# Is Your Information At Risk? Information Technology Leaders' Thoughts About The Impact Of Cybercrime On Competitive Advantage

Cyndy Jones, (Email: cyndyjones@bellsouth.net), Nova Southeastern University
Bahaudin Mujtaba, (Email: Mujtaba@sbe.nova.edu), Nova Southeastern University

**ABSTRACT**

*In the global market, communication, information, and information exchange between businesses and consumers are essential for a business to grow. As the need for information and information exchange increase, companies become more dependent on the information and the information technology systems, which are used to capture, process, store, distribute and use information. Information and information systems become a source of competitive advantage for twenty first century learning organizations. Thus, information should be viewed as a corporate asset like materials, money and personnel and as such needs to be managed and protected as any other corporate asset.*

*This paper provides the results of a qualitative study conducted with senior information technology officers and organizational leaders from seven international firms about cybercrime and information terrorism. More specifically, the study attempts to answer if a company's competitive advantage is at risk due to cyberterrorism and computer crime. Based on the views of these information technology leaders, the study also attempts to determine if the implementation of an IT security strategy can protect against cyberterrorism crime threats while offering a proposed model as a recommendation for organizational leaders.*

## CYBERCRIME AND INFORMATION SECURITY

Information impacts individuals, groups and organizations. Information, or lack of it, can impact the entire organization as it has a holistic trait. The holistic or systems thinking paradigm is concerned with the whole and their distinct characteristics or sectors (Checkland, 1999). According research, a basic *system* is inclusive of input, work-in-process, and output. Information can enhance a work environment, the environment affects the system, and the system can impact each component of the organization. Systems thinking paradigm requires leaders to look at problems, organizations, cyberterrorism challenges, cyber crimes, processes, from holistic perspective. Capra (1996) says it is about "seeing the world as an integrated whole rather than a dissociated collection of parts." Peter Senge (1990), Fritjof Capra (1996), Peter Checkland (1999), and other researchers have transferred systems thinking principles and theories into practice by applying them to real-world organizational-wide issues, thus encouraging the creation and development of learning organizations. The purpose of this paper is to discuss the systemic impact of information technology risks and cyber crimes associated with a company's competitive advantage.

Having access to information can make a person or a firm more powerful. So, information can lead to power as it is one source for it. Power is an important topic in leadership because, according to Hersey and Campbell (2004), it has the potential to influence; in other words, power has "the horsepower of making leadership work." Drs. Hersey and Campbell define power "as a leader's potential for influencing others." There are many bases for power and some

of the commonly cited sources of power are: expert, referent, legitimate, reward, coercive, connection, and information. Connection power comes from one's access to various powerful networks and individuals. Information power is based on one's access to valuable information (Hersey and Campbell, 2004).

Is there a best type of power for twenty first century managers and leaders? Hersey and Campbell (2004) state that, rather always using one form of power, the situational variables strongly influence the appropriate type of power. According to these authors, information power is effective when it is used with workers of moderate readiness to perform the job or task. Of course, information power is used by cyberterrorists to gain access to a firm's databases, ask for ransom, become high paid consultants for helping firms become more secure, steal information, sell information, and terrorize information technology professionals along with everyone else in their company. Such use and misuse of information is not limited to outside individuals, cyberterrorists, as internal employees can also steal or sell information.

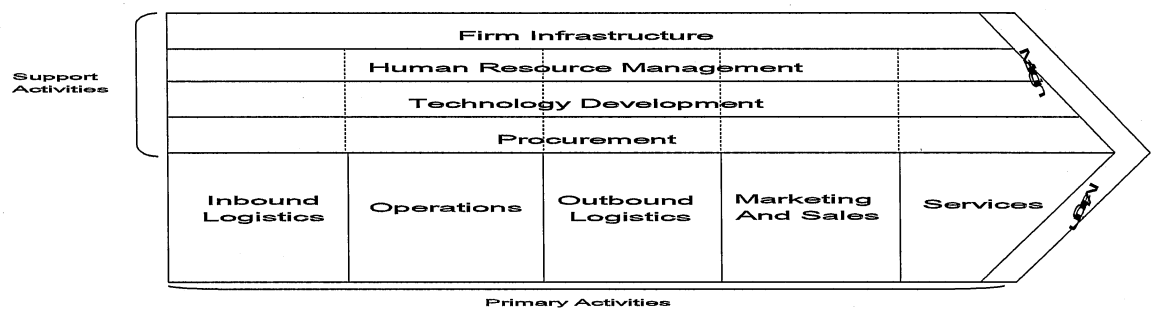
Companies are becoming increasingly vulnerable to both internal and external threats to their information and information technology systems. These threats are categorized as computer crime and cyberterrorism. With the increasing threat of cyberterrorism and computer crime, information technology security is becoming of great concern to companies. Information security is becoming vitally important to businesses as they operate in the global arena to guard and protect themselves from cyberterrorism and other computer crimes. The purpose of this study is to address two critical questions, which are:

- Is a company's competitive advantage at risk due to cyberterrorism and computer crime?
- Can the implementation of an IT security strategy protect against these threats and allow a company to maintain its competitive advantage?

