African Journal of Business Management Vol. 5(15), pp. 6138-6149, 4 August, 2011
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM10.529
ISSN 1993-8233 ©2011 Academic Journals

Full Length Research Paper

Sustainable economic development: A perspective from ICT loops in developing nations

Kevin Lock-Teng Low[1]*, Chee Seong Lim[1] and Ananda Samudhram[2]

[1]Faculty of Accountancy and Management, Universiti Tunku Abdul Rahman, Lot PT 21144, Jalan Sungai Long, Bandar Sungai Long, Cheras, 43000, Kajang, Selangor Darul Ehsan, Malaysia.
[2]School of Business, Monash University Sunway Campus, Malaysia.

Accepted 6 May, 2011

A green technoeconomic paradigm (TEP), based on emerging information and communication technologies (ICT), has been proposed as a basis for feasible models for sustained, environmentally friendly economic growth in developing nations. There has been very little discussion of cyber security, which is a major shortcoming in such models. Given the borderless world that such an ICT based paradigm promotes, the pursuit of these ICT based models opens doors to cyber security issues of an unprecedented scale that could potentially paralyse global commerce. This paper explores such cyber security problems. Firstly, it explores regional trade agreements (RTAs) that have immense global spread, and finds that little attention is paid to formally addressing cyber security within the RTAs. An empirical study indicates that reported cyber security issues are spiking in developing nations within the RTAs examined, while there are no such spikes in a developed nation in the same RTA. A second empirical study indicates little attention being paid to cyber security issues in private enterprises, with accountants being the first to detect cyber incidents in many cases. Based on these findings, some policy recommendations are offered for addressing cyber security issues that are particularly suitable for resource strapped developing economies.

Key words: 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),

*Corresponding author. E-mail: lowlt@utar.edu.my, niveklow@gmail.com. Tel: +6013 – 3886686. Fax: +603 – 90197062.

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). 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 explores 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 explores security issues associated with ICT based systems at three levels: multinational, national and private firms within a developing nation. At the multinational level, a number of regional trade agreements (RTAs) are examined. This examination finds little formal consideration of ICT security issues in these multinational agreements. It then considers two empirical studies. The first empirical study (empirical study 1) observes reported cyber security incidents in developing and developed nations. The second empirical study (empirical study 2) explores cyber security issues at the level of private firms in a developing nation. These studies are elaborated as follows:

Empirical study 1 considers reported cyber security incidents in two developing[1] economies (Malaysia and India) as well as a developed economy (Australia). Malaysia (a developing nation) and Australia (a developed nation) share an RTA, which is, APEC (Table 2). This study finds that the numbers of reported cyber security incidents have risen sharply in the developing nations in recent years. In contrast, no sharp rises are found in the developed nation. As such, these findings call for greater collaborative efforts among all nations to contain cyber fraud that could have regional and global repercussions. Considering that cyber security incidents that are not properly contained have the potential to cripple the world's economy, just like a global financial crisis, this paper suggests that global measures, akin to the Basle Committee's work in global finance and banking, are timely and necessary in the arena of cyber security. Such measures should include international standards and best practices and should comprise of tight collaboration involving both developed and developing nations.

Empirical study 2 explores measures that 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 indicate that while fraud is not uncommon in ICT based systems and users seem to be aware of this danger, surprisingly limited measures seem to be 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 in developing nations, 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 emerging 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 malice and profit. In some cases, entire economies could be paralysed due to criminal cyber attacks. As such, all developed and developing nations, especially those that are digitally linked via emerging.

[1] These nations have been selected to observe the trend of cyber security incidents between a developing nation (Malaysia) and a developed nation (Australia) within the same RTA (APEC, as indicated in Table 2), as well as to compare the trend of cyber security incidents amongst two developing nations (India and Malaysia) that have strong commitments to the ICT platform. The results indicate an upward spike in reported cyber security incidents in the developing nations, despite membership in an RTA that includes developed nations and ICT based initiatives.

RTAs, need to become involved in policing their borderless worlds, to prevent potentially economically crippling cross-border cyber attacks in the future

SURVEY OF LITERATURE

ICT systems are poised to become the next techno-economic 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 discusses past TEPs and places the ICT based TEP within the extant TEP literature. Further discussion considers the manifestation of this theoretical ICT based TEP in practice, that is, the embracing of this TEP in current RTAs, in the form of various ICT initiatives. The empirical studies, delve into related cyber security issues, at the levels of nations and private firms. These empirical studies indicate the manifestation of the cyber security issues in practice, and indicate that the rising numbers of reported cyber security incidents in developing nations is a cause for concern that needs to be addressed at international levels, perhaps, via a global body.

