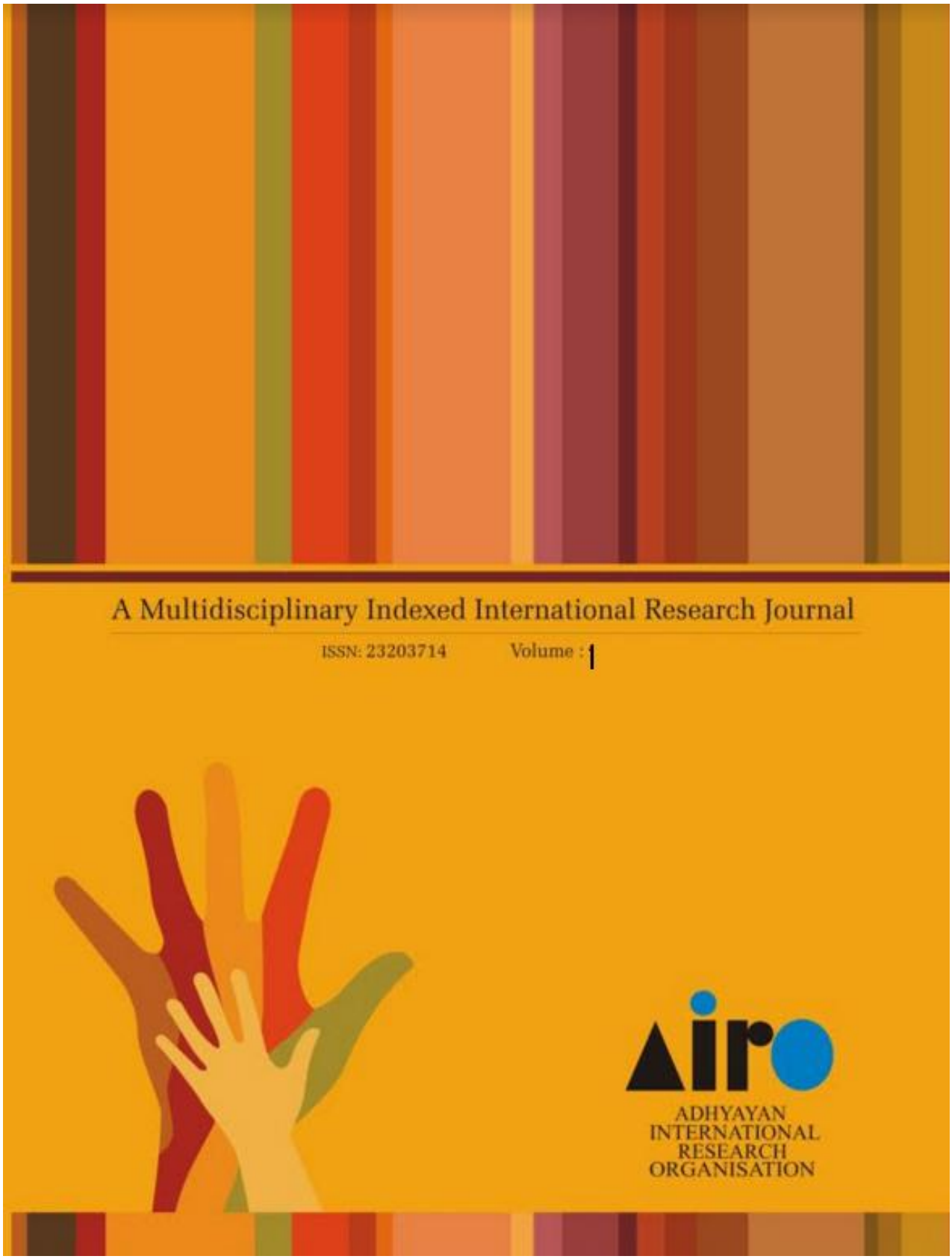
A Multidisciplinary Indexed International Research Journal
ISSN: 23203714 Volume : 1
Airo
ADHYAYAN
INTERNATIONAL
RESEARCH
ORGANISATION

