ISSN 2278-8808
SJIF 2015: 5.403
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

# A STUDU OF SECURITY OF INFORMATION INFRASTRUCTURE FOR CYBER-CRIME

**Kadam Sandeep Uddhavrao[1] & Piyush Pandey[2], Ph. D.**

***Abstract***

*Today are utilizing the opportunities offered by recent advances in information and communications technologies (ICTs) as vital business tools than ever before. SMEs are adopting innovative business operations, user-friendly products and services, and customer centric strategies. Unfortunately, a myriad of challenges threaten the SMEs, especially the issues of confidentiality, integrity and availability (CIA) vulnerabilities, as those weaknesses are exploited by threat agents. Whenever they are attacked, SMEs are adversely affected by way of loss of revenues, loss of customer confidence, loss of investor confidence, loss of resources, loss of credibility, cost related to dealing with the security breaches, cost of mitigation as well as possible business closure, etc. SMEs were surveyed and strategically interviewed on various cyber-security and business metrics. The elicited experts' opinions were used to model the risk function, using neuro-fuzzy techniques, that combines the human inference style and linguistic expressions of fuzzy systems with the learning and parallel processing capabilities of neural networks to analyze the cyber-security vulnerability assessment (CSVA) model.*

***Keywords:*** *Security, Information, Infrastructure, Cyber-Crime, SMEs, ICTs, challenges, resources, techniques, etc.*



## Introduction:

The Technology Strategy Board is working closely with other stakeholders in the area of information security, such as CPNI, CESG (the UK Government's communications-electronics 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 [2-4]. 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, and industrial confidence in the UK's ability to manage and protect information.

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 and 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 to information infrastructure and risk management [1]. Innovative technical solutions must be developed to enable systems to be mapped, monitored and managed – and to mitigate risks.

**Review of literature:**

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. This competition will address innovative solutions for information infrastructure protection tools, technologies and methodologies in both the public and private sector markets [5-8]. 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:

- The provision of risk assessment services supporting the above. Competition proposals will address these challenges by focusing on one or more of the following:
- 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.
- Increased understanding and subsequent improved management of complex interdependent information infrastructures

- The formation or expansion of existing business resilience tools

**Measuring and Tracking Cybercrime:** According to one expert, "the threat of cybercrime is largely being ignored, and that [threat] is greater than most people believe." However, comprehensive data on cybercrime incidents and their impact are not available, and without exact numbers on the current scope and prevalence of cyber-crime, it is difficult to evaluate the magnitude of the threats posed by cyber criminals [10]. There are a number of issues that have prevented the accurate measurement and tracking of cyber-crime. Firstly, the lack of a clear definition of what constitutes cybercrime presents a barrier to tracking comprehensive cybercrime data. This is compounded by the facts that (1) the range of cyber-crimes is ever expanding in the globalized world and (2) cyber-crimes often overlap with more traditional, non-cyber-crimes—thus providing challenges in gauging the true scope of cyber-crime. Various agencies and researchers have put forth estimates of the prevalence and costs of cybercrime. However, these often measure a different range of criminal activities and base estimates on differing victim populations.

**Investigation of Computer Related Crime:** Computer crime investigation and are evolving so that they are affected by many external factors, such as continued advancements in technology, societal issues, and legal issues. Computer security practitioners must be aware of the myriad technological and legal issues that affect systems and users, including issues dealing with investigations and enforcement. Incidents of computer related crime and telecommunications fraud have increased dramatically over the past decade. However, because of the esoteric nature of this crime, there have been very few prosecutions and even fewer convictions. The new technology that has allowed for the advancement and automation of many business processes has also opened the door to many new forms of computer abuse. Although some of these system attacks merely use contemporary methods to commit older, more familiar types of crime, others involve the use of completely new forms of criminal activity that has evolved along with the technology. Computer crime investigations are also evolving. They are sciences affected by many external factors, such as continued advancements in technology, societal issues, and legal issues. Many gray areas need to be sorted out and tested through the courts. Until then, the system attackers will have an advantage, and computer abuse will continue to increase.

**Integrity of Data: Data Security, Privacy and Confidentiality:** Data integrity is an assurance that unauthorized parties are prevented 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 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. The issues around protecting information about patients and related data sent via the Internet [9]. We begin by reviewing three concepts necessary to any discussion about data security in a healthcare environment: privacy, confidentiality, and consent.

**Conclusion**

Globally, SMEs have been defined in a number of different ways. Some definitions involve revenues, capital and staff strength. Interestingly, SMEs in developing countries are characterized by uncertain revenues. Coupled with that, most developing economies have fluctuating currencies. These challenges create uncertainties with any definitions involving monetary value; that is, the set of target SMEs population would vary with exchange rates. Cognizant of the above, the only common denominator is the number of employees. So this study defined SMEs based solely on staff strength, which is also consistent with the norms applied in the case study countries. At least, this approach enhances the generalization of findings to some reasonable extent. Having so defined the SMEs in developing economies, the study focused on those who have embraced the information and communications technology (ICT) and the surge in doing business in the cyber-space. They use the Internet to communicate with business stakeholders, they order and receive requests for supplies via web

portals, they store critical corporate information on computers and storage media, etc. In essence, SMEs in developing economies also stay competitive via the web presence and utilize the Internet resources in their business operations. New and innovative security challenges confront the SMEs on a daily basis, thus exploiting most "zero-day" vulnerabilities. SMEs are faced with lots of uncertainties. This results in various losses to the SMEs, even with the possibility of business closure. SMEs ought to ensure that their networks and systems are both available and protected. SMEs ought to safeguard their mission critical assets through the effective use of policies, education, training and awareness of their end-users, as well as deployment of appropriate technology solutions.

**References:**

*Sharma, Kunal, Amarjeet Singh &VedPrakash, "SMEs & Cyber-security Threats in e-Commerce," vol. 39, no. 5-6, pp. 1-49, 2009.*

*Dhillon, G. & J. Backhouse, "Information System Security Management in the New Millenium," Communications of the ACM, vol. 43, no. 7, 2000.*

*D. Parker, "Toward a New Framework for Information Security," in The Computer Security Handbook, 4th ed., New York, John Wiley & sons, 2002.*

*D. Denning, "Cyber-Security as an Emergent Infrastructure," in Bombs & Bandwidth: The Emerging Relationship between IT & Security, The New Press, 2003.*

*I. Perfilieva, "Fuzzy Function: Theoretical and Practical Point of View," in EUSFLAT, Aix-les-Bains, France, 2011.*

*L. Zadeh, "The Concept of a Liinguistic Variable and Its Application to Approximate Reasoning," Information Sciences, vol. 8, pp. 199-257, 1975.*

*Moller, Bernd & Uwe Reuter, Uncertainty Forecasting in Engineering, Berlin: Springer, 2007.*

*B. M. Ayyub, Elicitation of Expert Opinions for Uncertainty & Risks, CRC Press LLC, 2001.*

*S. Bavisi, "Penetration Testing," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 369-382.*

*J. Walker, "Internet Security," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 93-117.*