In order to investigate these questions, a review of the current literature is conducted to understand the meaning of competitive advantage, to define the scope of computer crime and cyberterrorism, and to define and explain the components of information security. The results of the annual information security conducted by Ernst and Young will be reviewed. The results of Ernst and Young survey will be compared to the results of a survey conducted for the current research study with senior officials of international information technology firms.

According to Michael Porter and the value chain theory, a firm may possess two types of competitive advantage: low cost and differentiation. These advantages stem from the firm's ability to perform activities either more cheaply or in a unique way relative to its competitors. The ultimate value a firm creates is what buyers are willing to pay for what the firm produces, which includes its products as well as any related services. Competitive advantage is a function of either providing comparable buyer value more efficiently than the competitors (low cost) or performing activities in ways that create more value than competitors allowing a premium price, differentiation (Bartlett et al., 2004, p.315). Porter's value chain is shown in Figure 1.

**Figure 1: Value Chain**



Porter considers technology development as encompassing the activities involved in designing the product as well as creating and improving the way the various activities in the value chain are performed (Bartlett et al., p 316). Information could be considered part of the technology development component of the value chain and as such would be a critical resource, just like money and people, supporting a company in producing and delivering products and services at a lower cost or in a unique way to gain a competitive advantage.

In order to gain and maintain a competitive advantage in the arena of information and information systems, companies are using the Internet as a way to access global markets. Internet technology began in the late 1960s and 1970s, when the U.S. Department of Defense launched a system called Network, which comprised four computers. This system was called ARPANET. The major goal of ARPANET was to establish data communications between remotely located computers at different universities. This system was designed mainly for military research. By 1974, sixty-two computers were connected. The use of the system increased to such a level that in 1983, it was divided into two separate systems. One system was dedicated for military use and the other was dedicated to university research. The university system became known as the Internet. In 1983, the number of computers connected to the Internet was approximately one thousand and increased to about ten thousand by the end of 1987. The size of the system resulted in poor performance in transaction response time making it difficult to use the Internet effectively. Due to this, in 1987, the National Science Foundation decided to improve the performance and built the high-speed backbone Network for NSFNET (Mujtaba et al, 2004).

By the early 1990s, several countries connected their systems with the U.S. Network, and adopted the US model and began using the name Internet and the protocol TCP/IP. In 1994, commercial use, supported by individual businesses, took over the Internet. Now, the Internet pervades everyday personal and business processing and has become a target of misuse and crime (Mujtaba et al., 2004). Computer crime and cyberterrorism threaten a company's competitive advantage through unauthorized access and deliberate misuse or destruction of information. Computer crime is defined as the "unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals" (Foltz, 2004, p.158).

Computer crime can come in many forms, such as viruses, worms, web site defacement, denial of service, theft of customer information and theft of customer financial information. McGuire and Roser identified nine basic threats that cover the areas of greatest concern to companies. These threats include:

1. Data destruction
2. Interference
3. Modification/Replacement
4. Misrepresentation/false use of data
5. Repudiation
6. Inadvertent misuse
7. Unauthorized altering/downloading
8. Unauthorized transactions, and
9. Unauthorized disclosure (McGuire & Roser, 2000, p. 52).

The Department of Justice categorizes cybercrime into several groups, including individual crimes, computers used as weapons, computer used as an accessory, and the use of computers as tools for terrorism.

*Individual crime:* This includes various crimes such as, harassment of an individual using a computer that could be in the form of e-mail, cyber-stalking and transmission of child pornography. "Cyberloafing" refers to the use of the computer for personal use at the workplace during working hours resulting in wasted productivity is another problem identified in this category.

*Computers used as weapons:* This relates to the use of a computer to commit "traditional crimes", such as fraud or illegal gambling. Altering, destroying, or stealing others data are considered violations of privacy. Hacking-for-hire is also an illegal activity whereby hackers sell their services to break into other computer systems. The theft of more than 100,000 credit card numbers by a freelance computer technician is an example of this type of crime.

*Computer used as an accessory*: This refers to the use of a computer as a storage device to hold illegal or stolen information. These acts are both illegal and unethical since they adversely affect productivity and morale (Mujtaba et al, 2004).

*The computer as a tool for terrorist activity*: The FBI defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. It is assumed that "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data, which result in violence against noncombatant targets by sub-national groups or clandestine agents" (Embar-Seddon, 2002, p. 1036).

Nelson et al. defines cyberterrorism as the "calculated use of unlawful violence against digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological" (Nelson et al., 1999. p. 12). Overall, three levels of cyberterrorism capability have been defined:

1. *Simple-Unstructured*: At this level, the organization has the capability to conduct basic attacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.
2. *Advanced-Structured*: The organization is capable of conducting more sophisticated attacks against multiple systems or networks and may be able to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control and learning capability.
3. *Complex-Coordinated*: At this level, the organization may be able to perform coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses. The organization has the capability to create sophisticated hacking tools and possesses target analysis, command and control, and organizational learning functions (Nelson et al., 1999, p.12).

