INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS AND MANAGEMENT

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Business Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email addresses: infoijrcm@gmail.com or info@ijrcm.org.in.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF** _____.

(e.g. Computer/IT/Finance/Marketing/HRM/General Management/other, please specify).

DEAR SIR/MADAM

Please find my submission of manuscript titled '_____' for possible publication in your journal.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication anywhere.

I affirm that all author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if our/my manuscript is accepted, I/We agree to comply with the formalities as given on the website of journal & you are free to publish our contribution to any of your journals.

NAME OF CORRESPONDING AUTHOR:

Designation:

Affiliation with full address & Pin Code:

Residential address with Pin Code:

Mobile Number (s):

Landline Number (s):

E-mail Address:

Alternate E-mail Address:

2. **INTRODUCTION:** Manuscript must be in British English prepared on a standard A4 size paper setting. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of the every page.
3. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.
4. **AUTHOR NAME(S) & AFFILIATIONS:** The author (s) full name, designation, affiliation (s), address, mobile/landline numbers, and email/alternate email address should be in italic & 11-point Calibri Font. It must be centered underneath the title.
5. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para.
6. **KEYWORDS:** Abstract must be followed by list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.
7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.
9. **MAIN TEXT:** The main text should be in a 8 point Calibri Font, single spaced and justified.
10. **FIGURES &TABLES:** These should be simple, centered, separately numbered & self explained, and titles must be above the tables/figures. Sources of data should be mentioned below the table/figure. It should be ensured that the tables/figures are referred to from the main text.
11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.
12. **REFERENCES:** The list of all references should be alphabetically arranged. It must be single spaced, and at the end of the manuscript. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio," Ohio State University.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITE

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Economic and Political Weekly, Viewed on July 05, 2011 http://epw.in/user/viewabstract.jsp

THE SUSTAINABILITY OF ICT ECONOMY DEVELOPMENT

KEVIN LOCK-TENG, LOW
ASSOCIATE PROFESSOR
FACULTY OF ACCOUNTANCY AND MANAGEMENT
UTAR UNIVERSITY
MALAYSIA

ABSTRACT

A green technoeconomic paradigm (green TEP), based on emerging information and communication technologies (ICT), has been proposed to address the sustainability issues in developing nations. An ICT driven green TEP would enable developing nations to conform to stricter environmental regulations while pursuing rapid economic development. However, cyber crime perpetrated by sophisticated cyber criminals, a potential pitfall in ICT based systems, has received little attention in these emerging global ICT networks. This paper addressed the potential danger in ICT driven growth models, in developing nations that have limited resources and knowledge to protect their interests. These findings also suggested that the benefits of "green ICTs" come at a potential security cost. ICT had been hailed as the system that could effectively improve the economic well-being of developing nations, improving productivity while reducing costs, wastes and environmental degradation. However, the sophistication of these systems had led to a new world of knowledge "haves" and "have-nots". This chasm enabled knowledgeable cyber criminals to tap into confidential databases and abuse the IT systems for personal gain while developing nations had little means to counter-act. Thus, the necessary knowledge base should be created by prioritising the development of a core human capital base. This core base would train a wider human capital base in implementing, maintaining, policing and protecting the networked electronic systems. The key objectives of such developmental initiatives should be able to prepare a pool of knowledge workers who are experts in critical ICT security and green ICT issues and solutions. The accounting profession's expertise in preventing and detecting corporate fraud can become the basis for developing cyber accountants - experts in establishing and monitoring cyber security in large, networked systems.

KEYWORDS

Sustainability, information and communications technology (ICT), green TEP, developing nations, free trade agreements (FTAs), regional trade agreements (RTAs), cyber crime

INTRODUCTION

Economic growth consumes natural resources and emanates wastes, contributing to resource scarcity and pollution. It is possible for excessive economic growth rates to generate wastes at levels that jeopardise nature's ability to sustain life on this planet (Gan, 2004; Gandhi et al. 2005). A focus on short-term profits causes businesses to regard environmental protection measures as impediments to firm performance (Rojšek, 2001). As such, developing nations may strategically employ looser environmental regulations to lure business investments from developing nations, pursuing foreign investments and quick economic growth at the expense of global environmental sustainability.

Pollution is considered an unavoidable by-product of economic growth (Roarty, 1997). If developing nations with growing populations follow the consumption driven growth models of Western countries in pursuing economic growth, there will be immense pressures on the environment. Even if the populations of developing nations stabilise in a few decades, these growth models would lead to consumption levels that surpass global sustainability levels by as much as fifty percent (Daniels, 2005).

However, rapidly developing internet and communication technologies (ICT) offer an alternate means to pursue economic growth. This alternate model offers environmentally sustainable growth prospects.

A key insight in addressing environmental issues related to economic growth in developing nations is that the environment is affected by pollution associated with escalating production processes (Valaskakis, 1979), rather than economic growth per se. Daniels (2005) contemplates a green technoeconomic paradigm (green TEP) that promotes economic growth while keeping the associated environmental problems in check. He considers "the successful adoption of materials and energy-saving technologies appropriate for the less-capital intensive, smaller-scale and more labour-intensive context of lower income nations" (Daniels, 2005, p. 458). Information and communication technology offers a means for poorer nations to improve their economic conditions (Gani and Clemes, 2006). The term "green ICT" looks into using information and communication technology in a manner that has minimal negative impact on the environment, where "green ICT" is defined as environmentally friendly internet and communication technologies.