The Survey Study on Maintaining of Data Privacy and Security Through Cyber Law

RAVINDER SINGH (Advocate)
BA LLB(Hons)
VILLAGE -JAGDISHPURA,
DISTT. KAITHAL (HARYANA)-136027
INDIA

Abstract

This study discusses the issues of cyber crime and what is being done to prevent it. Cyber criminals take advantages of vulnerabilities by using viruses, bots, etc to cause damage and/or maybe steal information. There are ways that this can be minimized by being aware of what the problems are. There are many pro ble- ms but common ones are discussed. Not can these problems be solved on an individual or organi -zation level but also on a global level. This study will look at what cyber crime is and three topics that discuss the problems with cyber crime and how to prevent it. The information age has made the public and private sectors of modern society increasingly dependent on technology, in which telecommunications play a vital role.Over the past thirty years, developed nations' transit from the industrial era to the new information age has enabled them to develop the nascent technology and produce ever greater quality in standards and value. The past decades have also delivered many opportunities in which the flaws and faults of the system have been exploited and mended, by hackers and legitimate users alike. The new society has engendered new types of crimes, such as phishing and botnets, and facilitated the commission of old crimes, for example the violation of intellectual property rights, with new technology facilitating breaches of copyright in music, films and software.

BACKGROUND OF PROPOSED WORK

Cyberlaw is a term that encapsulates the legal issues related to the use of communicative , transactional , and distributive aspects of networked information devices and technologies. It is less a distinct field of law in the way that property or contract are , as it is a domain

covering many areas of law and regulation. Some leading topics include intellectual property , privacy , freedom of expression and jurisdiction.

Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear , but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such , a single transaction may involve the laws of at least three jurisdictions:

1) the laws of the state / nation in which the user resides.

2) The laws of the state/ nation that apply where the server hosting the transaction is located.

3) The laws of the state/nation which apply to the person or business with whom the transaction takes place.

So a user in one of the United States conducting a transaction with another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is one of the aspect of state sovereignty and it refers to jurisdicial , legislative and administrative competence. Although , jurisdiction is an aspect of sovereignty , it is not coexistensive with it. The laws of a nation may have extraterritorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform , international jurisdictional law of universal application , and such questions are generally a matter of conflict of laws , particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.

Another major problem of cyber law lies in whether to treat the Internet as if it were physical space (and thus subject to a given jurisdiction’s law) or to act as if the Internet is a world into itself (and therefore free of such restraints). Those who favor the latter view often feel that

government should leave the Internet community to self – regulate . John Perry Barlow , for example , has addressed the governments of the world and staed , "Where there are real conflicts , where there are wrongs , we will identify them and address them by our means". We are forming our own social contract . This governance will arise according to the conditions of our world , not yours. Our world is different . A more balanced alternative is the Declaration of Cybersecession : "Human beings possess a mind , which they are absolutely free to inhabit with no legal constraints". Human civilization is developing its own (collective) mind . All we want is to be free to inhabit it with no legal constraints. Since you make sure we can not harm you , you have no ethical right to intrude our lives. So stop interuding ! " Other scholars argue for more of a compromise between the two nations , such as Lawrence Lessig' s argument that "The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once".

Computer crime issues have become high – profile , particularly those surrounding hacking , copyright infringement through warez , child grooming . There are also problems of privacy when confidential information is lost , lawfully or otherwise.

Computer crime encompass a broad range of potentially illegal activities. Generally, however , it may be divided into one of two types of categories:

crimes that target computer networks or devices directly.

1) crimes facilitated by computer networks or devices.

The primary target of which is independent of the computer network or device.

Examples of crimes that primarily target computer networks or devices would include

- Malware (malicious code)
- Denial_of_service attacks
- Computer viruses.

Examples of crimes that merely target computer networks or devices would include

- Cyber stalking

- Fraud and identify theft
- Phishing scams
- Information warfare

A common example is when a person starts to steal informations from sites, or cause damage to , a computer or computer network. This can be entirely virtual in that the information only exists in the digital form , and the damage , while real , has no physical consequence other than the machine ceases to function . In some legal systems , intangible property can not be stolen and the damage must be visible, e.g. as resulting from a blow from a hammer. Where human-centric terminology is used for crimes relying on natural language skills and innate gullibility , definitions have to be modified to ensure that fraudulent behavior remains criminal no matter how it is committed.

A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is excellent device for record keeping , particularly given the power to encrypt the data. If this evidence can be obtained and decrypted , it can be of great value to criminal investigators.

Specific crime computers are

- Spam
- Fraud
- Obsence or offensive content
- Harassment
- Drug trafficking
- Cyberterrorism etc.

