabosky, "Computer Crime: A Criminological Overview", Presentation at the Workshop on Crimes Related to the Computer Network, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (Vienna, 15 April 2000), at p. 18.

> readily forthcoming as would be ideal. Where letters seeking information go unanswered, or where judicial process can delay the transmission of information — in some cases, until after a trial is over. . . . There are disparities between jurisdictions as far as extraditable offenses are concerned. Many continental jurisdictions do not recognize private sector corruption as a crime and will not grant a request for extradition where that offense is alleged. There are differences between jurisdictions with regard to whether assistance can be afforded, depending on the stage at which proceedings have reached."[83]

It is difficult to curtail a crime that is committed from one jurisdiction when the potential impact lies in a different jurisdiction, because, technically, the criminal act may not be defined by the place where it has occurred but by the place where it was perpetrated. This distinction allows the criminal to exploit the situation and escape scot-free.

There also may be differences between the various law enforcement authorities that need to collaborate to address this form of global crime. Some law enforcement bodies may be focused on the different types of fraud (internet banking fraud, identity theft, shopping and auction site fraud, or the various types of scams), others on the posting of illegal content (such as copyright violations or online pornography), or even investigations that involve components of information and communications technology (ITC), such as forensic exploitation of crime scene evidence. As the scope of each law enforcement body varies, they may be unable to cooperate effectively enough to harness the synergetic interrelation between agencies and apprehend the criminal.

Cybercriminals, on the other hand, have a herd mentality. They even have their own collaborative forums, where they share new methods to perpetrate attacks. There is no such forum in the law enforcement domain where law-enforcers from the world over can meet to chalk out action plans and exchange information on the challenges of addressing and circumventing cybercrime. In fact, the responses have different characteristics and different objectives and vary from one jurisdiction to another. There is no uniform response

---

83 Wright, "Cybercrime from the UK perspective: the problem and some solutions", Address by the Director of the Serious Fraud Office, London, *Sixteenth International Law Conference of the International Society for the Reform of Criminal Law* (Charleston, South Carolina, 6–10 December 2002), at p. 12.

that addresses this form of crime; the responses are as varied as they are fragmented.

Need for Effective Global Collaboration

To effectively combat cybercrime, a concerted effort at effective global collaboration is imperative. Effective global policing highlights the importance of robust, effective, and speedy channels of communication between legal and investigatory authorities and, on a more formal basis, of mutual legal and judicial assistance to secure the production of evidence in a form which can be admitted in a criminal prosecution.

Laws, criminal justice systems, and international cooperation have to keep pace with technological change. Only a few countries have adequate laws to address the problem and, of these, no country has resolved all the problems related to legal issues, law enforcement, and preventive means. The answer lies in first recognizing the many strategic challenges and addressing them by forging relationships across borders to coordinate activities and collaborate efficiently.

An interesting observation has been to approach the transnational nature of cybercrime by fixing a point of sources to indicate jurisdiction. Such a measure will definitely entail defining the jurisdiction, but such is only possible if there is a global law acceded to by all.

However, the answer does not lie in an over-simplistic solution such as creating a uniform legislation that is applicable internationally (and which is hardly likely to occur, in any case). Rather, a stride in the right direction would be to ensure that individual countries are able to prosecute offenders who infringe national laws within their own borders and/or allow extradition or mutual assistance during the investigation and prosecution processes. This will only be possible when there is a common framework to identify the many problems and challenges and to address them effectively.

International Response to Cybercrime

In General

Today, law enforcement bodies and business enterprises have had to adopt new weapons in the fight against cybercrime. It is a new war fought on a new battlefield. Law enforcers, businesses, and individuals have been affected by attacks and are still coping with attempts to counteract and prevent continued assault. New techniques for

monitoring, tracking, and trapping criminals have been developed. New laws have been passed in an effort to safeguard personal and economic well-being, often at the expense of individual freedoms and privacy.

However, as technology becomes even more interlaced with human society, criminals will continue to find new ways to exploit, deceive, and cause damage. Society as a whole must evolve, adapt, and stay one step ahead. Facing this challenge will require radical measures.

Necessary Response Mechanisms

One of the most import response mechanisms is the establishment of appropriate legal instruments, especially procedural measures, which will allow effective detection and prosecution of high-tech offenses, particularly crimes of a transnational nature. Law enforcement bodies and the judiciary must gain new expertise in the methods of gathering electronic evidence and follow new procedural rules for using such evidence to prosecute cybercriminals.

Another necessary measure to respond adequately to cybercrime is to upgrade all applicable laws in each jurisdiction to make them technology-neutral, so that they avoid becoming obsolete. A harmonized approach across countries will go a long way toward ensuring that anonymity and lack of jurisdiction do not always become standard weapons of the perpetrators.

Firms should take the initiative in securing their networked information. Regardless of whether or not relevant laws exist, companies must take all precautionary measures to make their own information and systems secure.