Technoeconomic paradigms (TEPs)

TEPs theorise that waves off 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, 2005). These waves are summarised in Table 1.

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 socioeconomic development in developing nations (Gani and Clemes, 2006; Mutula and Brakel, 2007). Advances in ICT, including the internet, hand phones, personal com-puters, 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 improve-ment in social and economic conditions.

A number of RTAs[2] 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. 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, 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 1, discussed further, indicates that the reported cyber security incidents are rising sharply in developing nations. These sharp rises indicate the rising cyber security exposures of these nations, which could provide gateways for affecting the cyber security of developed nations via interconnected digital systems established by the various ICT initiatives within emerging RTAs.

[2]These RTAs are part of the bilateral and multilateral FTAs that are being established all over the world to promote and facilitate global trade.

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 system
TEP 6	Potential wave	Green ICT, environmentally friendly economic growth

Table 2. A comparison of selected RTAs in the Asia-Pacific Region (Wille, 2006).

Trade agreement	ASEAN/AFTA	APEC	SAARC/SAFTA
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

METHODS

Empirical study 1: Reported security incidents in developing nations

This empirical study explores the reported security incidents in developing nations, where such data is reported, and, hence, available. The first two nations covered in empirical study 1, which are, Malaysia and India, have several common characteristics. Firstly, they are part of some of the RTAs indicated in Table 2. As such, security incidents in these nations would translate to cyber security concerns that could potentially affect, via interconnected networks, to the rest of the nations in the RTAs. Secondly, both of these nations are developing countries. As such, they deal with emerging ICT systems, while grappling with issues of sufficient financing and expertise. Finally, as indicated in Figures 1 and 2, all of them have experienced a steady growth in the number of security incidents, particularly in recent years. This trend is compared with the trend of reported incidents of a developed economy, such as, Australia, in Figure 3.

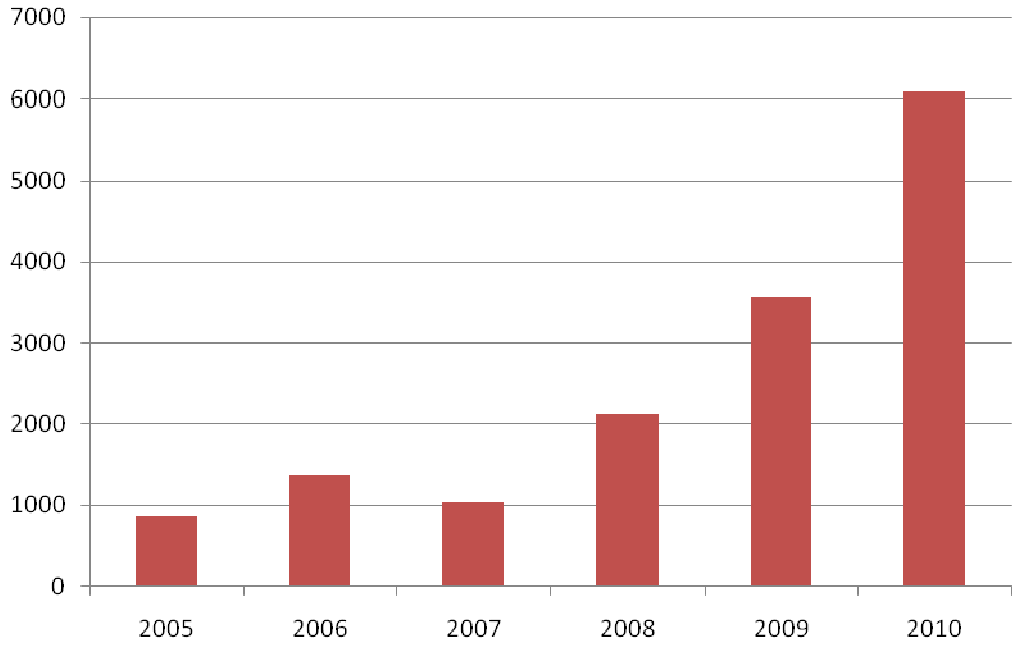

Figure 1. Number of cyber security incidents in Malaysia. Source: Malaysia computer emergency response team year 2010: estimated by extrapolating January to May 2010 data.

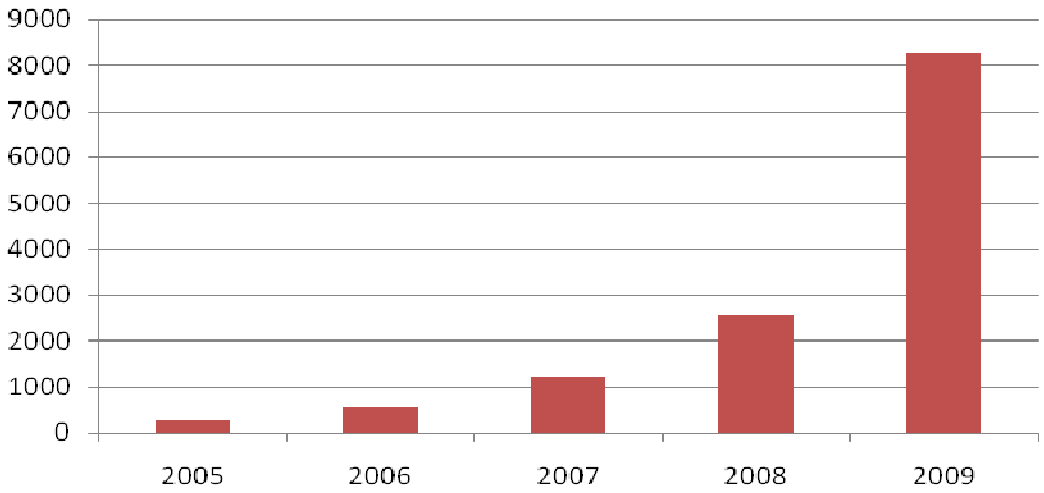

Figure 2. Number of cyber security incidents in India; source: Asia-Pacific computer emergency response team annual report (2009).

It is interesting to note the steep rise in ICT security incidents in the developing nations after 2007 (Figures 1 and 2). In contrast, Figure 3 indicates a relatively gentle rise in reported security incidents in Australia. In short, the developing nations indicate steep rises in cyber security incidences while the developed nation (Australia, which is in the APEC RTA, together with Malaysia) indicates a much slower rate of increase in the number of reported cyber incidents. Ideally, very tight and close collaboration in assessing and addressing various ICT based security incidents amongst the various nations in the RTAs indicated in Table 2, particularly between the more ICT savvy developed nations and the emerging developing nations, could indicate a similar tapering off of ICT based security incidents in both developing and developed nations. However, what is actually being observed is a sharply rising growth trend in developing nation (Figure 1) that contrasts with the gentler trend line of similar incidents in the developed nation (Figure 3). These trends point to a need for in-depth studies of tighter multinational collaborations in cyber security, including common standards based in best practices. Ideally, such standards should be promoted globally.

Empirical study 2: A study of cyber security within enterprises

Whilst international initiatives help in controlling the cross-border cyber security incidents, it is possible for private enterprises to

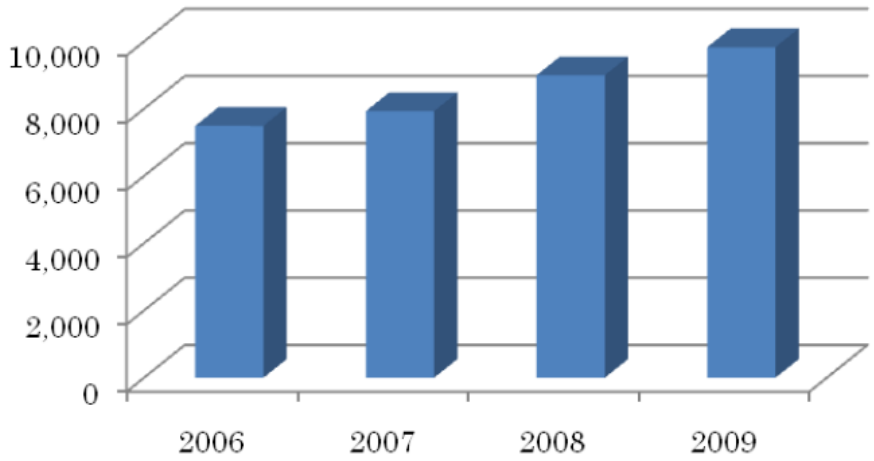

Figure 3. Reported cyber security incidents in Australia; source: Asia-Pacific computer emergency response team annual report (2009).

contribute to cyber security by esta-blishing sufficient processes and procedures for ensuring cyber security, including providing sufficient resources to address this issue in the workplace. While governmental organisations would possibly have government driven processes and procedures, including relatively extensive funding, to address cyber security, private firms would not necessarily have access to such sophistication or funding. Hence, private enterprises could potentially be more vulnerable to cyber security issues, and a study of how they address such issues could provide insights on policies and procedures at the firm level that could improve firm level cyber security. The improvements in firm level cyber security would in turn enhance national and regional cyber security.

As such, 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, fre-quency 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 analysis discussed further, 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.

FINDINGS

Risk assessment

The findings regarding the assessment of computer risks by the firms are presented in Table 3. Slightly over 58% of the respondents 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 35% indicated that their firms had prioritised budget allocations for assessment of computer security risk, while almost 17% indicated otherwise. Over 47% of the correspondents 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.

Prioritised budgetary allocations

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 shows the findings regarding the allocated amounts. The table indicates that when firms do provide budgetary allocations for addressing computer fraud, the amount is often ample. Within this group, around 60% allocate over RM 100, 000. However, there are also a number of firms that allocate mere token amounts for assessing computer

Table 3. Assessment of computer fraud risk.

Assessment	Yes		No		Do not know		Total	Percent
	Count	Percent	Count	Percent	Count	Percent		
The company performs risk assessment on computer security	38	58.5	24	36.9	3	4.6	65	100
The company has prioritized budget allocation for risk assessment on computer security	23	35.4	11	16.9	31	47.7	65	100

Table 4. Analysis of prioritized budget allocation.

Budget allocation	Count	Percent
Less than RM 1,000	5	21.74
RM 1,001 - 50,000	2	8.70
RM 50,001 –100,000	2	8.70
More than RM 100,000	14	60.87
Total	23	100.00

security risk. For instance, about 22% allocate less than RM 1, 000. Discarding these firms that allocate token amounts, which is indicative of a weak commitment towards addressing computer fraud, we find that in the total sample, only 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 provides further evidence in support of these conclusions. The table indicates that over 53% 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 (for example, internal divisions or internal audit departments) to detect or minimise computer fraud. Table 6 indicates the findings related to this area.

Computer fraud detection teams

Table 6 indicates that only about 28% of the respondents' firms had special divisions to detect and minimise fraud. Internal audit departments play active roles in this area in about 50% of the companies. The findings appear to indicate an important role for internal audit[3] 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 shows that in almost 50% of the firms, 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% 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% 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 indicate that the responsibility for the detection of computer fraud could vest with the auditing and accounting departments, since ensuring the reliability of corporate information is part of their normal duties. In essence, these findings indicate that accountants could play a valuable front-line cyber-incident detection role in a system designed to address global cyber security and stability issues.

[3] 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.

Table 5. Frequency of computer security system checks.

Frequency	Count	Percent
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 6. The presence of computer fraud detection teams.

Detection	Yes		No		Do not know		Total	Percent
	Count	Percent	Count	Percent	Count	Percent		
The company has a special division to detect or minimize fraud	18	27.7	47	72.3	0	0	65	100
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 7. Persons relied most to detect and prevent computer fraud in companies.

Person relied most to prevent and detect computer fraud	Count	Percent
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

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 the sampled organisations. However, the findings shown in Table 8 indicate that this explanation did not hold, because, computer security incidences were not uncommon in these firms.

Incidences of computer fraud in the surveyed firms

Nearly 57% of the respondents' firms experienced incidences of computer fraud within the previous 12 months. Over 50% of these 37 firms 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 that had experienced computer fraud estimated their direct and indirect losses to amount to RM 10, 000 to 50, 000. About 21% reported losses below RM 10, 000. Around 5% reported losses above RM 250, 000. The data in Table 8 indicates that incidences of computer fraud do occur in firms. Almost 80% of the respondents who had experienced incidences of computer fraud estimated the associated direct and indirect losses to be above RM 10, 000. In general, these findings that computer fraud is not uncommon in Malaysia private enterprises, is consistent with the increasing numbers of reported cyber security incidents observed in Figure 1.

The findings presented in Tables 3 to 8 indicate that the publicly listed companies in Malaysia do not place much emphasis on computer security, although they do experience computer security attacks and the direct and indirect losses from such attacks are not trivial. These

Table 8. Incidents of computer fraud and associated losses.

Incident	Yes		No		Do not know		Total	Percent
	Count	Percent	Count	Percent	Count	Percent		
Company experienced computer fraud cases within the last 12 months	37	56.9	26	40	2	3.1	65	100
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						
The company's direct and indirect loss amount due to computer fraud incidents								
Less than RM10,000	8	21.6						
RM10,000-RM50,000	16	43.2						
RM50,000-RM100,000	7	19.0					37	100
RM100,000-RM250,000	4	10.8						
More than RM250,000	2	5.4						

conclusions are further supported by the findings that only about 35% of the respondents provide 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 concur with the trends indicated by the examination of RTAs (Table 2). In both cases, limited attention appears to be paid to computer security, which essentially comprises ICT security. There was a lack of urgency in addressing this problem, which could potentially blow up into a major issue with global repercussions. Furthermore, they indicate that cyber security incidents are not uncommon in private firms, which is consistent with the observations in Figure 1 that indicates increasing cyber security incidents nationwide.

COMPUTER SECURITY ISSUES, IMPLICATIONS AND RECOMMENDATIONS

Many RTAs provide for the establishment, and networking of ICT, systems that enable 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, at the level of multinational RTAs, the nations and private firms within nations, 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[4] 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). This is disturbing, especially for developing nations that have experienced sharp rises in the numbers of reported cyber security incidents in recent years (Figures 1 and 2).

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

[4]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

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, such as, 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.

Furthermore, cyber security and the stability of interconnected, borderless multinational ICT systems is vital for long-term global economic stability, just as much as secure financial institutions and structures are vital for global financial stability.

As such, it is timely for international bodies to consider and organisation that will promote and compel international standards and best practices in ICT security at the level of the multinational borderless networks, as well as individual nations and firms. In short, such an organisation's work will provide an important impetus for focusing attention on global cyber security, just like the Basle committee's efforts have brought immense attention to best practices in financial institutions and global financial security. Such an organisation needs to address ICT governance issues, and promote tight collaboration between developed and developing nations for the mutual benefit of all. Figure 4, Human Capital Development Cost-Benefit Framework Human resource development for establishing ICT security at regional and national levels Figure 4 indicates that sometimes high levels of investment in ICT training may result in high levels of skills in containing ICT related fraud (Level 2), while in other cases, similar training results in limited development of ICT skills (Level 4). On the other hand, it members of operational departments to address company wide IT security problems. Cyber auditors and forensic accountants will be well positioned to serve as the front line defence[5] in 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: might also be possible to plan the human capital development programmes such that low investment levels in ICT training, provides high levels of skills in addressing ICT based issues (Level 1). 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 (Level 3).

Strategies that enable low levels of investment to give rise to high levels of ICT skills are particularly important for developing nations with limited resources[6]. 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

[5]Professional accountants who are trained in fraud detection and containment are already present in many developing nations, thanks to professional accounting bodies that have established rigorous training and certification regimes worldwide. This approach essentially leverages upon the fraud detection capabilities of the trained accountant, who then passes on the necessary documentation to the IT professionals for further corrective action. The accountants will also be able to test the effectiveness of controls that could prevent future problems.

[6] Developing nations are able to produce a highly skilled ICT based workforce through well funded universities and training labs, and heavily funded research (i.e. the strategy indicated by Level 2 in Figure 6). This is possible because these rich nations have sufficient cash to invest in such expensive methods for developing ICT savvy human capital. However, cash strapped developing nations do not have enough cash to follow a similar strategy. Therefore, they need to consider an approach where they can develop ICT savvy human capital without the need for great cash outlays (i.e. consider the strategy indicated by Level 1 in Figure 6).

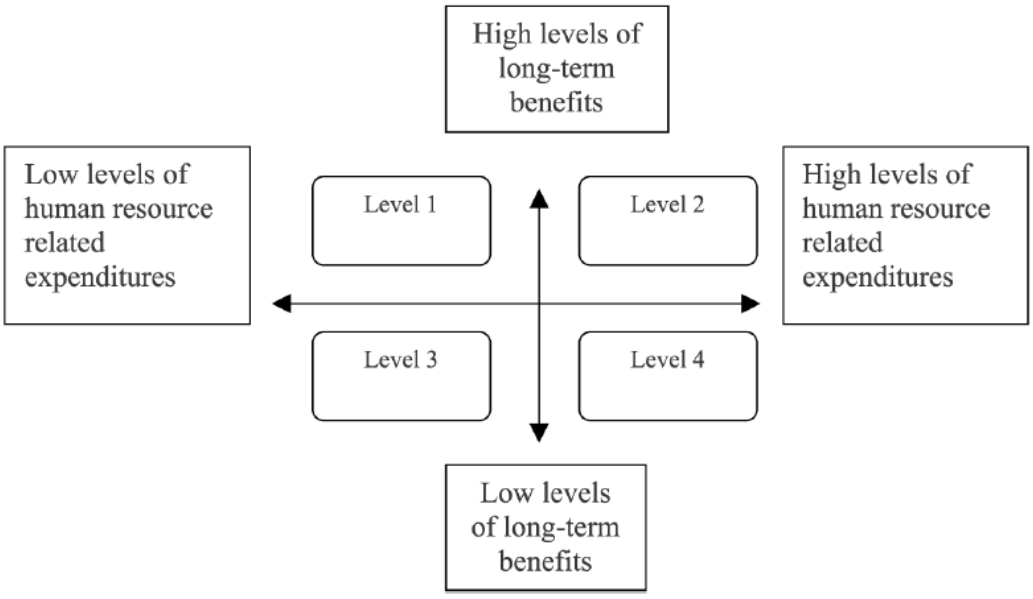

Figure 4. Human capital development cost-benefit framework human resource development for establishing ICT security at regional and national levels (Samudhram et al., 2008).

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

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, national level cyber security incidents in developing and developed nations as well as survey of listed firms in Malaysia suggests that very little attention is being paid to contain ICT security risk, particularly in developing nations.

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 help in developing cyber-auditors and cyber-forensic accountants, who can serve as the front line of defence, to help to detect cyber securities incidents within the system and pass the necessary information to IT professionals for corrective actions.

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. Given the potential for cyber security issues to cripple the world's economy, it is proposed that high level committees, akin to the Basle committee in global banking, be established to govern global cyber security.

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, JK, Tarimo, CN, Yngstrom L, Magnusson C, Kowalski S (2007). "Bridging the gap between general management and technicians – A case study on ICT security in a developing country". Comput. Secur., 26: 44-55.

Berry B (1997). "Long waves and geography in the 21st century". Futures, 29(4): 301-310.

Daniels PL (2005). "Technology revolutions and social development: Prospects for a green technoeconomic paradigm in lower income countries". Int. J. Soc. Econ., 32(5): 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, van der Straaten J (Eds), Environment, Technology and economic growth: The challenge to sustainable development, Edward Elgar, Cheltenham.

Freeman C, 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 NMD et al. (2006). "Green productivity indexing: A practical step toward integrating environmental performance into corporate performance". Int. J. Prod. Perform. Manage., 55(7): 594-606.

Gani A, Clemes MD (2006). "Information and communications technology: a non-income influence on economic well being". Int. J. Soc. Econ., 33(5): 649-663.

Kranacher MJ, Stern L (2004). "Enhancing fraud detection through education". CPA J., pp. 66-67.

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

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

Mutula SM, Brakel PV (2007). "ICT skills readiness for the emerging digital economy among small businesses in emerging countries". Lib. Hi Tech., 25(2): 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", Eur. Bus. Rev., 97(5): 244.

Rojšek I (2001). "From red to green: towards the environmental management in the country in transition". J. Bus. Ethics, 33(1): 37-50.

Samudhram A (2000). "Guarding vital data from security flaws", Computimes, New Straits Times, Malaysia, p. 22.

Samudhram A, Shanmugam B, Low LTL (2008). "Valuing human resources: an analytical framework". J. Intel. Capital, 9(4): 655-667

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 CM (2003). "Marketing and e-commerce as tools of development in the Asia-Pacific region: a dual path". Int. Mark. Rev., 21(3): 310-320.