THE RESEARCH PLAN

The information age has made the public and private sectors of modern society increasingly dependent on technology , in which telecommunications play a vital role. Over the past thity years, developed nations ‘transit from the industrial era to the new information age has enabled them to develop the nascent technology and produce ever greater quality in standards and value . The past decades have also produced many opportunities in which the flaws and faults of the system have been exploited and mended , by hackers and legitimate users alike. The new society has engendered new types of crimes , such as phishing and botnets , and facilitated the commission of old crimes , such as the violation of intellectual property rights , with new

technology facilitating breaches of copyright in music , films and software . As society grows ever more reliant on these technologies, so does the concern for security, especially in cyberspace. The emancipation of Internet has leaped ahead of the jurisdictional system, but authorities have taken heed and the wheels of the legal machine have stared turning. The difficulty, however, has been that the internet-based society has no physical boundaries and thus much traffic escapes national supremacy. Therefore, looking to an international framework would immensely facilitate regulation in this area. The European Union has enabled harmonized implementation of regulation on electronic commerce through directives in almost all European countries, with non member countries aligning themselves with the EU movement. As founding father to the internet, the US has both important knowledge and experience in the legal field of cybersecurity, with significant influence in the area. Developing countries are jumping onto the bandwagon. However, many of those countries are coming straight from an agriculture society and, with the technological know-how of developed nations , are starting to create the infrastructure needed to support a technology – based society. The problem is nonetheless that many have neither the expertise nor the experience to deal with the legal and policy issues necessary. In order to promote the development and use of technologies and the internet, security must be assured, especially for e-commerce business. The International Telecommunication Union's Development Bureau mandate is to assist such developing countries to acquire the knowledge and develop the founding blocks for an information society. One of these founding blocks is cybersecurity. In order to compile general but adequate guidelines on such a vast area , research on existing legislation in developing countries and multinational frameworks is examined on both a content level , encompassing intellectual property , digital rights management and anti circumvention, and a network security level , incorporating areas such as technical standards and integrity of data, with a close look at the security of information infrastructure (privacy and data protection) and computer-related crimes (spamming and identity theft) , among other topics.

RESEARCH METHODOLOGY

In this work, we will use simple type of survey in different types of offices and concerning people who relate with cyber

working. The survey will be both types either mock or through internet. Mostly we will use internet because in India not every normal men familiar to computer working or cyber working not even any cyber crime normally seen in surround.

ANALYSIS

The global digital economy depends on resilient and interdependent information systems, together with reliable and accurate information. These together form the information infrastructure which enables organizations and businesses to enjoy the provision of timely information, services and control systems. The dependence on these systems that deliver services to UK business and society is greater than it has ever been and is set to increase in the coming years. As an information system matures it typically converges with other systems to add richer functionality. This is driven by a demand for: increased agility, virtualization, outsourcing and interconnectedness. But, it also adds additional layers of complexity, interdependency an external uncertainty. The end result is usually an unplanned 'system of systems' where functionality overrides resilience. Moreover, the challenges of our increasing dependency on, and use of, enormous volumes of information necessitates a review of traditional approaches 106 to information infrastructure and risk management. Innovative technical solutions must be developed to enable systems to be mapped, monitored and managed – and to mitigate risks. The Technology Strategy Board is working closely with other stakeholders in the area of information security, such as CPNI, CESG (the UK Government's communicationselectronics security group), the Ministry of Defence, Central Sponsor for Information Assurance, and the Research Councils. This is in order to develop a range of projects which, as well as contributing to the UK's national security goals, also represent business opportunities for the UK within the new markets being created in information infrastructure protection, with potential for significant wealth creation in the UK. EPSRC may contribute to projects which involve academic partners in developing and applying the tools and techniques of complexity science in information infrastructure protection. Additional funding may also be provided by the ESRC for proposals which include high quality academic work. Projects should make real progress towards meeting the targets set out in the UK Government's

National Information Assurance Strategy and mitigating electronic risks cited in the National Risk Register. These take the form of clear and effective risk management; provision of the right 'tools' for organizations to protect themselves; protection of critical infrastructures from electronic attack; and enhanced public, commercial, 107 and industrial confidence in the UK's ability to manage andprotect information. This competition will address innovative solutions for information infrastructure protection tools, technologies and methodologies in both the public and private sector markets. This includes the development of real-time or near real-time predictive models for information infrastructure protection with particular emphasis on interdependency analysis, 'system of systems' and supply chains. In particular, we welcome proposals that will accelerate deployment of the technology and place emphasis on the development of the supply chain, system integration and issues around how people will use it. The high level challenges to be addressed include:

- Increased understanding and subsequent improved management of complex interdependent information infrastructures
- The formation or expansion of existing business resilience tools
- The provision of risk assessment services supporting the above. Competition proposals will address these challenges by focusing on one or more of the following: 108
- Development of models focused on real-world practical applications for SMEs, large enterprises or national infrastructures and the use of 'systems dynamics' type approaches, to enable business-relevant security planning and management.
- Systems developments or enhancements that include data capture, high security data segregation and where the integration of existing technologies and standards are encouraged. Projects which will demonstrate full systems operating at appropriate scales and in appropriate environments are welcome, For example, healthcare/ assisted living, intelligent transport, and high value systems and services.
- Small scoping studies into the development of certification, codes of practice and standards that will accelerate deployment will be

considered if included as part of a larger project and on the basis that the results will be made publicly available.

