

Security Issues in IT Management

Term Paper – Fall 2005

IT 4130: IT Issues and Management
Dr. E Sonny Butler

Grayson B. Kent
November 22, 2005

Table of Contents

Executive Summary	3
<i>Business Reliance on Information Technology.....</i>	<i>3</i>
<i>Management: An Ideal Supplement</i>	<i>4</i>
<i>Rational for IT Management.....</i>	<i>4</i>
Security and IT Management	6
<i>The Necessity for Security Management.....</i>	<i>6</i>
<i>Budgeting Security.....</i>	<i>7</i>
External Security: The Darkened Outside	9
<i>Hackers and Network Configuration.....</i>	<i>9</i>
<i>Viruses, Spyware, and Adware</i>	<i>9</i>
Internal Security and Control.....	11
Outsourcing: The Key to the Future of Security?	12
<i>Managing Outsourced Security</i>	<i>13</i>
Conclusion and Analysis	14
Works Cited.....	15

Executive Summary

Information technology can be defined as the development, acquisition, installation, and implementation of computer systems and applications. Throughout the second half of the twentieth century, information technology has grown from its infancy in the 1940s into an ever-evolving system that is now the backbone of communications and data transmissions. This span of over sixty years has brought about radical innovations that have forever transformed the world. These innovations include the computer, relational databases, and networking capabilities. Separately, these three innovations would lack the value to revolutionize infrastructure and data communication; however, together they are the catalyst which provides the ability to operate in a global market. After the implementation of these catalysts, businesses and people were no longer limited by natural boundaries such as geographic location.

Business Reliance on Information Technology

The information technology revolution began with the widespread access to, sharing of, and use of knowledge through technology primarily for business purposes. The information technology age has introduced two key transformations into the world. First, the concept of “real time response” transformed today’s business society by allowing information to be available instantaneously. Secondly, prior to the information technology revolution, most business organizations were limited by propinquity to customers and geographic location in which they were able to provide their products and services. One of the key advancements that aided the growth of information technology was the introduction of the Internet into the public domain in the mid-1990s. The Internet quickly provided a medium in which business firms had the opportunity to break

the previous barriers of time and location. This allowed the business society to enter into a swiftly maturing global market. This swift transformation has become known as globalization. Globalization has transformed worldwide economic markets to unprecedented points. Due to the economic globalization and the reliance on information provided by the latest technologies, information technology has made far-reaching, unalterable changes within business society.

Management: An Ideal Supplement

The College of Information Technology is designed to train tomorrow's innovators and entrepreneurs, those digital problem-solvers who will lead America's fastest growing career field ("College of Information Technology," 2003). CIT is on the cutting edge of providing the world's future IT professionals with the skills needed to lead the information technology industry into the next generation. Georgia Southern University's College of Information Technology boasts one of the first nationally accredited schools of Information Technology. One of the unique advantages of the Bachelor Degree in Information Technology at Georgia Southern University is the required accompaniment of a second discipline for all graduates. A wide variety of second disciplines exist including fields such as foreign languages, military science, criminal justice, health informatics, music, logistics, among many others. However, the second discipline of management seems to be the ideal supplement for information technology.

Rational for IT Management

The field of information technology is a highly demanding industry that is continuously shifting and must be monitored accordingly. There is a great need within

the field for IT managers who have the necessary skills to constantly supervise the latest trends within the field and make realistic decisions based on those trends. The overall success of a business's strategic movement is based upon the decisions made by the company's information technology manager. Aside from making important decisions concerning the future of the organization, an IT manager's duties also include controlling the current system. [Management control] is the process of monitoring activities to ensure that they are being accomplished as planned, and correcting any significant deviations (Robbins and Coulter, 2005). IT managers must maintain stable systems operations and ensure that both internal and external network utilities are functioning according to the organization's expected standards. Failure to ensure management control and expansion often results in the downfall and destruction of a business organization.

Security and IT Management

One of the core issues currently facing IT managers is the innumerable security challenges within information technology systems. It is irresponsible for an IT manager to deem that system security should not be one of an organization's top priorities in information technology management. With the increasing speed and power of the desktop computer, cyber-criminals possess "lethal" weapons which they can use to stage an attack with more speed, force, and methods than ever before. Information technology managers must stay abreast to the latest developments in cyber crime and manufacture a plan to defend against such attacks both internally and externally.