Governments should assure that their laws apply to cybercrimes and, furthermore, that these laws are updated so as to be current in the existing digital environment. It is imperative so that no one nation is placed at a disadvantage. If one nation identifies the unique challenges presented by cyber-security and makes an attempt to legally provide an adequate legal framework in response, it is crucial that other nations profit from this lesson and review their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cybercriminals.

Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security. To be prosecuted across borders, an act must be a crime in each jurisdiction. Thus, while

each country's legal traditions must be respected, nations must define cybercrimes in a harmonized manner.

Current Status of Crossborder Collaboration

The ENISA recognizes that effective collaboration between law enforcement bodies and the Computer Emergency Response Teams (CERTs) is essential to combat cybercrime effectively, particularly in a crossborder setting:

> "Evidence from our research indicated that in practice, data protection, data retention, and obligations to work with law enforcement constituted the greatest set of challenges for crossborder CERT cooperation. . . . For example, with respect to their own legislation 15 out of 17 respondents reported that they had at least some knowledge of definitions of computer crime or data protection and privacy law; 14 out of 17 respondents reported some knowledge of data retention rules [and] procedures for preserving computer data as evidence or national security rules; and 13 out of 17 respondents reported at least some knowledge concerning laws about working with law enforcement.
>
> With regard to international aspects, however, the situation is different. Here, 9 out of 17 respondents reported some understanding of international efforts to harmonize computer crime definitions (as afforded by the Convention on Cybercrime, for example). Eleven out of 17 respondents indicated some understanding of international efforts to harmonize data protection and communications privacy, whilst 9 out of 17 respondents reported some understanding of international efforts concerning national security laws.
>
> There was least familiarity with international efforts governing rules determining the competent court, applicable law for specific incidents, or legal value of evidence: only 7 out of 17 respondents indicated any degree of understanding [of] international harmonization regimes in this regard.
>
> Regarding the specific legal fameworks cited as justification for their own request being denied, 12 out of 14 respondents cited data protection and privacy law as having been used as a reason to justify a declined request by a peer. On the other hand,

> 5 out of 13 respondents indicated that with some degree of frequency data protection and privacy laws; rules concerning computer data as evidence; laws concerning crossborder mutual legal assistance; laws concerning working with law enforcement or rules concerning the legal value of evidence were all cited as a justification to withhold information in a crossborder request. Of course, this should not be taken as clear proof that such exchanges would certainly have been in clear breach of these laws, but rather that sufficient doubt existed on the legality of the exchanges to withhold them."[84]

The European Commission already plays an important role in various public-private structures dealing with cybercrime, such as the Fraud Prevention Expert Groups.[85] The Commission is convinced that an effective general policy for the fight against cybercrime also must include a strategy for cooperation between public sector and private sector operators, including civil society organizations.

Moreover, cybercrime, like other areas of criminal law, had been left to the EU Member States to regulate in the exercise of their police powers. Despite national legislation to combat cybercrime, policing by individual Member States is ongoing, and regulation and enforcement at the state level has exposed varied responses and understanding of this form of crime.

In the United States, the expansion of federal criminal jurisdiction over cybercrime has been a recent phenomenon, largely a product of broad legislative and judicial interpretation of the Commerce Clause of the Constitution.[86] By relying upon the Commerce Clause for authority, Congress acknowledged the stateless and global nature of the Internet by drafting specialized sections of the Criminal Code.

The innovation of any new technology or business model makes way for new forms of crime. With every advance in technology that enables advancement in commercial sectors, cybercrime evolves to provide ample scope for new forms of perpetuation which are perhaps designed to formulate a means to escape detection even before the

---

84 ENISA, *A flair for sharing — encouraging information exchange between CERTS. A study into the legal and regulatory aspects of information sharing and crossborder collaboration of national/governmental CERTs in Europe* (November 2011), at p. 9.

85 Additional information on the expert groups is available at http://expertgroups.govtrace.com/fraud-prevention.

86 The United States Constitution, Article 1, Section 8, Clause 3 (the Commerce Clause), which allows Congress to regulate matters that affect commerce with foreign countries and among the states.

perpetration of the crime. There seem to be no limits to the extent of loss or damage resulting from cybercrime.

The seemingly unstoppable advance of new forms of cybercrime has motivated many countries to devise suitable responses to curtail the damage caused by cybercrime. The initial response was to work within the existing legal framework, which soon proved too daunting a task. Nations then tried to enact comprehensive laws to try and curb as many forms of cybercrime as possible. However, the futility of this task became abundantly clear. The piecemeal approach in addressing the ever-evolving dynamics of cyberspace by enacting new laws to combat specific crimes and then reworking current legislation to incorporate other forms of cybercrime did not seem to be working in many countries.