- Real-time or near real-time disaster recovery and business continuity models and simulations with 'what-if' planning capabilities.
- Knowledge transfer activities that bring atypical ideas and consortia together are encouraged, and should be included in project proposals as a separate work package. 109

All proposals must explain how the work will help in positioning the UK in the global market and against other global innovation leaders in the area. Projects should be mindful of how they might contribute to the European Commission ICT Objective 1.4 Secure, Dependable and Trusted Infrastructures and Objective 1.7 Critical Infrastructure Protection. Proposals must include quantitative development targets for the project outputs, together with (where appropriate) the relevant performance and cost targets for the ultimate device, application or service. We recognize the close synergies between the areas of physical and information infrastructure protection and welcome proposals that cover both areas, however emphasis must be given to information infrastructure protection. Project partners who bring large real-world datasets which could be used for modeling complex information infrastructure risk scenarios are also welcomed. Innovative projects are particularly encouraged which build on the transfer of analytical tools and techniques from other domains such as safety critical engineering, probabilistic mathematical and agent based modeling, network theory, transport infrastructure simulation, sociological interactions, financial risk modeling, drug discovery, consumer complexity and business continuity and resilience.

INTEGRITY OF DATA: DATA SECURITY, PRIVACY AND CONFIDENTIALITY

Data integrity is an assurance that unauthorized parties areprevented from modifying data. Participants in distributed data exchange include primary data sources, intermediate sources, and end users. Integrity benefits both primary sources (who need to make sure data attributed to them is not modified) and end users (who need guarantees that the data they use has not been tampered with). After publishing data, a source can never directly prevent the

modification of data by recipients, since they are autonomous and not regulated by a trusted system. However it is possible to annotate data with virtually un-forgeable evidence of its authenticity that can be verified by any recipient. To do this, data sources need techniques which allow them to annotate data with claims of authenticity. These claims should be difficult to forge or transfer, and must be carried along with the data as it is exchanged and transformed. In addition, users should be able to derive useful integrity guarantees from query results containing these claims. The ultimate goal, therefore, is to develop a framework to

(1) allow authors to annotate data with evidence of authorship,

(2) allow recipients to query, restructure, and integrate this data while propagating the evidence, and

(3) enable recipients to derive useful conclusions about the authenticity of the data they receive. To accomplish these goals we propose two related integrity annotations which are 111 applied to data to represent useful claims of origin authenticity. Data integrity is defined to mean data that has not been altered in an unauthorized manner. This includes both privacy and confidentiality in its scope. Privacy is the right of individuals to control or influence what information related to them may be disclosed. Confidentiality relates to the protection against unauthorized disclosure of data content. In this chapter we introduce the issues around protecting information about patients and related data sent via the

Internet. We begin by reviewing three concepts necessary to any discussion about data security in a healthcare environment: privacy, confidentiality, and consent.

'Privacy' is a vaguely defined term that, in an online context, includes the right of an individual to:

- Determine what information is collected about them and how it is used.
- Sometimes we are not aware what data are being collected about us (e.g. via 'cookies' on a Web site see Glossary) or how it may be used. Registering with a Web site (i.e. giving your name, e-mail address, medical registration number, etc.), for example, may 112 enable that site to keep track of what you—a readily identifiable individual—view or spend online.

- Such information could be passed on to third parties. Some sites publish 'privacy policies' in an attempt to inform users and reduce the chances of patients or healthcare professionals placing their privacy at risk.
- Access information held about them and know that it is accurate and safe.
- Anonymity (e.g. not having your Web-browsing habits tracked).