Currently, ICT plays an important role in the development of regional and national economies. For instance, a number of free trade agreements that involve ASEAN nations promote the establishment of ICT systems, to improve productivity. However, this exuberance in regarding ICT as a solution for improving the economic welfare of poorer nations, and the emerging notion of a "green ICT" that offers a means to pursue environmental protection and economic development simultaneously, overlook a major flaw in ICT based systems: ICT based fraud and security of sensitive and confidential information.

In Malaysia, KPMG's 2008 survey on fraud indicated that seventy-seven percent of respondents felt that computer and information systems comprised a potential security risk (KPMG, 2008). This figure shot up to eighty-five percent in KPMG's 2009 survey (KPMG, 2009). The costs of fraud are substantial. Kranacher and Stern (2004) estimate that fraud costs every company in Asia around a tenth of sales.

This paper explored security issues that comprise a weakness in ICT based systems. Lax security in globally networked systems enables sophisticated cyber criminals to tap these systems for personal gain. Cyber crime includes unauthorised access, modification, use, copying and destruction of material stored and processed within the ICT systems; theft of identities, records, computer time and resources via the ICT infrastructure; conspiring to utilise available computer technology to commit criminal activities and illegally getting access to confidential, sensitive information via corporate and government based computer systems. For instance, important documents may be altered without the knowledge of the authorities, such as entry permits for contraband goods that may be otherwise denied.

This paper also examined a number of regional trade agreements (RTAs) and concluded that there was little formal consideration of ICT security issues in these agreements. It then explored measures to deal with ICT based fraud and unauthorised access to sensitive data and processes in publicly listed firms in Malaysia, by means of a survey of the experiences and perceptions of users of computer systems. The findings of this survey indicated that while fraud is not uncommon in ICT based systems and users were aware of this danger, surprisingly limited measures were in place to control computer based fraud. In essence, these findings suggested a need for strategic planning of the training and development of human capital, to effectively prevent and contain fraud in ICT driven environments. In particular, large-scale multi-national systems, such as those envisioned in multilateral FTAs to ease the flow of information and data across borders, as well as upcoming green ICT systems that intend to uplift developing economies while protecting the global environment, are vulnerable to criminal cyber attacks. These global ICT networks offer cyber criminals unprecedented opportunities for profit. In some cases, entire economies could be paralysed due to criminal cyber attacks.

SURVEY OF LITERATURE

ICT systems are poised to become the next technoeconomic paradigm (TEP) that drives economic growth. However, unlike preceding TEPs, ICT has the potential of protecting the environment while promoting economic growth. The weakness of ICT based TEP is poor security in protecting confidential information and processes. This section also discusses this security issue that can derail economic growth.

Technoeconomic paradigms (TEPs)

TEPs theorise that waves of technological innovations have enabled the production of new products and services that are in demand across large areas of the economy in the West. The resulting bursts in economic activity drove productivity, profit and broad economic growth in developed Western nations. Five main TEP waves have been identified, with the likelihood of an emerging sixth wave, called a "green TEP" (Freeman and Peréz, 1988; Berry, 1997; Freeman, 1992, 1997; Daniels, 2004). These waves are summarised in Table 1.

TABLE 1: FIVE TEP WAVES WITH A POTENTIAL SIXTH TEP

Wave	Period	Driving technological innovations
TEP 1	1770s – 1840s	Cotton and iron
TEP 2	1840s - 1880s	Coal fuelled transport, factories,
TEP 3	1880s - 1940s	Steel, transportation based on railways, Electricity
TEP 4	1940s – 1990s	Oil fuelled energy, mass production
TEP 5	1990s – present	Micro-electronics, ICT, lean production and just-in-time systems
TEP 6	Potential wave	Green ICT, environmentally friendly economic growth

The first five waves of TEPS did not pay specific attention to environmental issues. Consequently, Western nations developed during these periods at the cost of environmental pollution and degradation. Today, ICT offers a means for lower income nations to improve their economic well-being (Gani and Clemes, 2006) while containing environmental pollution and degradation. A green TEP focusing on driving economic growth with carefully planned, environmentally friendly ICT would help low income nations to realise sustainable economic growth without damaging the environment (Daniels, 2005). Such green (environmentally friendly) ICT systems would be able to promote sustainable growth in developing nations while helping to protect the global environment.

Information and Communication Technologies (ICTs)

ICT is widely regarded as a tool for promoting socio-economic development in developing nations (Gani and Clemes, 2006; Mutula and Brakel, 2007). Advances in ICT, including the internet, hand phones, personal computers, broadband connections and wireless networks, allow information to be disseminated cheaply and swiftly across wide, geographically dispersed audiences. The easy access to pertinent information drives improvements in many areas, including healthcare, education, hygiene and sanitation, which in turn improve the quality of life (Gani and Clemes, 2006) and set the stage for improvement in social and economic conditions.

A number of RTAs[1] promote ICT, viewing this technology as a vehicle for automating certain tasks and creating paperless environments that help to facilitate trade. Trade facilitation is defined as "the simplification and harmonisation of international trade procedures including the activities, practices and formalities involved in collecting, presenting, communicating and processing data and other information required for the movement of information in international trade (OECD, 2005)".