The Necessity for Security Management

Table 1 lays out the exponential growth of security incidences reported since the late 1980s. Note the tremendous escalation experienced following the dot-com boom on the Internet following 1998.

Number of Reported Security Incidences

*By Year**

<i>Year</i>	<i>Reported Incidents</i>
1988	6
1990	252
1992	773
1994	2,340
1996	2,573
1998	3,734
2000	21,756
2001	52,658
2002	82,094
2003	137,529

*Table 1 (Ciampa, 2005)

Information technology professionals must recognize this historic growth and realize that the trend will continue into the future. Cyber-criminals thrive on finding the security flaws in the latest developed operating systems, databases, and network

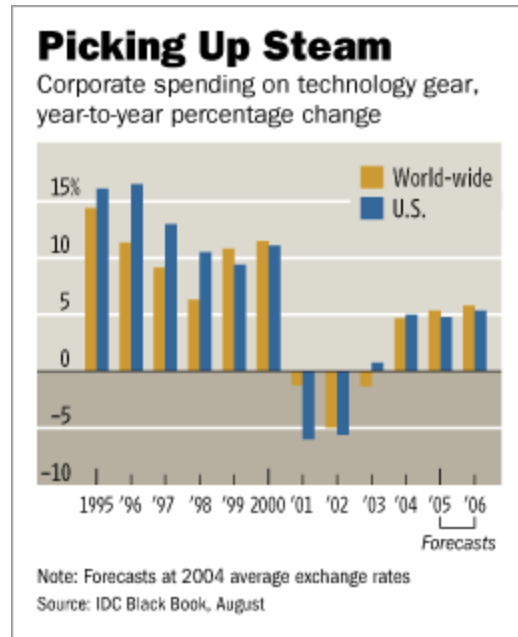
configurations in order to expose the information contained in those systems. Three of the characteristics of information [systems] that [IT managers] must protect by information security are integrity, confidentiality, and availability (Ciampa, 2005). These three characteristics are essential for not only the data itself but also the devices interacting with the data.

In recent years legislation has been passed to assist in maintaining adequate information security. IT managers must comply with this legislation in order to avoid their organizations facing legal penalties. One such example is the Sarbanes-Oxley Act. Following the WorldCom, Enron, and Tyco scandals in the early part of this century, the Sarbanes-Oxley Act of 2002 was passed by Congress to enhance internal control among organizations. The act was created to enforce standards in financial and other data reporting. Because the majority of organizations use electronic systems to maintain data, IT managers must, by law, take the procedures of internal control that are outlined in the Sarbanes-Oxley Act and implement them into the overall information system of their organizations.

Budgeting Security

As the need for information security increases, information technology managers will be forced to adjust technology spending to meet the demands created by the requirement of greater security measures. Financial technology spending polls from recent years have shown a steady increase with only a few years of mild decrease as shown in Graphic 1. The technology sector...has benefited from higher sales...as companies move to upgrade their aging infrastructures; the uptick is also being aided by the slew of new U.S. regulatory rules and a need for greater protection from hackers and

other cyberspace culprits... Security is a no-brainer (Fuscaldo, 2005). Information security is one of the top drivers of technology spending. The market for security-related hardware, software, and services is expected to continue to experience healthy growth, swelling to more than \$45 billion in revenue by 2006 from just \$17 billion in 2001, according to a recent study by market researchers at IDC (Roberts, 2003).



*Graphic 1 (Fuscaldo, 2005)

Information technology managers should work closely with higher management within their business organizations in order to develop a dependable plan of action concerning security spending. It is impractical for most organizations to spend the majority of their technology budget on security, because other areas of operation essential to the organization would lack improvements needed to maintain stable competition with outside rival competitors. However, both upper business management and IT managers must realize that increasing security is necessary to comply with regulations and to ensure integrity, availability, and confidentiality.

External Security: The Darkened Outside

Since the dawn of networking capabilities in information technology, there have always been those individuals who desire to find ways around network boundaries. Perimeter security, as it is most commonly known, is the first line of defense against outsiders trying to compromise a business's network infrastructure.

Hackers and Network Configuration

With the evolvement of personal desktop computers and tools used by hackers, such as trojans, sniffers, spoofers, and keyloggers, information technology managers must implement solutions to thwart attacks upon their business's information systems. It is impossible for hardware and software manufacturers to ensure that their products are flawless and contain no security vulnerabilities. Therefore, IT managers must stay ahead of cyber-criminals by patching security vulnerabilities as they are uncovered and a patch is released by the vendor.

IT managers must also oversee the installation and configuration of the network to make certain that all elements of the system are appropriately configured and accurately secured according to corporate standards. Known vulnerabilities must be blocked and strong passwords should be used on network configuration administration utilities. IT managers are responsible to research the latest advancements in firewalls and other security applications and recommend products and services to be purchased.

Viruses, Spyware, and Adware

With over 53,000 known viruses in circulation throughout the world today, virus protection and detection should be atop the list of concerns for all IT managers. Since the introduction of desktop computing with network capabilities, cyber-criminals have tried

to exploit vulnerabilities and deliver malicious programs designed to damage information systems. While viruses seem to be most widespread among home users, corporate environments must never become lax when it comes to defending an organization's information systems against viruses. A virus released within a firm's information system could cause massive data corruption which, depending on the reliance of the system and its data, could severely interrupt the firm's operations. Spyware is another major issue facing business information technology managers. Roughly, approximately twenty-five percent of all business desktop computers are affected by spyware.

One of the latest trends in cyber-crime is the so called "zero-day" attack. These types of attacks are ever-increasing. Zero-day attacks are used by hackers to take advantage of vulnerabilities before hardware or software vendors can release a security fix. Unfortunately, due to the nature of the attacks, information technology managers cannot secure the vulnerability prior to the attack. However, an IT manager that has considered other methods of security outside of external security has a relatively safe system even if the perimeter is breached.

Internal Security and Control

Internal security is a growing area of concern for most information technology managers. Congressional legislation passed in recent years following the numerous corporate scandals has intensified responsibilities of internal control. Information technology managers are responsible for maintaining corporate data availability and confidentiality.

One of the driving forces that led to the boom of the information technology revolution was the electronic availability of data and information. Relational databases made electronic storage and retrieval faster than any prior method of information archiving. IT managers must maintain adequate network operations to effectively operate a firm's information systems. Data transmission must be reliable, secure, and available to those needing to store new data and retrieve old data.

As previously stated, information technology managers must also ensure that the data contained in their systems is confidential. Privacy is and will continue to be one of the hottest topics of information technology debate. Congress and other legislative bodies have passed numerous laws in recent years to enforce data privacy. The California Database Security Breach Notification regulation requires that companies with customers in California notify their customers if they have discovered a breach in their databases that could expose the customers to identity theft (Antonopoulos, 2005). IT managers must consider implementing security policies data such as user authentication or early breach detection systems on critical private.

Outsourcing: The Key to the Future of Security?

Recent changes in management of information technology have led to a trend of outsourcing security. According to [the September 2005] CIO Insight survey, only fourteen percent of companies currently outsource security – and only one percent plan to within the next twelve months (D’Agostino, 2005). Table 2 provides a summary of advantages and disadvantages provided by outsourcing.

	<i>Advantages</i>	<i>Disadvantages</i>
Information Security Infrastructure	Even if the information security function is managed in-house, it is often beneficial for a third party to design, implement, and/or validate implementation of the infrastructure.	Third parties might over-engineer the solution and/or propose a solution that may be better suited to third-part implementation and management.
Physical Security	Generally an organization will find it more economical and less burdensome to use third-party guard services to secure a facility and check identities and authorized destinations (who they came to visit) of those wanting access.	A significant amount of trust is put on these outside services, so that when there is a problem it can be doubly dangerous because the outsider has insider access.
Operations Management	Certain operational functions, such as payroll processing, are specialty commodity services and are generally outsourced by all but the very smallest or largest of organizations.	Loss of control is a considerable concern here, as is reduced flexibility.
Protection Against Malicious Software	Outside services generally have the size and scope to be able to provide a broader perspective. Also, they have an incentive to keep their antivirus signatures very current and to screen out a high proportion of spam and similarly unauthorized messages.	If there are false positives, it may be more difficult to retrieve quarantined e-mails from outsourcers.
Network Management	There have been quite a number of highly visible, large-scale and successful outsourcing programs in which a third part is assigned full responsibility for managing large firms’ networks. There are considerable savings and other benefits to be had, especially for 24/7 global networks.	High dependency on an outsourcer for such a critical area might lead to significant problems was the provider to go out of business.