In 2003, various independent surveys revealed that between 36 to 90 percent of organizations reported computer security breaches over the twelve month period. The frequency of information technology security incidents seems to be on the rise at a disturbing rate. This increasing frequency of security breaches is driving higher spending on information technology security, expected to over $30.3 billion by 2006 (Garg *et al.*, 2003). Companies tend not to report information technology breaches and if they do report them, they undervalue the financial loss. The self-reported impact is valued at $50 thousand to $2 million per incident, while the study conducted by Garg *et al.* concluded that the average loss to a company was $17 to $28 million (Garg et al., 2003 p. 74). In 2004, the Association of Certified Fraud Examiners estimated that the typical organization in the United States loses 6 percent of its annual revenues to fraud, which amounts to approximately $660 billion in total losses (Ernst & Young, 2004, p. 13).

In 2005, a five-year industry analysis showed a gradual rise in the number of security incidents, with 34 percent of companies reporting one to five security breaches in 1999 and 47 percent reporting one to five breaches in 2004. Last year, 20 percent of organizations had six to ten "incidents" and 12 percent had at least ten or more. Another disturbing statistic is that 22 percent or one in five companies actually don't know or can't measure whether they've had a security incident or not (Emrich, 2005, p. 10).

While these studies indicate that there is a clear and present threat to companies with computer crime, there is still some debate about the actual threat of cyberterrorism. In 1999, Nelson *et al.* argued that the threat of cyberterrorism is a long-term threat as terrorist groups develop their expertise. Most of the threats that can be implemented are less dramatic threats that would be classified at the simple or advanced-structured levels. Only a few terrorist organizations would pursue advanced-structured and complex-coordinated cyberterrorism. The connectivity to all parts of the world enhances the potential of cyberterrorism by increasing the number of possible targets and improving the efficiency and effectiveness of cyberterror support activities. Nelson and his colleagues argue that cyberterrorism has the potential to cause widespread disruption; but its actual physical effects are limited. It does not currently have the capability to cause widespread physical destruction. The principal consequences of a cyberterror attack include a loss of reputation and confidence, a loss of proprietary information and privacy, and a loss of money and capital (Nelson et al., 1999 p. 32). It is unclear the disruption is a substitute for destruction and the results of an

attack are difficult to predict. Terrorist groups may not be willing to pursue a capability with so much uncertainty (Nelson et al., p. 34).

Others believe that cyberterrorism is on the rise and this trend will continue due to the widespread availability of powerful computers that can reach a broad international set of users in large metropolitan areas as well as remote areas. One of the more popular forms of cyberterrorism is to threaten financial institutions. The terrorists hack into the system leaving an encrypted message threatening to destroy bank files with electromagnetic pulses and high-emission radio frequency guns unless they are paid money. Most banks would rather pay the money than have the public know how vulnerable they are to such acts of terrorism. It is very difficult to catch the criminals given that they could be in another state or country at the time the crime is committed (Mujtaba et al., 2004).

Furthermore, the perpetrator of a cybercrime is increasingly being identified as an employee, rather than an unknown hacker. According to a Computer Security Institute study (gosci.com), 55 percent of network computer users reported malicious activities by legitimate users of the corporate network. In a 2001 survey, 91 percent of Information Technology departments reported detecting serious employee abuse of Internet access. These breaches of security ranged from opening e-mail attachments known to be infected, to loading 'mischievous' software on the office computer, such as unauthorized encryption, downloading viruses, spyware (programs that allow an outsider to spy on your computer on an ongoing basis), scamware (programs that dial international long distance calls and bill the caller's phone account automatically), and surfing for private purposes on company time (Evans, 2002, p. 29). According to the 2005 Global Security Survey for Financial Services Survey, which surveyed 100 of the top global financial institutions, 35 % respondents indicated attacks from inside their organization within the last 12 months were up from 14% in 2004 as compared to 26% from external sources up from 23% in 2004 (Deloitte, 2005).

Viruses have become a popular tool of many individual hackers as well as criminal organizations. Many hackers attack corporate or home computer security with malicious code. This combination of hacking and malicious code distribution is called a 'blended threat'. The hacker introduces software that ranges from spyware designed to watch the computer user, keystroke loggers to catch passwords and banking information, trojans which leave a back door into the hacked system, 'zombie' software which takes over the computer for use in a distributed denial of service attack, or various kinds of virus codes which can cause the infected computer to perform functions at the hacker's command (Evans, 2002, p. 28).

A recent example of a virus attack occurred on May 22, 2005, when over 40 million customers were exposed to fraud when Card System Solutions, a company that processes credit card transactions, was attacked by hackers through the introduction of a virus. The hackers stole the credit card number, the security code on the back of the card and the expiration date (Pegues, 2005).

There is increasing concern in government and law enforcement groups over the use of malicious code as a tool of state-sponsored or freelance industrial espionage and cyberterrorism. There have been hacker and virus 'wars' between The People's Republic of China and Taiwan, and many terrorist and hate groups have an active Web presence, and are developing the technical capabilities to conduct both spying and military or economic sabotage on government and corporate networks (Evans, 2002. p. 30).