A comparison of several regional trade agreements (Table 2) indicates the importance placed on ICT in trade facilitation.

TABLE 2: A COMPARISON OF SELECTED RTAS IN THE ASIA-PACIFIC REGION

Trade Agreement	ASEAN/AFTA [2]	APEC[3]	SAARC/SAFTA [4]
Members	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Phillipines, Singapore, Thailand, Vietnam	Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua-New Guinea, Peru, Philippines, Russia, Singapore, South Korea, Taiwan, Thailand, USA, Vietnam	Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, Sri Lanka
Integration	Goal: Integrated single market by 2020	Trade, investment liberalisation through high quality, multilateral regional and bilateral trade agreements. Goals: free, open trade and investments by 2010 in developed and by 2020 in developing economies	Goal: Free trade area by 2016. Non-developed nations (India, Pakistan, Sri Lanka) to phase out tariffs by 2009; least developed states given till 2016
ICT initiatives	Use of ICT, ASEAN e-customs	Common data elements, paperless trading, electronic certificates	Automated customs clearance procedures and electronic data interchange
Exchange and handling of information	Use state of the art technology compliant with UN/EDIFACT (Vision 2020)	Use ICT to facilitate movement of goods and people; remove barriers to and promote e-commerce	Implement automated customs clearance procedures and electronic data interchange
Cooperation/assistance: Training and human resource development	Training to promote regional uniformity, coordinated action, equivalent treatment and homogeneity (Vision 2020)	Workshops on customs related issues	Identify national training institutions and training instructors to undertake training programs in customs administration
Cooperation/assistance: Technical assistance (TA)	TA to promote equal levels of development amongst customs administration so as to enhance regional efficiency, effectiveness and uniformity (Vision 2020)	TA regarding evaluation and implementation of trade facilitation measures, assessment of trade facilitation costs, WTO customs valuation	TA regarding customs valuation, and tariff classification
Cooperation/assistance: Capacity building (CB)	No specific details	CB regarding document examination, development, implementation of standards and legal infrastructure	CB regarding customs valuation, and tariff classification
Cooperation/assistance: Cooperative measures	Mutual assistance to enhance the effectiveness of customs compliance and to control and reduce smuggling (Vision 2020)	Cooperative initiative on regulatory reform	Promotion of bilateral or multilateral agreements on customs cooperation to prevent and investigate customs offences

(SOURCE: WILLE, 2006)

AFTA, APEC and SAFTA were chosen for this analysis, from the larger universe of regional trade agreements, RTAs, (that includes, for example, the Pacific Agreement on Closer Economic Relations, PACER and the Australia-Singapore Free Trade Agreement, AS-FTA) because they embrace nations that are widely dispersed across the globe, and hence illustrate the extensiveness of the impact of the ICT security risk. This security risk is accentuated by the fact that there is little formal consideration of this issue in the RTAs. Security risk associated with ICT systems that offer borderless flow of sensitive and confidential information,

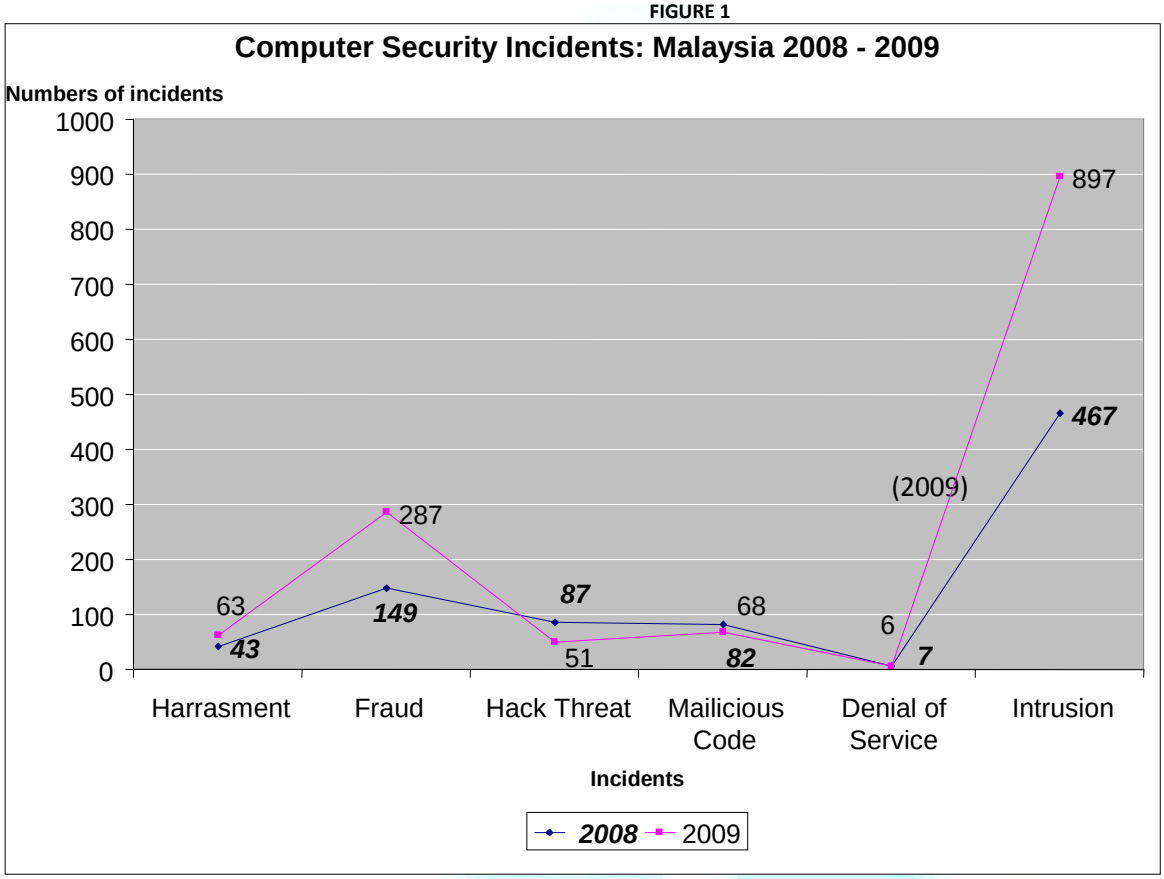
[1] These RTAs are part of the bilateral and multilateral FTAs that are being established all over the world to promote and facilitate global trade.
[2] ASEAN (Association of Southeast Asian Nations) Free Trade Agreement – AFTA
[3] Asia-Pacific Economic Cooperation (APEC)
[4] (South Asian Association for Regional Cooperation) Agreement on South Asian Free Trade Area - SAFTA