Send and receive e-mail messages or other data (e.g. credit card numbers) that will not be intercepted or read by persons other than the intended recipient(s). Encryption (discussed below) is one way of ensuring this. Privacy is one of the fundamental tenets of democracy and it has been entrenched within the international human rights framework from the Bill of the Rights to the many regional instruments. The laws relating to privacy, however, are peculiar. For example, within the European Convention on Human Rights (ECHR), there is a provision for a limited protection of family and private life. The European Court of Human Rights has been very meticulous in interpreting this within stringent lines and has often afforded Member States 113 a wide margin of appreciation. The ECHR nevertheless permits the State to derogate from the right of private and family life in certain cases. Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information. Confidentiality ensures the protection of component from unauthorized access throughout an organization's\ information architecture, which extends to all component directly associated with the architecture's applications, component stores, communication links and/or processes. Integrity ensures that component, services, and other controlled resources are not altered and/or destroyed in an unauthorized manner. Integrity based controls provide safeguards against accidental, unauthorized, or malicious actions that could result in the

alteration of security protection mechanisms, security classification levels, addressing or routing information, and/or audit information. Because of increasing information sharing and 114 the cost of securing information, it is important to classify information correctly. Under-classification of sensitive information can have serious consequences. Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.115

The ethical duty of confidentiality is defined by the British Medical Association as ‘the principle of keeping secure and secret from others, information given by or about an\ individual in the course of a professional relationship’. In the UK the legal duty of confidentiality is underpinned by the Data Protection Act (1998), regulating the processing of information (‘data’) that could lead to the identification of individuals—including its collection, storage, and disclosure. To ensure the protection of confidentiality in an electronic environment the General Medical Council (GMC) recommends that doctors should:

- Make appropriate security arrangements for the storage and transmission of personal information.
- Obtain and record professional advice given prior to connecting to a network.

- Ensure that equipment, such as computers, is in a secure area.
- Note that Internet e-mail can be intercepted.

Conclusion

The problems with cyber crime; how to improve efforts of prevention; and the response to cyber crime are what help us to look at the dangers of cyber space. The Internet is a very powerful tool and effective means of communication but it is vulnerable just like anything else. The way to protect it for now is for everyone to be smart and follow preventive measures; individuals, institutions, and government alike should all follow these measures. We have seen the actions of the government and what bots and viruses are capable of and it is important that security measures be implemented. In response to these issues there

have been requests from the WGIG as well as congress to implement more standards and laws to help minimize cyber crime. In response to some problems there have been efforts by some nations by arresting individuals and The Lack of Attention in the Prevention of Cyber crime and How to Improve it 27 groups that commit cyber crimes like the ones discussed earlier. If everyone does their part, not only will they be safer but it will be setting an example for others as well as making it more difficult for hackers to cause damage. As suggested earlier in this study, cyber security and cyber crime control are related but nevertheless different concepts. The same applies to the respective strategies. They pursue different objectives and comprise different measures. A cyber security strategy does not address the full range of cybercrime, and a cybercrime strategy not the full range of cyber security issues. At the same time, they are intersecting and interrelated and complement each other. Credibility in a country's e-commerce activities heavily relies on the validity and authenticity of electronic contractual relationships. If legislative enforcement cannot be guaranteed, then contractual relations will be undermined. Electronic contracts and electronic evidence have become an accepted format in the courts and recognized by governments in many developed countries. With the use of encryption technologies, electronic signatures have become binding on contractual documents. Cryptographic techniques such as the Public Key Infrastructure have become one of the most reliable technologies to date for

authenticating individuals. This form of electronic signature has become internationally recognized, with involvement by the United Nations with the UNCITRAL Model Law on Electronic Signatures of 2001. Encryption technologies also help secure confidentiality of communication, for contractual and non contractual communication alike. Privacy, however, has become another matter. Although encryption technologies may be applied to protect users' privacy, not all data about a user will be under his control.

BIBLIOGRAPHY

1. Digital Music Usage and DRM : Results from a European Consumer Survey by Nicole Dufft , Andreas Stiehler, Danny Vogeley , Thorsten Wichmann, May 24 , 2005.

2. The UCLA Online Institute for Cyberspace Law and Policy. A & M Records v Napster : MP3 file Sharing Disputes Continues in the Aftermath of Recent Court Rulings ,

3. Electronic Frontier Foundation: Unintended Consequences: Five Years Under the DMCA, September 24, 2003.

4. Critique of the Proposed U.K. Implementation of EU Copyright Directive , by Julian T. J. Midgley , Campaign for Digital Rights

5. National Institute of Standards and Technology , Computer Security : Recommendation for Key Management – Part 1 : General , by Elaine Barker , William Burr , William Polk and Miles Smid. NIST Special publication 800-57 , April 2005

6. Explanatory Notes to Electronic Communications Act 2000.

7. Study for the European Commision – DG Information Society: The Legal and Market Aspects of Electronic signatures, by Jos Dumortier , Stefan Kelm , Hans Nilsson , Georgia Skouma and Patrick Van Eecke.

8. Interdisciplinary Center for Law and Information Technology , Katholike University Leuven.