In order to protect the information, it is essential for companies to develop an information security strategy and to implement information security measures. Many definitions of information security can be found in the literature. In their study on information security management, Hong *et al.* defines it as the "set of systems, operations and internal controls combined to ensure the integrity and confidentiality of data and operations procedures in an organization" (Hong et al., 2003, p.243). One goal of information technology security is to prevent the unauthorized acts of computer users. The objectives of computer security policy are to ensure the data confidentiality, integrity and availability within information systems.

The British Standard Institution established BS7799-1 in 1995 and was the first complete framework for information security. This standard was updated in 1999 and incorporated in the ISO 17799 Standard in 2000. The standard has been updated over the last five years and is considered to be a comprehensive set of controls for

information security developed in line with the best practices followed by leading organizations around the world. The standard combines the business experience and know-how of the multinational companies, as well as the culture and regulatory compliance of real-world environments (InnoKAT, 2005, p.1). Certification of compliance to the information security practices identified in the standard can serve as a major market differentiator for companies. Literature shows that an information security program should have five key elements that include:

1. A process to take the message to the user community to reinforce the concept that information security is an important part of the business process
2. Identification of the individuals who are responsible for the implementation of the security program
3. The ability to determine the sensitivity of information and the criticality of applications, systems, and business processes
4. The business reasons why basic security concepts such as separation of duties, need-to-know, and least privilege must be implemented
5. That senior management supports the goals and objectives of the information security program (Peltier, 2005, p. 3).

In addition to the basic security measures, such as traffic filtering, virus control, and intrusion monitoring and prevention devices, Barlock, a senior consultant at Accenture, describes three strategies companies can employ to strengthen security. *First*, an organization must develop a "complete view" of what information security means by defining an overall security blueprint, which shows how the security framework is structured, what the security governance model looks like, and what procedures should be taken to address security issues. *Second*, an organization needs to deal with the regulatory compliance problem with a standard process that addresses overall compliance rather than working on procedures on a per regulation basis. Once the strategy is in place, it must be continually reviewed including updating, revising and monitoring risk assessment, policy definition, and processes surrounding privacy and security breaches. *Third*, an organization needs to plan for "identity and access management" (I&AM), which involves designing and implementing a set of business process controls and an integrated architecture to streamline operations, reduce costs and regain control of user access (Emrich, 2005, p. 10).

As important as a set of written policies, standards, and procedures is in defining the architecture of the security program and the infrastructure that supports it, in actuality, most employees do not take the time to read and understand these documents. It is critical that companies ensure that employees are aware of and are trained in the security policies and procedures within the organization. The objective of the awareness program is to communicate to employees what the security strategy and procedures are within the company as well as the employee's role in protecting the corporate information.

## ERNST AND YOUNG SURVEY RESULTS

Ernst & Young has conducted an annual information security survey since 1993. In 2004, more than 1230 organizations across 51 countries participated in the Ernst & Young annual survey on information security. The survey indicated the criticality of senior management involvement in setting the direction for information security and communicating the strategy throughout the organization. The survey indicated that many organizations are indifferent to the information technology controls and the importance of information technology security to meeting the organizational goals, leading to an overall response of only 20% that strongly agreed that their organizations perceive information security as a CEO priority. Respondents who indicated that an effective information strategy was important to meeting organizational goals also indicated that the CEO placed a high priority on the information security strategy.

While senior management stated that information security is important, gaps continue to exist in the amount of diligence and resources that are deployed to improve the degree of protection. Respondents cited lack of security awareness by users as one of the top obstacles to effective information security. Management, however, is reluctant to place a priority to human investment in terms of employee awareness and training, but will readily commit to technology security expenditures. Less than half of the organizations provided their employees with ongoing training

in security. Less than 30% listed raising employee information security training and awareness as a top initiative in 2004.

Respondents continued to indicate that their organizations were more vulnerable to external attacks than internal breaches. Employee misconduct involving information systems was cited as a distant number two concern behind major virus, trojan horse or Internet worms regardless of geographic region, industry or organization size and controls. This was an interesting finding given the fact that leading research groups contend that the greatest security threats are from internal users, including current, temporary and former employees.

Almost 100% of the organizations deployed anti-virus technology to protect themselves. Less than 64% have vulnerability and penetration assessments conducted on a regular basis. Less than 50% agreed that they could continue business operations in the event of a serious disruption.

## RESEARCH FOCUS AND METHODOLOGY

Through a review of the literature, other surveys, and a qualitative survey of senior information technology officers of firms that operate around the world, this study attempts to clarify the risks associated with terrorism and whether information technology security can be a source of competitive advantage. As such, the purpose of this study is to investigate two key propositions:

1. *Proposition One:* A company's competitive advantage is at risk due to cyberterrorism and computer crime.
2. *Proposition Two*: The implementation of an IT security strategy can protect against cyberterrorism crime threats and allow a company to maintain its competitive advantage.

As more companies participate in the global economy using the Internet becomes essential to corporate growth and market share in the multi-billion dollar Business to Business (B2B) and Business to Consumer (B2C) markets. Companies are increasingly vulnerable to both internal and external threats to their information technology systems. Information security is becoming increasingly important to businesses as they operate in the global arena. Very little empirical research has been done in the past to measure and quantify the impact of IT breaches to an organization. Most attempts of measuring the impact of IT breaches have depended upon self-reporting by the organization. The methodology used in this research is to review the Ernst and Young Global Information Security Survey in 2004, presented in the earlier section. The results of Ernst and Young's survey can be compared with the results obtained through an independent survey conducted with seven international businesses having offices in the United States.

It is assumed that information technology professionals of the twenty first century environment are at the forefront of securing their company's most valuable asset: the information related to the firm's core competency and, thus, their competitive advantage. The survey implemented for this study attempts to gather the views of IT professionals to provide a status report on the perceptions related to security risks associated with cyberterrorism and computer crime. Respondents were directed to answer the questions truthfully based on their expert opinion. Furthermore, the respondents were assured that each their names and their companies' names will remain confidential as no such information is collected nor kept track of for specific firms.

This current study used qualitative phenomenological research methodology. Qualitative research is seen as the "modes of systematic inquiry concerned with understanding human beings and the nature of their transactions with themselves and with their surroundings" (Polit & Hungler, 1993). The phenomenological approach was chosen for this study as it provides useful insights into some of the challenges that security concerns and risks can bring to management decision making. Researchers such as Creswell (2003) see phenomenological research "as a method in which the researcher identifies the essence of human experiences concerning a phenomenon, as described by the participants in a study." This method of research provides sufficient time to explore all possible challenges associated with cybercrime and information technology risks. The phenomenological approach of qualitative study can allow researchers to describe a population's life experiences and some researchers (such as Miller, 2003) believe that only those who have actually experienced phenomena are capable of best communicating their observations, feelings and

concerns to the outside world. Furthermore, the phenomenological research allows researchers to explore and describe the targeted population's perceptions of the challenges associated with decision-making in retaining a competitive advantage. Overall, the main objective of using a phenomenological research approach is to allow each participant to describe his or her experiences in a formal and structured manner while allowing researchers to ask follow up questions for clarification and more details. The data for this study was collected using structured interviews and structured surveys with the senior officers, information technology professionals, presidents, divisional heads, and IT experts working for international firms. Some of the available information that can be shared without compromising the confidentiality of the respondents' organizations is presented in Table 1.

**Table 1 – Demographic Information Of Respondents' Firms**

| Firm | 2004 Revenue | Number of Employees | Headquarters |
|---|---|---|---|
| 1 | 19,178,000,000 | 70,200 | United States |
| 2 | 18,176.000,000 | 28,600 | United States |
| 3 | 20,300,000,000 | 63,000 | United States |
| 4 | 1,346,391,000 | 46,500 | India |
| 5 | 2,554,669,000 | 25,000 | Canada |
| 6 | N/A | N/A | United States |
| 7 | N/A | N/A | United States |

Nine information security assessment surveys were distributed to information technology officers of international companies having offices in the United States. Seven responses were received. Of the respondents, one was based in Canada, one was based in India and the other five companies were headquartered in the United States. One of the companies was a not-for-profit organization while the other organizations were for-profit corporations. Questions in the survey were presented using a Likert format. The survey questions are shown in Appendix A – Information Security Survey.

## STUDY RESULTS

The survey conducted for this study revolved around three areas: the organization's information technology security strategy, procedures and policies; the perceived threat of computer crime and cyberterrorism; and the impact of cybercrime on a firm's organizational goals and market share. The Ernst & Young survey did not specifically address the threat of cyberterrorism.

Seven international organizations were interviewed through structured surveys either face-to-face, over the phone, or via written survey for this qualitative study. Contact information was available for the respondents for follow-up questions. The organizations had at least 25% of their revenue from international sources or were dependent on international partners for goods or manufacturing support. The seven respondents from international information technology firms represented chief security officers, presidents, vice presidents, and senior divisional officers. One of the respondents was interviewed over the phone and two others were called once their completed surveys' were received to confirm and clarify their answers through a follow up set of questions.

All seven respondents agreed that over 75% of the corporate information was stored in electronic format. All but one of the organizations had a formal information security strategy and strongly agreed that the information technology security was essential in meeting the goals of the organization, although the results were mixed in terms of the impact of the information technology security strategy on protecting the company's market share. One respondent remarked that he did not believe that having an information security strategy helped the company win the business, but without an information security strategy and controls, the company would have lost business. All agreed or strongly agreed that the information security breaches would have a negative impact on the company business.

All respondents also agreed that senior management was directly involved in the development and execution of the information security strategy and that protecting the corporate information was not strictly an information technology function. Five of the seven respondents agreed or strongly agreed that over 75% of the staff

has personal and immediate access to corporate data. Four of the seven respondents felt that the greater threat to their information systems was from external sources. One respondent suggested that there was a greater likelihood of breaches from inside the organization, but the impact to the overall organization would be minimal. On the other hand, the respondent believed that if there was an external attack, the magnitude of the attack and the breadth of the destruction would be greater than an internal breach.