especially over widely dispersed areas, includes the potential to cripple economic activity over large portions of the globe. For instance, APEC's membership ranges from the US to Malaysia to New Zealand. A cyber attack that cripples the interconnected computer systems of APEC, or even one that surreptitiously harvests confidential information, would pose serious consequences for these nations that are spread all over the world, and potentially become a major global issue. For instance, an unanticipated denial of service (DOS) attack (Samudhram, 2000) could paralyse the computers, and halt all processes and trade between the nations for a sizeable length of time.

EMPIRICAL STUDY

Computer fraud in not uncommon in Malaysia. Figure 1 showed the statistics on computer fraud in Malaysia for the years 2008 and 2009.

FIGURE 1



Source: Malaysia Computer Emergency Response Team (2009)

The following empirical study was conducted with the objective of examining the preparedness of the Malaysian public listed companies in addressing computer fraud, where computer fraud is taken to include the following:

a. Unauthorized use, access, modification, copying and destruction of software or data.
b. Theft of money by altering computer records or the theft of computer time.
c. Destruction of computer hardware.
d. Conspiracy to use computer resources to commit a felony.
e. Intent to illegally obtain information or property via computers.

This study also explored the assessments of computer security risk, prioritised budgetary allocations to address computer fraud, frequency of checks on the security of computer systems, incidences of computer fraud, policies to manage risk, persons relied on to prevent computer fraud risk and follow-up actions taken following computer frauds.

The study was based on survey questionnaires. In January, 2010, anonymous questionnaires were sent, via post and email, to 200 companies that were randomly selected from the population of firms listed on Bursa Malaysia (formerly Kuala Lumpur Stock Exchange, KLSE). Of the returned questionnaires, sixty five (32.5%) were complete, and suitable for this study. Thus, the following analysis was based on these 65 questionnaires.

Overview

Overall, the sample of sixty five responses mainly represents firms that employ 100 to 200 workers. One firm reported employee numbers of 4000 to 5000 while two reported employing over 5000 people.

Risk assessment

TABLE 3: ASSESSMENT OF COMPUTER FRAUD RISK

	Yes		No		Don't know		Total	%
	Count	%	Count	%	Count	%		
1. The company performs risk assessment on computer security	38	58.5	24	36.9	3	4.6	65	100
2. The company has prioritized budget allocation for risk assessment on computer security	23	35.4	11	16.9	31	47.7	65	100

The findings regarding the assessment of computer risks by the firms were presented in Table 3. Only slightly over half of the respondents (58.5%) had performed qualitative and/or quantitative risk assessments on the security of their corporate computer systems. Over 40% did not perform such assessments. Around 5% were not aware of whether their companies performed risk assessments on computer security. About a third of the respondents (23 firms, or 35.4%) indicated that their firms had prioritised budget allocations for assessment of computer security risk, while almost 17% indicated otherwise. Almost half of the

correspondents (47.7%) did not know whether their firms provided prioritised budget allocations for this purpose. Considering the serious implications of uncontained computer fraud for commercial firms, these findings indicate a somewhat lackadaisical attitude towards computer security.
In addition to providing prioritised budgetary allocations, the depth of a firm's commitment to fight computer fraud is further indicated by the amounts allocated. Table 4 showed the findings regarding the allocated amounts.

Prioritised budgetary allocations

TABLE 4: ANALYSIS OF PRIORITIZED BUDGET ALLOCATION

Budget allocation	Count	%
Less than RM1,000	5	21.74
RM 1,001 - RM50,000	2	8.70
RM 50,001 – RM100,000	2	8.70
More than RM100,000	14	60.87
TOTAL	**23**	**100.00**

Table 4 indicated that when firms do provide budgetary allocations for addressing computer fraud, the amount is often ample. Within this group of 23 firms, around 60% allocate over RM100, 000. However, there are also a number of firms that allocate mere token amounts for assessing computer security risk. For instance, over a fifth of these firms (5 firms, or 21.74%) allocate less than RM1, 000. Discarding these 5 firms that allocate token amounts, which is indicative of a weak commitment towards addressing computer fraud, we find that in the total sample of 65 firms, only 18 (about 28%) appear to provide sizeable amounts for assessing computer fraud risk. These findings support the earlier conclusions from the analysis of RTAs that limited strategic attention is paid to computer security in organisational planning.