Most countries soon realized that any approach to regulate cybercrime would need swift action and prosecution if the cybercriminal was to be brought to justice. Constantly reworking the current system to address new forms of cybercrime was both an impractical and futile exercise, only resulting in the increased incidence of more innovative forms of cybercrime, but not in its curtailment. As one writer has commented, the correct response is to gain a better understanding of the scope of cybercrime and to derive more reliable statistics regarding cybercrime, so as to:

> ". . . better measure existing harms, anticipate trends, and determine the need for constant and greater legislative reform. The idea is to understand that the responses should not be designed to punish a few perpetrators who might get caught, but to curtail those larger infrastructural environments that allow domestic and global networks to profit from these acts. Outdated laws and weak enforcement mechanisms create an inhospitable environment in which to conduct e-business and create barriers to its exchange and growth."[87]

Nations have therefore realized that the need of the hour is to establish a legal system that can create a regime where cyberspace is secure. This requires not only comprehensive study and continual review of substantive and procedural laws that might be drafted to create a regulatory environment, but also practical consideration of how law

87 McConnell International, "Cyber Crime . . . and Punishment", *Computer Crime* (3 November 2007), at http://knowaboutcomputercrime.Blogspot.com/2007/11/cyber-crime-and-punishment.html.

enforcement agencies will enforce the regulatory environment so created against acts that easily escape detection, investigation, and prosecution.

Currently, chances are that if five acts breach cyber-security, one act will fall within the regulatory regime. This is because of the dichotomy in cyber regulation — it is extremely challenging to enact and enforce laws that address the many challenges of crime in cyberspace; at the same time, law enforcement agencies cannot function efficiently without such a legal or regulatory framework.

In the last 10 years there have been significant developments in the number of legislations and policies that have been promulgated to counter cybercrime. A UNDOP study identified five possible "clusters" of instruments:

(1) Instruments developed in the context of, or inspired by, the Council of Europe or the European Union;
(2) Instruments developed in the context of the Commonwealth of Independent States or the Shanghai Cooperation Organization;
(3) Instruments developed in the African context;
(4) Instruments developed by the League of Arab States; and
(5) Instruments developed under the auspices of, or associated with, United Nations entities.[88]

The study has indicated that each of the clusters there is an inter or intra relationship between the instruments promulgated such as United Nations entities, such as UNECA and the International Telecommunications Union (ITU) also have had some involvement in the development of instruments in the African context, including the Draft African Union Convention and the SADC Model Law. The Commonwealth Model Law, for example, is based closely on the Council of Europe Cybercrime.[89]

National Policy Initiatives

The dichotomous nature of cyberspace has evoked turbulence in the regulation of the Internet by most nations. Several countries, particularly in Europe and Asia, have addressed a number of these broader

88 United Nations Office on Drugs and Crime Vienna, *Comprehensive Study on Cybercrime*, February 2013.
89 United Nations Office on Drugs and Crime Vienna, *Comprehensive Study on Cybercrime*, February 2013.

information security factors, but very few countries can actually demonstrate that they possess adequate legal measures to curb cyberspace violations. Apart from legislative initiatives, many countries have launched major policy initiatives to combat this threat.

Europe

The EU's Internal Security Strategy[90] is the EU's shared agenda to address security challenges affecting the social market economy proposed in the Europe 2020 vision.[91] Also notable is the Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the EU Member States (the "Swedish Initiative"),[92] which aims to "enhance the effective and expeditious exchange of information and intelligence between law enforcement authorities".[93]

In 2008, the European Council took a decision[94] which specifically states the conditions under which personal data may be processed "for the purposes of preventing, investigating, detecting, or prosecuting a criminal offense or of executing a criminal penalty".[95]

The EU went one step further when it launched its European Cybercrime Platform (ECCP). This is managed by Europol and brings together law enforcement, the private sector, and Internet service providers and tries to establish a wider and more coordinated approach to address cybercrime. Other noteworthy initiatives are the Prüm Decision and the European Criminal Records Information

90 Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673, 22 November 2010.

91 Guild and Carrera, "Towards an Internal (In)security Strategy for the EU?", CEPS (January 2011), at http://aei.pitt.edu/15475/1/LSE_No_35_EG_&_SC_on_internal_insecurity_strategy.pdf.

92 Council Framework Decision 2006/960/JHA of 18 December 2006, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2006F0960:20061230:EN:PDF.

93 Council Framework Decision 2006/960/JHA, Preamble, Paragraph 6.

94 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed within the framework of police and judicial collaboration in criminal matters.

95 ENISA, *A flair for sharing — encouraging information exchange between CERTS, A study into the legal and regulatory aspects of information sharing and crossborder collaboration of national/governmental CERTs in Europe* (November 2011), at p. 15.

System (ECRIS).[96] The Prüm Decision is a framework for Member States to gain access to one another's automated DNA analysis files, automated fingerprint identification systems, and vehicle registration data. ECRIS is based on a decentralized IT architecture: criminal records data are stored solely in national databases and exchanged electronically between the central authorities of EU countries upon request.

United Kingdom

The United Kingdom's Cyber Security Strategy was issued in 2009, with the aim of "protecting and promoting the United Kingdom in a digital world". It established the Cyber Security Operations Center to "actively monitor the health of cyberspace and coordinate incident response". The Strategy was updated in 2011, with the primary objectives of tackling cybercrime and making the country "more resilient to cyber-attacks".

Germany

In Germany, the Cyber Security Strategy issued in 2011 proposed the establishment of a National Cyber Response Center and a National Cyber Security Council. The focus of the Cyber Security Strategy is on civilian approaches and measures, which are complemented by measures taken by the German armed forces to protect the nation's capabilities and by mandatory measures make cyber-security a part of Germany's preventive security strategy. One of the objectives of the National Cyber Security Council is to promote better cooperation within the federal government and between the public and private sectors.

France

France has recognized the role of incident response communities through the formation of the National Agency for Information Systems Security (*Agence nationale de la sécurité des systèms d'information* — ANSSI) and the elaboration in its Defense and

96 ENISA, *A flair for sharing — encouraging information exchange between CERTS, A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe* (November 2011), at p. 15.

Security Strategy for French Strategic Information Systems 2011 (*Défense et sécurité des systems d'information Stratégie de la France*). Through these initiatives, France acknowledges that incident response is an important mechanism for resilience against cyber-attacks.

The Netherlands

The Netherlands released its National Cyber Security Strategy (NCSS), "Success through cooperation", in 2011. The NCSS outlined plans to "expand and reinforce the current GOVCERT.NL and place it with a National Cyber Security Center".[97]

The focus of GOVCERT.NL is to bolster information security within the Dutch government by online monitoring of sources, providing guidance on possible vulnerabilities, and issuing warnings in case of threats.

Denmark

Denmark enacted the Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats on 1 June 2011. The Act established a clear legal basis for the processing of personal data by the Danish National Information and Technology and Telecom Agency for the purpose of running the governmental warning service. It indicates that no court order is required to "process . . . collect, register, analyze, and store . . . incoming and outgoing packet and traffic data of connected authorities and private enterprises".[98]

Czech Republic

The Czech Republic has issued the 2011–2015 Cyber Security Strategy. It notes the importance of incident response and proposes the establishment of a National CERT Agency as a government coordination agency able to respond immediately to computer incidents. This agency will become part of the national and international cyber threat early warning systems.

---

97 National Cyber Security Strategy, at p. 5.

98 ENISA, *A flair for sharing — encouraging information exchange between CERTS, A study into the legal and regulatory aspects of information sharing and crossborder collaboration of national/governmental CERTs in Europe* (November 2011), at p. 16.

Australia

In early 2013, Australia announced the establishment of a new Australian Cyber Security Center (ACSC), drawing on the skills of the nation's best cyber security experts. The ACSC will be the hub of the government's cyber-security efforts and will boost Australia's ability to safeguard itself against cyber-attacks. It will analyze the nature and extent of cyber-threats and lead the government's response to cyber-incidents.

Australia's response to cybercrime came in 2011–2012, when there were more than 400 cyber incidents against government systems, requiring a significant response by the Cyber Security Operations Center. In 2012, 5,400,000 Australians were victims of cybercrime, with the cost to the economy estimated at AU $1,650,000,000.[99]

National Laws and Legislative Amendments

In General

As a response to the growing menace of cybercrime, national policy initiatives were followed by legislative changes in various countries. In a study undertaken by McConnell International,[100] most countries were rated as needing "substantial improvement in information security". Some of these countries indicated that they were addressing the concerns. Among the countries studied, the various forms of cybercrime are not treated uniformly.

In some countries, unauthorized access to computers, networks, and personal information is a crime only if there is wilful intent to cause harm; in others, data theft is only considered a crime if the data relates specifically to an individual's religion or health records or if the intent is to defraud. Many national laws prohibit crimes committed with or against government computers, but do not provide reciprocal protection to private sector computers.[101]

According to the McConnell study, Mauritius, the Philippines, and the United States have more stringent penalties for cybercrimes falling

---

99 "Australian cyber security center to be established", reported on the website of the Australian Government, Department of Defense (24 January 2013), at http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm.

100 McConnell International, "Cyber Crime . . . and Punishment", *Computer Crime* (3 November 2007).

101 McConnell International, "Cyber Crime . . . and Punishment", *Computer Crime* (3 November 2007), at p. 4.

within the scope of their laws than do many other countries. Several other countries, such as Cuba and Albania, are trying to update their laws, while others, such as Latvia, deter and punish cybercrime following the lead of the European Economic Commission (EEC) and the EU regulatory measures. Kazakhstan seeks to provide an answer within its national legislative system (the Criminal Code). Countries such as Iran have yet to identify and enact an adequate response, while countries such as Vietnam are aware that legislative action is needed.

United Kingdom

The United Kingdom Computer Misuse Act 1990 was enacted before the advent of the Internet and the growing incidence of cybercrime. The modifications to the Act were included in the United Kingdom Police and Justice Act 2006. These amendments to the Computer Misuse Act were further amended by the Serious Crime Act 2007. To prevent confusion, the government decided to apply these changes all at once, through a legislative order,[102] which came into effect on 1 October 2008.[103]

The scope of the Computer Misuse Act of 1990 was "to make provision for securing computer material against unauthorized access or modification; and for connected purposes". It established three computer misuse offenses and the corresponding penalties: unauthorized access to computer material (punishable with six months' imprisonment), unauthorized access with intent to commit or enable the commission of additional offenses (punishable with five years' imprisonment), and unauthorized modification of computer material (punishable with five years' imprisonment).