Additionally, 85% of the respondents agreed that formal procedures had been developed regarding the execution of the information security strategy and to assess and mitigate risks associated with threats to information systems and corporate data. About 57% of the respondents noted that employees had not been trained in the information security processes and procedures. These results are consistent with the Ernst and Young survey which found that while senior management in organizations believed information security was important, this was not conveyed to employees effectively. Employees were not well versed or trained in the information security procedures. This was also consistent with the 2005 Global Security Survey that indicated that security and training is not considered a high or top priority at the C levels and that less than 46% had training and awareness initiatives scheduled in the next 12 months. It was further reported that 64% of the budget allocation for security was targeted to tools and only 15% to employee awareness programs (Deloitte, 2005).

As seen in the Ernst and Young survey, most of the respondents in the current study also believed the information security threat was greatest from external sources. In this research survey, a similar finding was found in that all of the respondents agreed or strongly agreed that there is a real threat to corporate information in the form of information security breaches and cyberterrorism and most agreed the threat was from external sources. All agreed or strongly agreed that an information security strategy was essential to combating the threat of cyberterrorism and computer crime and felt that the corporate information was better protected from cyberterrorism as a result of the information security strategy.

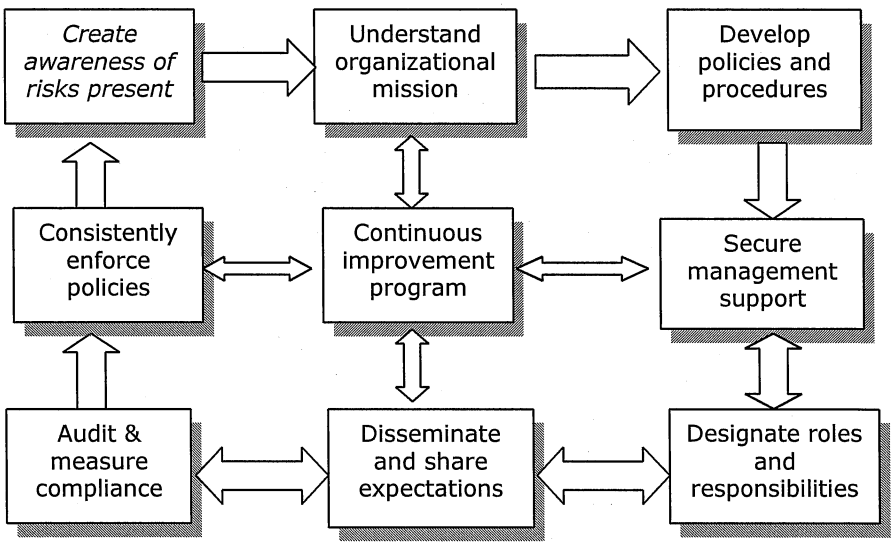
The results were mixed in terms of whether the threats would come from within the home country borders or outside. Likewise, the results were mixed as to whether information security measures were more critical to protecting against cyberterrorism and computer crime in the home country market.

## IMPLICATIONS OF FINDINGS AND RECOMMENDATIONS FOR MANAGERS

National and international business managers must understand that threats of computer crime in the form of information breaches and cyberterrorism are real and they must ensure that appropriate information security strategies, policies, procedures, and measures are in place, communicated to employees and enforced throughout the organization. Destruction or loss of information or information systems could seriously affect the company's bottom line as well as the company's share of the market. The impact of cybercrime could be even more severe if the corporate information is sold or given to competitors from hackers or disgruntled employees. Although most organizations believe the threat is greater from outside organizations, independent studies have indicated that inside threats are more likely.

In order to create awareness and a practical model, information technology professional and managers should institute relevant policies and procedures to bring about appropriate safeguards in the organization. As presented in Figure 2, information technology professionals can apply the following steps to better manage various organizational-relevant security concerns and, thus, have a better database management process.

**Figure 2 – Database Security and Management Model**




The Database Security and Management Model offer nine steps that managers can use as they create an information security program. The initial steps are offered by the authors and the remaining steps have been identified for the establishment of a database management system by Wayman (2005). These steps are directly applicable to creating and establishing an information security strategy, security policies and procedures. The international manager should consider implementing these steps within the organization to protect the company and its corporate data.

1. *Create awareness of present risks for the organization*: Organizations need to assess their existing information and database management security systems. It is important to assess the existing infrastructure honestly and thoroughly. Once the current status is clear, gaps are recognized and the information is communicated to employees, then appropriate steps can be taken to synergistically work toward filling the gaps.
2. *Understand the organization's goals, mission and vision*: Organizations have vision and mission statements that show their purpose, goals and overall direction. Information security and database management programs must be linked to the achievement of this mission and vision which will demonstrate the organization's commitment to effective database management. Making such links will also make it easier to get support and resources from top management for the implementation process.
3. *Develop and implement policies and procedures*: Organizations are beginning to understand the risks associated with information management. As with any management program, policies and procedures provide the foundation of a successful information security management program and demonstrate the organization's commitment to sound management (Wayman, 2005, p. 2).
4. *Elicit support from all levels of management*: A successful program requires senior executives and managers to take responsibility for the program's development, implementation and ongoing improvement (Wayman, 2005).
5. *Delegate proper program roles and components*: Responsibility for information security management programs must be delegated only to those individuals with appropriate training, qualifications and authority. Every employee in an organization shares responsibility for compliance, but specific roles and responsibilities also must be created, and appropriate authority delegated to oversee specific program components (Wayman, 2005).
6. *Disseminate, communicate and train employees*: The organization must take steps to effectively communicate policies and procedures to all employees. These steps might include requiring all employees to participate in training programs or the widespread distribution of information that explains in a practical and understandable manner the expectations and roles of employees (Wayman, 2005).