Table 5 provided further evidence in support of these conclusions

TABLE 5: FREQUENCY OF COMPUTER SECURITY SYSTEM CHECKS

Frequency of Computer Security System Checks	Count	Percentage (%)
Very Frequent	8	12.3
Frequent	22	33.9
Seldom	25	38.5
Rarely	9	13.8
Never	1	1.5
TOTAL	**65**	**100.0**

Table 5 indicated that 53.8% of the companies surveyed conduct computer security system checks very infrequently (includes those who check their systems rarely, seldom and never). Furthermore, only about 46% of the respondents state that their computer security is checked frequently or very frequently.
The firms' commitment to fighting computer fraud may be further explored by examining if they have special teams (e.g. internal divisions or internal audit departments) to detect or minimise computer fraud. Table 6 indicated the findings related to this area.

Computer fraud detection teams

Table 6: The presence of computer fraud detection teams

	Yes		No		Don't know		Total	%
	Count	%	Count	%	Count	%		
1. The company has a special division to detect or minimize fraud	18	27.7	47	72.3	0	0	65	100
2. The company has internal audit departments that play active roles in detecting computer fraud	33	50.8	29	44.6	3	4.6	65	100

Table 6 indicated that only about a quarter of the respondents' (27.7 %) firms had special divisions to detect and minimise fraud. Internal audit departments played active roles in this area in about half (50.8%) of the companies. The findings appear to indicate an important role for internal audit[5] teams, particularly in comparison with IT teams, in containing computer fraud. The findings depicted in Table 7, which explored the persons most relied upon to detect computer fraud, provide further evidence in support of this conclusion.
Persons most relied upon for detecting computer fraud

TABLE 7: PERSONS RELIED MOST TO DETECT AND PREVENT COMPUTER FRAUD IN COMPANIES

Person Relied Most to Prevent and Detect Computer Fraud	Count	%
External Independent Auditors	4	6.2
Internal Auditors	31	47.7
Accounts	3	4.6
Board of Directors	1	1.5
MIS Team	9	13.8
IT Team	17	26.2
Others	0	0.0
TOTAL	**65**	**100.0**

Table 7 showed that in almost half of the firms (47.7%), the persons most relied upon for detecting and preventing computer fraud are the internal auditors. The external auditors take up this role in another 6.2 percent of firms. Taken together, these findings indicate that auditors are seen as very important persons in addressing computer fraud. In contrast, the IT and MIS teams appear to play very important roles in detecting and preventing fraud in only 26.2 and 13.8 percent of the firms, respectively. Considering that auditors are generally seen as providers of reliable information, the perception that they are generally the persons most relied upon to detect and prevent computer fraud is not surprising. These findings also indicated that the responsibility for prevention and detection of computer fraud should vest with the auditing and accounting departments, since ensuring the reliability of corporate information is part of their normal duties.

[5] The internal audit teams are assumed to be part of the accounting/finance function, rather than an IT or MIS function. The data in Table 7, that shows Internal Audit and IT/MIS teams as separate categories, gives validity to this assumption.

It might be possible that the limited interest in computer security at the firm level could be perhaps due to low levels of computer security incidents in these organisations. However, the findings shown in Table 8 indicated that this explanation did not hold, because computer security incidences were not uncommon in these firms.

Incidences of computer fraud in the surveyed firms

TABLE 8: INCIDENTS OF COMPUTER FRAUD AND ASSOCIATED LOSSES

	Yes		No		Don't know		Total	%
	Count	%	Count	%	Count	%		
1. Company experienced computer fraud cases within the last 12 months	37	56.9	26	40	2	3.1	65	100
2. Number of separate computer fraud incidents that occurred within the last 12 months:								
1-10	21	56.8					37	100
11-20	11	29.7						
More than 20	5	13.5						
3. The company's direct and indirect loss amount due to computer fraud incidents								
Less than RM10,000	8	21.6					37	100
RM10,000-RM50,000	16	43.2						
RM50,000-RM100,000	7	19.0						
RM100,000-RM250,000	4	10.8						
More than RM250,000	2	5.4						

Over half of the respondents' firms (37 firms, or 56.9 %) experienced incidences of computer fraud within the previous 12 months. A majority of these 37 firms (about 57%) had experienced 1 to 10 incidences of computer fraud within the last year. About 30% had experienced 11 to 20 incidences. Almost 14% experienced over 20 incidences of computer fraud. Most of the firms (43.2 %) that had experienced computer fraud estimated their direct and indirect losses to amount to RM10, 000 to RM50, 000. About a fifth (21.6%) reported losses below RM10, 000. Only two firms (about 5 %) reported losses above RM250, 000. The data in Table 8 indicated that incidences of computer fraud do occur in firms. Almost 80 percent of the respondents who had experienced incidences of computer fraud estimated the associated direct and indirect losses to be above RM10, 000.