The scope of the Police and Justice Act 2006, which includes the amendments to the Computer Misuse Act, extends to more than computer crime. The maximum prison sentence for unauthorized access to computer material was increased from six months to two years. The "unauthorized modification of computer material" was amended to read "unauthorized acts with intent to impair or with recklessness as to impairing, operation of computer" and carries a maximum prison term of ten years.

---

102 The Police and Justice Act 2006 (Commencement Number 9) Order 2008.

103 Leyden, "UK cybercrime overhaul finally comes into effect, DDos doubly illegal from 1 October", *The Register* (30 September 2008), at http://www.theregister.co.uk/2008/09/30/uk_cybercrime_overhaul/.

The amended Computer Misuse Act also added another section, "Making, supplying, or obtaining articles for use in computer misuse offenses", punishable by a maximum prison term of two years. This section has been heavily criticized. While the legislator's intention clearly was to make the use of hacking tools illegal, this provision could equally be applied to the use of legitimate tools that could be used to conduct ethical hacking to identify security holes.

India

The Indian response emerged in the 1998 National Informatics Policy issued by the National Taskforce on Information Technology and Software Development. The taskforce submitted three key reports suggesting various measures to build India's infotech industry and spread the use of IT in the country. Subsequent to these findings, India passed the Information Technology Act in 2000.

The most important element of this Act is that it derives its concepts from the United Nations Commission on International Trade law (UNICTRAL) Model Law on Electronic Commerce. With thirteen chapters comprising ninety-three sections and four Schedules, the Indian Information Technology Act is an attempt to change the outdated laws and provide ways to deal with cyber-security and legally recognize electronic commerce, digital documents, and digital signatures.

Under the Information Technology Act, civil liability and stringent criminal penalties may be imposed on any person who causes damage to a computer or computer system. No penalty imposed or confiscation made under the Act will prevent the imposition of any other punishment under any other law in force. Sections 65–68 of the Act include provisions on the punishment that can be meted out for cybercrimes. Section 66 specifically deals with the offense of hacking.

What is interesting is that India has tried to combat the terrestrial nature of cybercrime by extending the applicability of the Information Technology Act globally. However, its provisions on penalties for cybercrime may be difficult to impose in the international arena. Under Section 76 of the Information Technology Act, the adjudicating court also has the powers to confiscate any computer, computer system, floppies, compact disks, tape drives, or any accessories in relation to which any provisions of the Act are being violated. No penalty or confiscation made under this Act will affect the imposition of any other punishment under any other law in force.

The Act also provides for wide search and seizure powers and investigative powers to be vested in the enforcement authorities. However, despite such provisions, a recent hacking of government websites saw government agencies refusing to give up access to the e-mails and systems, citing the right to privacy, which proved to be a huge impediment to the investigation of the offense.

The adjudication mechanism under the Information Technology Act relates to violation of specific provisions as enumerated in the statute. For grievances/offenses not covered by the Information Technology Act but arising out of online transactions, other statutes come into play. For crimes not specifically covered under the Information Technology Act (such as cheating), the adjudicating procedure and punishment as contained in the Indian Penal Code becomes applicable.

To harmonize the Information Technology Act with other national laws, supplementary statutes also were amended. For example, Section 3 of the Evidence Act was amended to include electronic records as evidence. Further, electronic records became acceptable evidentiary items under Sections 17, 34, 39, and 59 of the amended Evidence Act. Sections 65A and 65B clearly enunciated the procedure to admit electronic records as evidence, while Sections 73A and 85B made digital signatures acceptable in the courts of law. However, the Act is unable to throw any light on the evidentiary challenges and has not fine-tuned the nuances of giving evidence in cases of cybercrime.

The latest round of amendments to the Information Technology Act were implemented in the form of the Information Technology (Amendment) Act 2008. This Act amended Sections 43 (data protection), Section 43(b) (data theft), Section 66 (hacking), Section 66C (identity theft), Section 67 (protection against unauthorized access to data), Section 69 (cyberterrorism), and Section 72 (privacy and confidentiality) of the Information Technology Act 2000, all of which relate to computer crimes and cybercrime.

The Information Technology (Amendment) Act 2008 has several commendable features, particularly in terms of the government's efforts to promulgate a technology-neutral policy, although it is not beyond criticism. For example, the introduction of Section 67B that deals with child pornography is highly commendable; however, the age limit, which includes those who are legally above the age of consent,[104] may be problematic.

104 According to the Information Technology (Amendment) Act 2008, Section 67B, a child is an individual who has not completed 18 years of age.

The overall effect of the Information Technology Act and its amendment, which is the amalgamation of Internet security and regulation becoming part of India's legal framework, is the clear message that India is serious about identifying instances of cybercrime and penalizing offenders. From the perspective of e-commerce in India, the Information Technology Act has many positive aspects.

In July 2013, India released its first National Cyber Security Policy. This Policy prescribes measures for securing cyberspace and critical infrastructure of India and covers a wide range of topics, from emergency response networks, private-public partnerships to national cybersecurity issues.

The framework though comprehensive and "aspirational" has numerous lacunae. Probably as this is a policy framework, legally it is not soundly drafted. Further not only methodology but implementation of this policy also is suspect considering the manners in which in its nascent stage numerous bodies have been introduced with responsibilities for cybersecurity.

One interesting observation is that while the document does endeavour to define cybersecurity in paragraph 5 of the preamble when it refers to "cyber related incident[s] of national significance" involving "extensive damage to the information infrastructure or key assets...[threatening] lives, economy and national security," it has equated individual and business cybersecurity threat with national cyber security threat, and this collation will lead to numerous other issues of enforcement in the implementation stage.

However, a positive factor that it has taken is the advocating of "fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security". This does go along with the earlier observations that businesses must give more importance to the security of their systems.

Apart from other serious concerns with the policy, one aspect that would have required adequate focus was a framework for institutional cooperation beyond the designation of CERT-In "as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management" and the designation of the "National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country".

The Policy mentions additionally "a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles and responsibilities". What is missing is clarity with regard to roles and responsibilities of these bodies.

The Policy also does not more fully address questions of roles and responsibilities among government entities. What is further disappointing is that there is no mention of how the public and private sectors are to cooperate on cyber security information-other than oblique references to "public-private partnerships".

However, it still leaves a whole gamut of complicated and complex legal issues unexplored, as numerous areas have still not been covered, either under the Act or the various rules and regulations on IT. A prominent legislative flaw is the large number of powers vested with the investigating authorities. Other important legislative gaps are the absence of specific provisions on jurisdiction, intellectual property rights, and extent of liability.

Pakistan

Pakistan enacted the Prevention of Electronic Crime Ordinance 2007, which was amended in 2008 and 2009. Article 1 of the Ordinance states that it applies to all of Pakistan and:

> ". . . to every person who commits an offense under this Ordinance irrespective of his nationality or citizenship whatsoever or in any place outside or inside Pakistan, having detrimental effect on the security of Pakistan or its nationals or national harmony or any property or any electronic system or data located in Pakistan or any electronic system or data capable of being connected, sent to, used by or with any electronic system in Pakistan."

The Ordinance was expected to be converted into law, but this has been delayed due to lack of consensus. Critics of the proposed law claim that it threatens "freedom of speech and action, intellectual property, and the right to conduct business in a safe environment".[105]

International Conventions

European Convention on Cybercrime

When responding to the problem of cybercrime through national legal frameworks covering criminal justice, international law is a possibility. Some degree of harmonization at the international level was attempted

105 Phneah, "Pakistan Cybercrime faces delay, consensus not reached", *ZDNet* (21 November 2012), at http://www.zdnet.com/pakistan-cybercrime-bill-faces-delay-consensus-not-reached-7000007710/.

with the Council of Europe's Convention on Cybercrime, which was signed by forty-seven countries, although only thirty-one of them have ratified the convention.

Although the European Convention was designed as a regional response to computer-related crimes, it has global significance. Apart from enhancing the protocol for mutual legal assistance, the Convention provides comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data; to make production orders; to search computer systems; to seize stored computer data; to enable real-time collection of traffic data; and to intercept the content of questionable electronic data.

The European Convention also obligates signatories to criminalize a minimum list of specific offenses on which there is consensus, and thus harmonizes offenses to eliminate problems of dual criminality. Offenses that are defined by the European Convention include illegal access and interception, data or system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighboring rights. The hope was that the European Convention would be widely ratified, but this has not been the case.

Convention against Transnational Organized Crime

Another international initiative was the United Nations (UN) Convention against Transnational Organized Crime (the UN Convention).[106] This global response indirectly deals with cybercrime. Article 29 of the UN Convention expressly refers to methods for combating the misuse of computers and telecommunications networks, provisions for training and materials (especially assistance to developing countries), and places obligations on capable states.

Though dealing with cybercrime only indirectly, it has put in place international cooperation, which may be taken as an example of a potent global instrument against cybercrime, in line with Article 13.1(a) of the UN Charter, emphasizing the progressive development of international law. It includes regulations limiting the rule of dual criminality for mutual assistance purposes and introduces "enterprise" responsibility.

Article 27 of the UN Convention "deals with police-to-police cooperation and reflects the types of assistance routinely provided among

106 UN Convention against Transnational Organized Crime and Protocols Thereto.

police officials in the absence of a formal agreement and reflects international consensus on the need for close coordination between law enforcement authorities".[107] To achieve this objective, it is recommended that states promote the exchange of expert personnel, including liaison officers. Additionally, signatories are required to "make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies".[108]

In the Resolution adopted by the UN General Assembly on cyber security and the protection of critical information infrastructures,[109] the UN invited its members and all relevant international bodies to duly consider the need to protect critical information structures from possible misuse and, when necessary, to consider the need for disclosure of information to other nations.