7. *Audit, monitor and measure program compliance:* The organization must take reasonable steps to measure compliance with policies and procedures by utilizing monitoring and auditing programs. The role of auditing and monitoring is to provide management with a method of measuring and improving information security management programs. The organization must also develop a way to effectively measure the cost of the impact of an attack on the corporate data and information systems (Wayman, 2005).
8. *Implement effective and consistent program enforcement:* Program policies and procedures must be consistently enforced through appropriate disciplinary mechanisms and the proper configuration and management of related systems. The existence of a compliance program is not sufficient. Effective and consistent enforcement of the program policies and procedures is essential in order to minimize liability and risk (Wayman, 2005).
9. *Implement continuous program improvement:* With the growing threat of computer crime and cyberterrorism, organizations must continuously evaluate the effectiveness of their information security program (Wayman, 2005, p. 2).

Security is becoming a growing concern for customers. According to Josh (2004), in an opinion poll conducted jointly by the National Association of Software and Service Companies and Information Technology Association of America, 115 information technology companies in India and the US were asked questions ranging from the role and importance of information security in an organization and the growing importance of information security offerings and practices as a source of competitive advantage. Results showed that 82% of customers of Indian firms and 76% of customers of U.S. firms were more concerned about information security. Security is emerging as a key differentiator for these companies. The survey found that 75% of Indian companies and 82% of U.S. companies agreed that sophisticated information security offerings and practices offer a competitive advantage. According to the survey, 75% of the Indian companies and 64% of the U.S. companies agreed that information security practices are a critical selling point while marketing their products and services to global clients (Joshi, 2004).

As companies grow and operate in the global arena, information and the information systems are major components of conducting business and are integral to the success of companies' profitability and growth. Protection of this corporate information is critical. Companies with sensitive information, such as credit card data, need to be even more aggressive in protecting their information. Based on the recent studies and the reported incidents, the threat of computer crime and cyberterrorism is real and increasing. More incidents of computer crime are being reported each year and the criminals are becoming more sophisticated in their attacks. No company is 100% protected from these threats.

Given the large negative impact on the company's goals and finances, companies must develop mechanisms to better measure the impact of information technology breaches, and more importantly, companies need to develop an information security strategy and invest in information technology security measures to protect their corporate information. These measures must include investment in physical information technology security, such as firewalls and virus protection software as well as documentation and training of employees in the information security polices and practices. Senior management must take an active role in developing this strategy and communicating it throughout the organization.

## CONCLUSION

The information technology security strategy is important to protect the critical information resource and to protect the company from many of the threats of computer crime. These information security measures must be maintained and monitored to keep pace with the ever-changing types of threats. Without an effective information security strategy, procedures and measures, the company's competitive advantage can be seriously jeopardized.

Through a structured survey of senior information technology officers, this study concludes that there are both internal and external security threats for companies competing in the twenty first century's competitive work environment. Therefore, because of the qualitative survey in this study, the first proposition is supported: A company's competitive advantage is at risk due to cyberterrorism and computer crime. Because of the results provided by the information technology professionals, the second proposition is also supported: The implementation of an IT

security strategy can protect against cyberterrorism crime threats and allow a company to maintain its competitive advantage. As a result, recommendations are offered for organizations and their managers to appropriately increase the security of their information, and consequently their competitive advantage.