*Table 2 (D’Agostino, 2005)

Outsourcing will continue to grow in the future of information technology. Financially, outsourcing is beneficial for both the business and economy as a whole. The business firm is provided with the latest in security technology with the added bonus of having 24/7 monitoring. Most firms would be unable to financially support on-hand security personnel with the same capabilities and skills provided by a third-part source. Outsourcing adds an extra layer to the supply chain, and that typically means one more safety cushion (Craumer, 2002). While IT jobs are lost through outsourcing, more jobs are created because costs are lower to IT companies, allowing them to spend money on other things, which in turn results in lower prices, lower interest rates, and higher spending throughout the economy, spurring job creation...(Carlson, 2005).

Managing Outsourced Security

IT managers must weigh the benefits and costs associated with outsourcing prior to making a decision. Any vendor will tell you that trust is fundamental when it comes to outsourcing security (D'Agostino, 2005). Outsourcing is a gigantic step for an organization to take because it relinquishes control of a major portion of the overall scheme of the business's information systems. The firm becomes totally reliant on the third-party. IT managers must be careful to structure deals with outsourcing companies in order to avoid a bad or weak deal that leaves the firm with security vulnerabilities. Larger firms can hire a CRO to manage outsourced security. CRO is short for Chief Resource Office. The CRO will be the technology executive who oversees all of [the] company's outsourcing agreements and makes sure all [the] vendors cooperate (Dignan, 2004).

Conclusion and Analysis

Management has a bright future in the field of information technology. Effective IT managers must be willing to research the most up-to-date developments to provide their businesses with the latest technology advancements. They will give their organization the cutting edge advantage to compete with shrinking markets.

As information technology advances security will continue to be an issue that will plague all managers in IT. Management cannot forget the three essential characteristics that formulate IT security strategy: integrity, availability, and confidentiality. The future will hold a more stringent governance of data management as state, federal, and potentially international legislation is created to secure transferred and stored data.

As long as there are information systems of data to be maintained and exchanged, information technology will lead the field in providing that data. Management will be the key to maintaining an effective IT strategy that will lead the world to the next generation of communication and data exchange.

Works Cited

- Antonopoulos, A. (2005). Are California's database breach notification rules going national?. *NetworkWorld.com*. Retrieved November 17, 2005, <http://www.networkworld.com/newsletters/datacenter/2005/0425datacenter1.htm>.
- Carlson, C. (2005). ITAA study pushes for outsourcing. *eWeek.com*. Retrieved November 17, 2005, http://www.eweek.com/print_article2/0,1217,a=164056,00.asp.
- Ciampa, M. (2005). Security+ guide to network security fundamentals (2nd ed.). Boston: Course Technology.
- College of information technology. *Georgia Southern University*, Retrieved November 1, 2005, <http://cit.georgiasouthern.edu/about.php>.
- Craumer, M. (2002). How to think strategically about outsourcing. *Harvard Management Update*.
- D'Agostino, D. (2005). Outsourced security: an idea CIOs loathe. *CIOInsight.com*, Retrieved October 15, 2005, <http://www.cioinsight.com/article2/0,1540,1855228,00.asp>.
- Dignan, L. (2004). Outsourcing overseers needed. *eWeek.com*. Retrieved October 20, 2005, http://www.eweek.com/print_article2/0,1217,a=136860,00.asp.
- Fuscaldò, D. (2005). Tech spending is on track to rise as worries about security mount. *The Wall Street Journal*. B3.
- Lucas, H. (2005). Information technology strategic decision making for managers. Hoboken: John Wiley & Sons, Inc.
- Robbins, S., & Coulter, M. (2005). Management (8th ed.). Upper Saddle River: Pearson Prentice Hall.
- Roberts, P. (2003). Security spending swells. *PCWorld.com*, Retrieved November 5, 2005, <http://www.pcworld.com/resource/printable/article/0,aid,109221,00.asp>.