DISCUSSION OF RESULTS

Tables 3 to 8 presented the findings that the publicly listed companies in Malaysia did not place much emphasis on computer security, although they did experience computer security attacks and the direct and indirect losses from such attacks were not trivial. These conclusions were further supported by the findings that only about a third of the respondents (35.4 %) provided prioritized budget allocations for assessment of computer security risk (Table 3). Nevertheless, firms that did provide budgetary allocations often set aside generous sums (Table 4).

In essence, the findings of this empirical study concurred with the trends indicated by the examination of RTAs. In both cases limited attention appeared to be paid to computer security, which essentially involves ICT security. There was a lack of urgency in addressing this problem, which could potentially blow up into a major issue with global repercussions.

The following section discusses policy recommendations and strategic procedures to address computer security.

COMPUTER SECURITY ISSUES, IMPLICATIONS AND RECOMMENDATIONS

Many RTAs provide for the establishment and networking of ICT systems that enables data and information to flow seamlessly across borders while commercial firms adopt ICT to improve productivity and profitability. These developments naturally lead to greater and greater reliance on ICT systems at regional, bilateral and multilateral levels as well as within corporations. However, the issue of ICT security has attracted little attention, which is a flaw that could have major repercussions. Generally, top level strategists and executives appear to pay very limited attention to ICT security, leaving the task to technical teams rather than comprehensively addressing the issue in strategic planning. Bakari et al (2007) opines that most CEOs seem to view ICT security as "a new phenomena and managers perceive ICT security as a technical problem rather than a potential business issue". These perceptions of top level corporate managers and planners[6] regarding ICT systems helps to explain the lack of emphasis on ICT security revealed in the examination of RTAs (Table 2) and the empirical investigation (Tables 3 to 8). Nevertheless, a lack of attention to ICT security can potentially lead to major problems, leading to everything from debilitating denial of service attack to theft of proprietary information, sabotage and financial fraud (Richmond, 2003). As such, national and international level initiatives aimed at building an awareness of the dangers of lax ICT security, and efforts to build capacity to prevent, detect, contain and overcome computer fraud, are important for long-term global economic stability.

Moreover, insecure ICT systems allow knowledgeable cyber criminals to tap into confidential databases and abuse the IT systems for personal gain while developing nations, at both the firm and governmental levels, have little means to counter-act. This may lead to vast problems that would be difficult to contain, from the loss of valuable data to an ineffectiveness of control procedures. For instance, important documents may be altered without the knowledge of the authorities, such as entry permits for contraband goods that may be otherwise denied. However, the necessary knowledge base can be created by prioritising the development of a core human capital base. This core base will then train a wider human capital base in implementing, maintaining, policing and protecting the networked electronic systems.

The education of high level strategy planners (such as CEOs, CFOs and government based policy makers) regarding the importance of ICT security is important for addressing the underlying ICT security issue. This has to be followed through with the development of sufficient human capital, namely, trained manpower, to detect and prevent ICT fraud.

Both developed and developing countries are today plagued by a shortage of skilled manpower in ICT (Mutula and Brakel, 2007). A key strategy to overcome this shortage would be strategic plans for training human resources in ICT, with particular emphasis on ICT security. A well trained workforce would prove instrumental in maintaining the overall security in ICT driven economies, and adequately address this potentially critical drawback of the green ICT concept. Regional and national level policies should drive human capital development in this area, to prepare a pool of knowledge workers who can support the ICT systems of public and private organisations. Public and private organisations, including universities and multinational corporations (MNCs), should work together, pooling resources, to develop the necessary manpower.

[6] Assuming that these perceptions, of top level corporate managers, are also reflective of the outlook of the top level policy planners involved in drafting RTAs

FIGURE 2: HUMAN CAPITAL DEVELOPMENT COST-BENEFIT FRAMEWORK
HUMAN RESOURCE DEVELOPMENT FOR ESTABLISHING ICT SECURITY AT REGIONAL AND NATIONAL LEVELS