Convention on Mutual Assistance in Criminal Matters

Parties to the European Convention on Mutual Assistance in criminal matters may call upon each other for mutual assistance in prosecuting criminal offenses that come under any signatory party's jurisdiction. The ENISA has suggested that:

> "National criminal law in conjunction with a request to the country where the attacks were identified as originating from under the European Convention on Mutual Assistance in Criminal Matters and [the] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters would be another possibility. However, given the noted inefficiency, ineffectiveness, and reluctance of nation states to cooperate in public international legal obligations in general (due to the absence of sanctions) this route would also likely yield insufficient results.
>
> Another option for management of major cybercrime incidents (which implies a degree of information sharing) is via

107 Broadhurst, "Developments in the global law enforcement of cyber-crime", 29/2 *Policing: An International Journal of Police Strategies and Management* (2006) 408, at p. 420.

108 UN Convention against Transnational Organized Crime and Protocols Thereto, Article 27(2).

109 UN General Assembly, Fifty-Eighth Session, Resolution Number 58/199 (24 January 2004).

> the legal framework governing Information Communications Technology (ICT) more generally. This might include, for example, obligations on providers of e-communication networks to provide for the security and integrity of their communications services (as detailed in Article 13a of the Revised Telecommunications Regulatory Package 2009); provisions regarding the protection of personal data (which creates a clear understanding of the terms of using data available about the incidents for the purposes of investigation and further prevention) and legal obligations governing data retention."[110]

Other International Initiatives

Lyon Group

The G8 Senior Experts Group on Transnational Organized Crime[111] has developed initiatives to combat international crime. At the Halifax Summit in 1995, G8 heads of state established a cross-disciplinary group of senior government experts (the Lyon Group) to address methods of combating transnational organized crime.

The Lyon Group issued forty recommendations aimed at increasing the efficiency of collective action against transnational organized crime via two interrelated objectives: strengthened capacity in the investigation and prosecution of high-tech crimes; and more effective regimes for crossborder cooperation in criminal matters.

Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN)[112] has provided a limited pan-Asian approach toward mutual assistance in criminal matters. It mirrors the EU approach, but has not made much progress due to the sheer cultural and economic diversity of Asia.

---

110 ENISA, *A flair for sharing — encouraging information exchange between CERTS, A study into the legal and regulatory aspects of information sharing and crossborder collaboration of national/governmental CERTs in Europe* (November 2011), at p. 34.

111 Comprising Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

112 ASEAN members comprise ten nations: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

Organization for Economic and Cultural Development

The OECD has been active in the area of cybercrime and online security, especially with regard to encryption technology, evaluating the balance between law enforcement and privacy concerns, and the means by which OECD members can coordinate encryption policies. In 1997, the OECD issued a series of guidelines addressing these issues.

In the wake of the 9/11 attacks, the OECD issued the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security in 2002. These guidelines aim to develop a "global culture of security" through advice on policies and measures to address internal and external threats such as cyber-terrorism, computer viruses, or hacking in a globally interconnected society, while preserving important societal values such as privacy and individual freedom.

Asia Pacific Economic Council

The Asia Pacific Economic Council (APEC), founded in 1989 in Canberra, consists of twenty-one members. It has increasingly been looking at a vehicle for crossborder police cooperation. APEC's work over the past several years also has evolved in a number of areas relevant to cybercrime enforcement, including the Intellectual Property Experts Group (IPEG) and the Electronic Commerce Steering Group (ECSG).The initiatives of the APEC forums have yet to evolve into fully institutionalized forms of crossborder legal cooperation.

Although the recommendations of all these groups are not legally binding, they reflect consensus among key jurisdictions on issues affecting the security of the online environment. However, if these varied responses convey anything, it is the pressing need for international regulation of cyberspace.

Future Challenges

In any international regulation or collaboration regarding cybersecurity, a pertinent issue would be the laws governing privacy and personal data protection. This challenge is not necessarily unique to any one country: the question of achieving a balance between meeting legal obligations concerning user privacy and the privacy of subscriber data versus network security obligations is a massive roadblock for most countries.

Some countries, such as the EU Member States, have burdensome laws that make information exchange on transborder cybercrime very cumbersome. Other countries have implemented specific legal protection with respect to judicial information, which will be subject to additional safeguards under applicable national laws.

For example, in Belgium, Article 8.1 of the Privacy Act contains a prohibition on the processing of personal data concerning disputes presented to courts or administrative tribunals regarding suspicions, prosecutions, or convictions relating to crimes, or regarding administrative sanctions or security measures.

A comparable rule is enshrined in Section 21 of the Italian Personal Data Protection Code. Ignoring these obligations may result in any evidence-gathering being rejected by a court as being unlawfully acquired, which undermines subsequent investigations. Thus, any international law on cybercrime may be confronted with diverging national restrictions which would need to be circumvented.