## REFERENCES


1. Bartlett, C.A., Ghoshal, S., & Birkenshaw, J. (2004). *Transnational Management: Text, Cases and Readings in Cross-Border Management* (4th Edition). New York: McGraw/Irwin.
2. Capra, F. (1996). *The web of life.* New York: Doubleday.
3. Checkland, P. (1999). *Systems thinking, systems practice: A 30 year retrospective.* New York: John Wiley & Sons, Inc.
4. Collins, J.C. (2001). *Good to great: Why some companies make the leap...and others don't.* New York: Harper Collins.
5. Creswell, J. (2003). *Research design: Qualitative, Quantitative, And Mixed Methods Approaches.* London: Sage Publications.
6. Embar-Seddon, A. (2002). Cyberterrorism, Are We Under Siege? *American Behavioral Scientist,* 45(6), 1033-1043. Retrieved May 20, 2005 from ABI/INFORM Complete.
7. Emrich, A. (2005). Information Security Poses Increasing Problems. *Grand Rapids Business Journal*, 23 (11), 10. Retrieved June 18, 2005 from ABI/INFORM Complete.
8. Ernst & Young. (2004). Global Information Security Survey. 1-25. Retrieved May 28, 2005 from http:/www.ey.com.
9. Evans, J. (2005). Virus! Worms! Why Worry? *Computer Dealer News*, 18 (15), 28-31. Retrieved June 18, 2005 from ABI/INFORM Complete.
10. Foltz, B. (2004). Cyberterrorism, Computer Crime, and Reality. *Information Management and Computer Security*, 12 (2), 154-166. Retrieved May 25, 2005 from Emerald.
11. Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management and Computer Security*, 11 (2), 74-83. Retrieved May 25, 2005 from Emerald.
12. Hersey, P. and Campbell, R. (2004). *Leadership: A Behavioral Science Approach.* Leadership Studies Publishing. Escondido, CA.
13. Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An Integrated System Theory of Information Security Management. *Information Management and Computer Security*, 11 (5), 243-248. Retrieved May 20, 2005 from ABI/INFORM Complete.
14. InnoKAT announces new edition of ISO 17799. *Middle East Company News,* June 15, 2005. Retrieved June 16, 2005 from ABI/INFORM Complete.
15. Joshi, S., (2004). Information Security Practices, a Critical Selling Point. *The Hindu.* October 17, 2004. Retrieved June 27, 2005 from ABI/INFORM Complete.
16. McGuire, B. & Roser, S. (2002). What Your Business Should Know About Internet Security. *Strategic Finance* 82 (5) 50-54. Retrieved May 20, 2005 from ABI/INFORM Complete.
17. Miller, S. (2003). Analysis of phenomenological data generated with children as research participants. *Nurse Researcher*, 10(4) 68-82. Retrieved June 22, 2004, from http://proquest.umi.com
18. Mujtaba, B., Griffin, C., & Oskal, C. (2004). Emerging Ethical Issues in Technology and Countermeasures for Management and Leadership Consideration in the Twenty First Century's Competitive Environment of Global Interdependence. *Journal of Applied Management and Entrepreneurship,* 9 (3) 1-17.
19. Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror Prospects and Implications. Center for the Study of Terrorism and Irregular Warfare. Prepared by Naval Postgraduate* School. Monterey, CA. US Navy.
20. Pegues, J. (2005). 40 Million Credit Card Holders Facing Possible Identity Theft. *Eyewitness News*, June 18, 2005. Retrieved June 26, 2005 from 7Online.com.
21. Peltier, T. (2005). Implementing an Information Security Awareness Program. *EDPACS*, 33 (1), 1-19. Retrieved June 18, 2005 from ABI/INFORM Complete.
22. Polit, D. & Hungler, B. (1993). *Essentials of nursing research: methods, appraisal, and utilization.* Philadelphia: J.B. Lippincott Company.

23. Senge, P.M. (1990). *The fifth discipline: The art and practice of the learning organization.* New York: Currency/DoubleDay.
24. Wayman, W. (2005). In or Out of Database Management, *Security*, 42 (6), 14-15. Retrieved June 18, 2005 from ABI/INFORM Complete.

## APPENDIX A – INFORMATION SECURITY SURVEY

Dear IT Professional,

Information technology professionals of the twenty first century environment are at the forefront of securing their company's most valuable asset: the information related to the firm's core competency and, thus, their competitive advantage. This survey attempts to gather the views of IT professionals, such as yourself, to provide a status report on the perceptions related to security risks associated with cyberterrorism and computer crime. Answer the following questions truthfully based on your expert opinion. Be assured that each respondent's name and his/her company's name will remain confidential as no such information is collected.

1. Does 25% of your total sales revenue come from markets outside your home country? 1. Yes__. 2. No__.

2. Does your organization have an IT security strategy? 1. Yes__ 2. NO__.

3. How long has your IT strategy been in place? _____.

4. Over 75% of our corporate information is stored in electronic format.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

5. Protecting the corporate information is solely an IT function.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

6. IT security is essential to meeting the corporate business goals.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

7. Senior Management is directly involved in the development and execution of the IT security strategy.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

8. There is a real threat to corporate information in the form of cyberterrorism and IT security breaches.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

9. IT security and cyberterrorism threats are stronger from external sources than internal sources.
   1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

10. An IT security strategy is essential to combating the threat of cyberterrorism and IT security breaches.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

11. As a result of your IT strategy, your company information is better protected from cyberterrorism and IT security breaches.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

12. The corporate IT security strategy has helped to protect market share.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

13. The source of the cyberterrorism and IT security threats are most likely to be within the home country borders.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

14. IT security measures to protect against cyberterrorism and IT security breaches are more critical in the home country market.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

15. Over 75% of the staff has personal and immediate access to corporate data.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

16. Formal procedures and processes have been documented regarding the execution of the IT security strategy.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

17. Formal procedures to assess and mitigate risks associated to threats to IT systems and corporate data have been developed.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

18. Employees have been trained in the IT security processes and procedures.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

19. IT Security breaches would have a negative impact on company business.
    1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

20. You can share any other comments and concerns in regard to information technology, cybercrime and globalization as you wish.