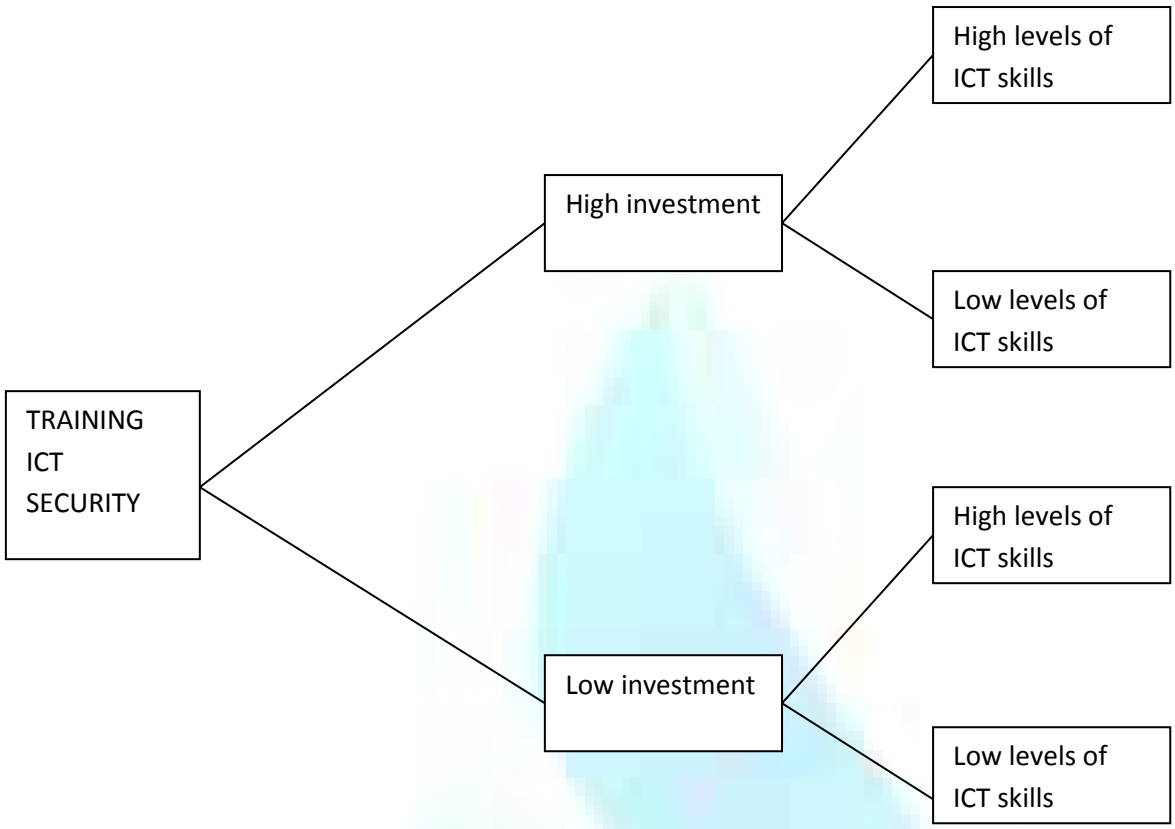


Figure 2 indicates that sometimes high levels of investment in ICT training may result in high levels of skills in containing ICT related fraud, while in other cases similar training results in limited development of ICT skills. On the other hand, it might also be possible to plan the human capital development programmes such that low investment levels in ICT training to provide high levels of skills in addressing ICT based issues. Finally, it is also likely for low levels of investment in human capital development to result in low levels of the anticipated ICT based skills.

Policies that aim to develop human capital will only be effective when the investment results in high levels of ICT skills. In particular, strategies that enable low levels of investmcfent to give rise to high levels of ICT skills are particularly important for developing nations with limited resources. This could be realised through cooperative, regional training arrangements. Developing nations may, for instance, identify expert trainers from abroad and bring them over to their own nations for limited periods to train local knowledge workers. Regional groups of developing nations could conduct such development programmes, with trainees travelling inexpensively within their regions to undertake the necessary training. This could further be supported with web based learning technologies that are able to train large numbers while controlling costs. The burden of funding could be reduced by sharing expenses amongst several nations, in addition to support from international bodies such as the United Nations Development Program. Once a nucleus of local talent has been trained, these groups could in turn train the others in the nation, with on-going web based support from abroad, to deepen the national skill base.

In the planning stage, each human resource development strategy for establishing nation and region wide ICT skills must compared with the Human Capital Development Cost- Benefit Framework. Programs that provide high levels of ICT skills should be pursued while those that do not offer such benefits should be reconsidered and re-engineered so they are able to provide meaningful results.

The training in ICT fraud prevention, detection and containment would include instruction in ensuring data integrity and reliability. Professional accountants, particularly auditors, are experts in detecting fraud and establishing and evaluating controls that ensure data integrity and reliability. Furthermore, forensic accountants are skilled in dealing with fraudulent activities. Indeed, the findings of our empirical research indicate that accountants appear to be the persons most relied upon to detect computer fraud in listed firms (Table 7). As such, the advent of the cyber age and the proliferation of ICT systems offer an opportunity for the accounting profession to develop cyber-auditors and the cyber-forensic accountants, with a speciality in computer fraud prevention, detection and containment. At the firm level, Bakari et al (2007) suggest teams that include three IT specialists (representing hardware, software and networking areas), a legal officer, an internal auditor and members of operational departments to address companywide IT security problems. Cyber auditors and forensic accountants will be well positioned to lead such teams, serving as a bridge between the technical ICT teams and the operational team members. Accountants will be able to establish, maintain and review measures and controls to contain ICT fraud at the level of detail that works effectively in major corporations. As such, they would be instrumental in setting up ICT fraud detection and prevention systems that are able to work effectively.

The manpower development initiatives should be followed through with additional initiatives to contain and mitigate ICT security risks, such as establishing an ICT security team composed of personnel from several functional areas. This team, which can be established at regional, national and firm levels, should then undertake the following tasks:

i.) Report on ICT-based security risks and implications
ii.) Document current ICT status and tasks required to address security risks
iii.) Assess current risks levels, analyse the impact of suggested corrective or preventive measures in risk levels
iv.) Work out contingency plans in case of security breaches
v.) Establish policies, protocols and procedures to prevent security breaches.

This team would need to constantly communicate the importance of addressing ICT based risks to the top management and planners, to create an awareness of the importance of this issue and maintain the support of the top management.

SUMMARY AND CONCLUSIONS

The traditional TEPs that have driven economic growth and prosperity in Western nations are associated with environmental pollution and degradation. The emergence of green TEP paradigms, driven by the ideology of green ICT possibilities, offers the promise of environmentally friendly economic growth models for

developing nations. Today, ICT is embraced openly by major international agencies, including the United Nations, as a means to accelerate economic growth (Wood, 2003).