As stated earlier, India has no specific legislation dealing with privacy and data protection and/ or confidentiality. It is also to be noted that the Indian Information Technology Act has taken extraterritorial proportions and the Act has been enacted to apply for offence or contravention outside India too, by any person, irrespective of nationality, if the computer, computer system or computer network is located in India. The laws require the disclosure of information to Governmental Authorities.

However, such power cannot be abused by the Government as the Government is required to state clearly the reasons for such extraction of information and also obtain lawful orders before carrying out their duty.

A notable feature in the enactment of national laws in response to cybercrime is a general awareness of the need to implement legislative changes to address this new-age crime. It is equally clear that there is little uniformity across nations in terms of how they deal with cybercrime. In the final analysis, a nation's culture is reflected in its legislation, which is an impediment to the harmonized regulation of cybercrime. These concerns need to be addressed when creating a regulatory environment for cyberspace.

This section of the chapter has discussed the salient features of national and international responses to cybercrime. While the response from the international community is a major step in the right direction, it will require comprehensive review and substantial rework, especially as it still does not address all forms of cybercrime

and fails to adequately visualize either the methodology that cyber-savvy criminals may use to circumvent national data protection laws or the mechanisms that enable real-time response to a cybercrime. The corporate sector worldwide needs to safeguard itself against the perpetration of these new forms of cybercrime and, to this end, nations must rise above national politics to provide the necessary support.

Conclusion

> "It is a very familiar truth that regulation is national and business is international and business is more international across cyberspace."
>
> — Sir Steve Robson

When extending the rule of law to cyberspace, which remains a work in progress, a critical step is the creation of a trustworthy environment for people and businesses. Organizations today must first defend their own systems and information from attack, with reliance on effective law enforcement being secondary. This aspect assumes greater priority as Internet criminals keep getting more "professional", trying to run their affairs like major business enterprises to improve their skills and become more profitable.

A report published by Symantec details a startling trend of the inventive ways criminals are figuring out ways to make money online.[113] The most recent is how cybercriminals are not just making away with all available customer data, but are actually crunching numbers to figure whether the credit card numbers being sold in underground chat rooms are valid. This startling trend emphasizes that responses are unable to keep pace with the acts of cybercriminals. The evolving cyber-environment impacts all aspects of society and the economy and presents a complex set of challenges for lawmakers.

The Internet is constantly changing, and it is impossible to foresee the nature and possible scope of all of the current and future opportunities for cybercriminals. Lawmakers at every level of government will need to watch and study the nature of human interactions with and

113 Symantec, "Report on the Underground Economy: July 07–June 08" (November 2008).

via computers and networks, adapting laws to deal with the most pressing risks as they become apparent.

Cybercrime's potential for enormous cost to the economy, society, and national defense demands constant vigilance and ongoing efforts to develop feasible solutions to address new problems as they emerge. Appropriate steps need to be taken to constantly revamp laws and to educate law enforcers and legislators to recognize the changing face of crime.

Self-protection is the prime tool. Organizations should focus on implementing cyber-security plans that address people, processes, and technology issues. Organizations need to commit the necessary resources to educate employees on security practices; develop systematic plans for the handling of sensitive data, records, and transactions; and incorporate robust security technology into their infrastructure.

However, the "technological 'fix'"[114] would only be temporary, "as the rapid global expansion of the Internet renders it highly vulnerable to a lawless frontier-style Internet culture",[115] providing an environment for criminal opportunities that cannot be addressed merely by this technological fix. In this scenario, every player — public law enforcement, the corporate sector, or private enforcers — has a noteworthy role in the concerted response to cybercrime. This is because the Internet is no ordinary crime scene, but a medium that allows offenders to route attacks through various jurisdictions with impunity and the assurance of anonymity; this situation can be countered only by a collaborative crossborder and international policing response.

The international community has responded with a number of mechanisms to facilitate crossborder cooperation in criminal matters, including in the investigation and prosecution of cybercrime. Although this approach is commendable, it does question the independent capability of nations to regulate the social and economic order within their territories.

In this context, it would be apt to mention what the criminologist Sheptycki calls a "transnational state system". In this system, new configurations of players and power will emerge, and transnational organizations (both legitimate and criminal) will flourish due to "the

114 Broadhurst, "Developments in the global law enforcement of cyber-crime", 29/2 *Policing: An International Journal of Police Strategies and Management* (2006) 408, at p. 414.

115 Broadhurst, "Developments in the global law enforcement of cyber-crime", 29/2 *Policing: An International Journal of Police Strategies and Management* (2006) 408, at p. 414.

diminishing sway of the state".[116] In the context of cybercrime, this would mean "governance without governments".[117] Therefore, to develop an effective solution to address cybercrime, an international response must be supplemented with public awareness, strong industrial support, and public-private partnerships.

116 Lizee, *Peace, Power, and Resistance in Cambodia: Global Governance and the Failure of International Conflict Resolution* (2000), at p. 165.

117 Rosenau, *Goverance Without Government: Order and Change in World Politics* (1992).