This paper brings attention to a potential pitfall of ICT systems that has gained little notice, despite the increasing reliance on ICT for economic development and improving profits. Developing nations may pursue a green TEP, based on the concept of an environmentally friendly ICT (green ICT), to improve their economic well-being without degrading the environment. However, they need to be cognizant of cyber crimes and ICT security issues that could pose a great danger, and potentially bring their economies to a standstill. An examination of RTAs as well as survey of listed firms in Malaysia indicates that very little attention in being paid to ICT security.

Developing nations should undertake human capital development policies in ICT based on the Human Capital Cost-Benefit Framework, to create a pool of trained knowledge workers who can help to maintain ICT security. The accounting profession is particularly well placed today to develop cyber-auditors and cyber-forensic accountants, who can serve as specialists in maintaining data integrity and reliability in ICT based systems.

Multifunctional ICT security teams should be set up at regional, national and firm levels to advice planners and policy makers on sound procedures and strategies to address the ICT security risk.

Proper attention to this ICT risk will enable developing economies to pursue environmentally friendly economic growth (green TEP based on green ICT) while containing the ICT security risks. This will enable the pursuit of sustainable, long-term economic growth that will benefit all nations.

REFERENCES

Bakari, J.K., et al. (2007).“Bridging the gap between general management and technicians – A case study on ICT security in a developing country”, *Computers and Security,* Vol. 26, pp. 44 – 55.

Berry, B. (1997). “Long waves and geography in the 21st century”, *Futures*, Vol. 29, No. 4, pp. 301 – 10.

Daniels, P.L. (2005). “Technology revolutions and social development: Prospects for a green technoeconomic paradigm in lower income countries”, *International Journal of Social Economics,* Vol. 32, No. 5, pp. 454 – 482.

Freeman, C. (1992). *The Economics of Hope,* Pinter Publishers, New York.

Freeman, C. (1997). “The political economy of the long wave”, in Tylecote, A. and van der Straaten, J. (Eds), *Environment, Technology and economic growth: The challenge to sustainable development,* Edward Elgar, Cheltenham.

Freeman, C. and Peréz, C. (1988). “Structural crises of adjustment, business cycles and investment behaviour”, in Dosi, G. et al, *Technical change and economic theory,* Pinter Publishers, London.

Gandhi, N.M.D, et al. (2006). “Green productivity indexing: A practical step toward integrating environmental performance into corporate performance”, *International Journal of Productivity and Performance Management,* Vol. 55, No. 7, pp. 594 – 606.

Gani, A. and Clemes, M.D. (2006). “Information and communications technology: a non-income influence on economic well being”, *International Journal of Social Economics*, Vol. 33, No. 5, pp. 649 – 663.

Kranacher, M.J. and Stern, L. (2004). “Enhancing fraud detection through education”, The CPA Journal, November, pp. 66-67.

KPMG (2008), *Fraud Survey: 2008 Report,* KPMG Forensic, Malaysia.

KPMG (2009), *Fraud Survey: 2009 Report,* KPMG Forensic, Malaysia.

Kranacher, M.J. and Stern, L. (2004). “Enhancing Fraud detection through education”, The CPA Journal, November, pp. 66 – 67.

Low, L. T. K. and W.C., Poon (2008). The Utilisation of Fuzzy Logic in Corporate Governance Assessment in Business Economics. International of Corporate Governance, US. Vol. 1 No 2. Inderscience.

Low, L. T. K. and Samudhram, A. (2008). “Valuing Human Resources – from the costing perspective”. *Journal of Intellectual Capital*, UK. Vol 9. No 4.

Malaysia Computer Emergency Response Bulletin (2009). www.jpm.gov.my

Mutula, S. M. and Brakel, P.V. (2007). “ICT skills readiness for the emerging digital economy among small businesses in emerging countries”, *Library Hi Tech,* Vol. 25, No. 2, pp. 231 – 245.

OECD, (2005). “Policy brief: The costs and benefits of trade facilitation”, The Organisation for Economic Cooperation and Development, October, Paris.

Richmond, R. (2003). “How to find your weak spots”, *The Wall Street Journal,* September 29th, p. R3

Roarty, M. (1997), “Greening business in a market economy”, European Business Review, Vol. 97, No. 5, p. 244.

Rojšek, I, (2001). “From red to green: towards the environmental management in the country in transition”, *Journal of Business Ethics*, Vol. 33, No. 1, pp. 37 – 50.

Samudhram, A. (2000). “Guarding vital data from security flaws”, *Computimes*, New Straits Times, Malaysia, January, 13th, p. 22.

Valaskakis, K. (1979). *The conserver society: A workable alternative for the future*, Harper and Row, New York, NY.

Wille, P. (2006). “A comparative analysis of trade facilitation in selected regional and bilateral trade agreements”, ARTNeT Working Paper Series No. 17, Institute for International Business, Economics and Law, University of Adelaide.

Wood, C.M., (2003). “Marketing and e-commerce as tools of development in the Asia-Pacific region: a dual path”, *International Marketing Review,* Vol. 21, No. 3, pp. 310 – 320.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, Economics & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mails i.e. **infoijrcm@gmail.com** or **info@ijrcm.org.in** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator