Global Information Assurance Certification Paper

Achieving Competitive Advantage using Information Security

GIAC Security Essentials Certification (GSEC)
Assignment 1.4c
Option 1

Ezekiel W. Chhoa
January 31, 2005

Table of Contents

Abstract 3
Introduction 4
I. Competitive Advantage 4
Quality 4
Efficiency 5
Innovation 5
Customer Responsiveness 5
II. The Current State of Information Security Strategy 5
III. Trends in Information Security and E-Commerce 6
Growth in E-Commerce 6
Growth in Threats 7
Growth in the Importance of Information Security 8
Growth in Information Security Staff 9
Growth in Information Security Products 9
Paradigm Shift – Value Realized 9
IV. Case Study: Evolution of Safety in Automobiles vs. Evolution of Information Security 9
V. Achieving Competitive Advantage Using Information Security 11
Management Strategies 11
C-I-A 12
Risk Assessment 13
Data Classification 13
Threats, Vulnerabilities and Risk 13
Risk Assessment 14
Defense-In-Depth 14
Network Layer 15
Host Layer 15
Application Layer 16
Security Awareness Training 17
Security Policy 17
VI. Examples of Competitive Advantage Using Information Security 17
Virtual Keyboard 18
Digital Stamp 19
One-Time-Password Token 19
Customer Authentication 20
Conclusions 20
List of References 22

Abstract

The line of sight between information security cost and the bottom line may be nebulous, and the return on investment may be difficult to quantify; however, information security can be used as a competitive advantage. Recent trends indicate that an increase in the number of risks and customer awareness is leading to increasing pressure on organizations to deliver secure solutions. Understanding that information security is both a business and technological driver is essential to leveraging information security's potential as a competitive advantage. Organizations that are able to build security into their business model and cascade it throughout the organization will foster an environment that is secure and competitive.

Introduction

Information security is inherently an overhead cost. Why then, are a select few companies able to use information security to positively impact the bottom line, while the majority of companies spend large sums of money with seemingly little or no returns? In a field where success is often equated with "nothing happening" or "business as usual," it is not surprising to find confusion in the minds of businesspeople as the line of sight between information security and the bottom line is seemingly blurred. Nevertheless, the success of a minority can inspire a fundamental change in the way information security is perceived. As the trends seem to suggest, the emphasis given to information security is likely to increase, rather than to fade.

I. Competitive Advantage

In order for us to understand how some companies realize value using information security, we must first have a good understanding of competitive advantage. Competitive advantage is achieved when a company is able to sustain profits that are higher than the industry average.[1]

The two main types of competitive advantage are cost advantage and differentiation advantage.[2] If a company can consistently deliver a product that is of lower cost, or can provide value in a unique way to its customers, it is able to attain competitive advantage. In order to achieve lower cost or differentiation, a company must use four generic building blocks: quality, efficiency, innovation, and customer responsiveness.[3] If any company can achieve superiority in any of these areas, they will be able to achieve lower cost, or differentiate their product.

Quality

Quality refers to a product's ability to carry out its designated purpose in an excellent manner. In terms of information security, quality is achieved when systems are performing the way we expect them to: the system is available for use at the users' demand and the system functions without any adverse instances. As an industry matures, consumers will increasingly demand high quality products or services. As such, quality becomes an essential part of competitive advantage; it becomes the foundation upon which the other three areas must build.

---

[1] QuickMBA.com. "Competitive Advantage." 3 Jan. 2005. <http://www.quickmba.com/strategy/competitive-advantage/>

[2] Porter, Michael E., Competitive Advantage: Creating and Sustaining Superior Performance, New York: The Free Press, 1985.

[3] Hill, Charles W. L., and Gareth R. Jones. Strategic Management: An Integrated Approach, 5th ed. New York: Houghton Mifflin Company, 2001.

Efficiency

Although a secure environment may not provide companies with gains in efficiency per se, the consistent availability of a system negates any downtime that would cause inefficiencies in business processes.

Innovation

Typically, the general population does not think that innovation and information security go hand in hand, but the reality is that many aspects of information security will provide a company with a novel way of providing products and services, or even a novel way of doing business. Innovation is an integral part of the overall competitive advantage because it provides the company with a unique edge over their competitors. Since the information security field is still in its infancy, the opportunities for discovering innovative ways of incorporating information security into the overall business strategy are abundant.

Customer Responsiveness

As the world economy embraces new technology as an essential business driver, customers will increasingly expect companies to deliver their products and services using new technology over a secure channel. Companies that can correctly identify and meet the needs of the customer will gain a competitive advantage.

II. The Current State of Information Security Strategy

Historically, the information security discipline was confined to the realm of the military. The need for secure methods of communication is vital to the military's success. However, as networks proliferated and the Internet was moved into the public domain, it became increasingly clear that the need for secure information is everyone's concern.

Due to its roots, information security personnel have historically evolved from network administrator type roles. Since this field is arguably still in its infancy, the current role of information security is often misunderstood. Companies do not have a good grasp of how information security fits into its overall strategy. Evidence for this fact is shown by a survey conducted by Ernst & Young. [4] The results show that the information security department has varying reporting structures. In at least 42% of all cases, information security reports into IT, with only 27% reporting directly to top executive management. The traditional mind-set that information security is predominantly an IT concern is still pervasive

[4] Global Information Security Survey 2004. Ernst & Young. 3 Jan. 2005. <http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf>

throughout organizations.

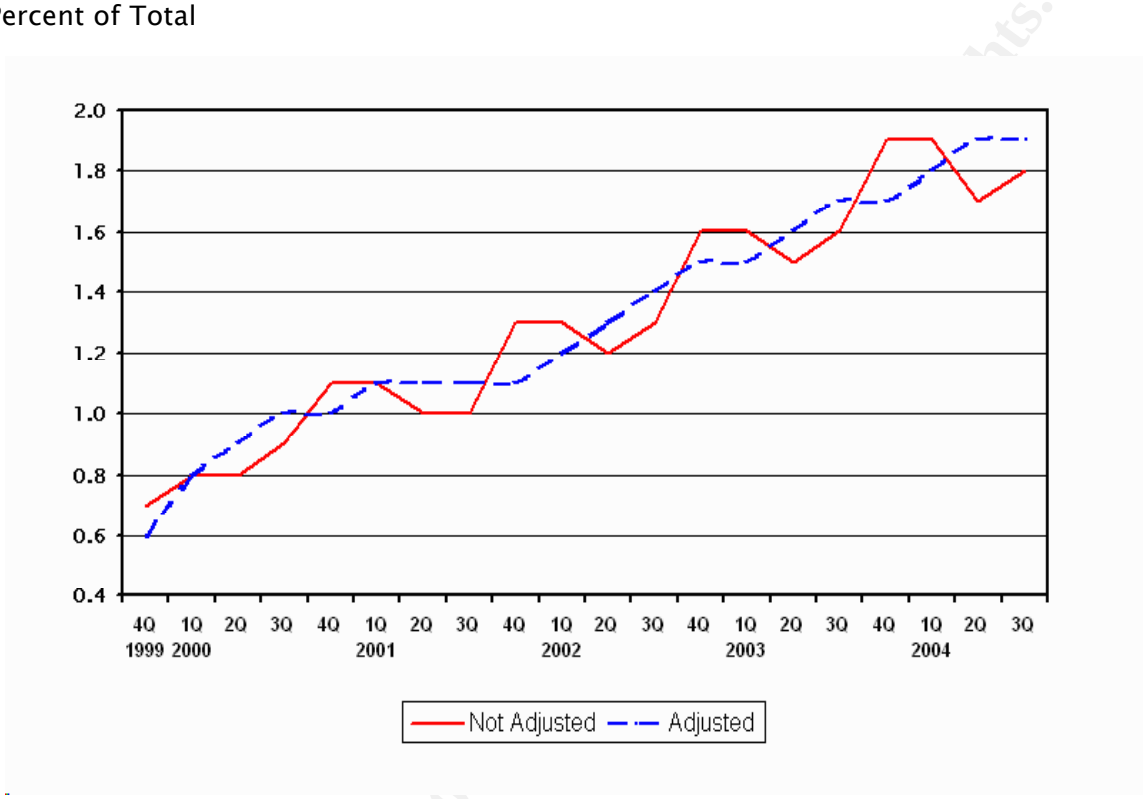
One reason why organizations do not think of information security as a business concern may be due to the difficulty in perceiving value from information security. One role of information security is to ensure that business runs smoothly with no disruptions to normal operating procedures. Information security is a background operation; it is only when a system fails that the spotlight is focused on security. In addition, since information security does not traditionally generate revenue, it is perceived as adding to the cost of doing business.

III. Trends in Information Security and E-Commerce

Growth in E-Commerce

E-Commerce has no doubt grown at a rapid pace since the adoption of the Internet as a viable marketplace. As shown in the graph below, consumers are turning increasingly towards the Internet for retail purchases:

Estimated Quarterly U.S. Retail E-commerce Sales as a Percent of Total Quarterly Retail Sales: 4th Quarter 1999– 3rd Quarter 2004



Source: US Census Bureau (http://www.census.gov/mrts/www/current.html)[5]

Figure 1: Growth of E-Commerce Sales

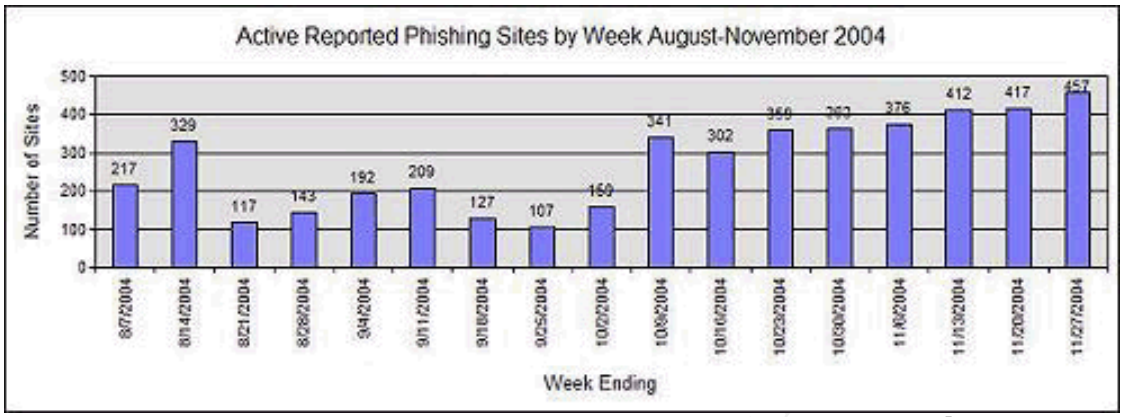
In an independent study, US online retail sales are predicted to reach $65 billion in 2004, and continue to grow at an annual compounded rate of 17% through 2008, at which time, sales are expected to top $117 billion.[6]

Growth in Threats

The growth of e-commerce signifies a shift in the way consumers are purchasing; therefore, the importance of having a secure environment for which the marketplace can flourish increases to match the increased demand. The proliferation of worms, viruses, and phishing attacks is a very clear sign that security must be a priority if e-commerce continues to grow. In the graph below, we see an overall increasing trend in the number of phishing attacks. Essentially, a phishing scam involves an attacker sending an email to the victim

[5] United States. United States Census Bureau. Department of Commerce. Quarterly Retail E-Commerce Sales 3rd Quarter 2004. 3 Jan. 2005. <http://www.census.gov/mrts/www/current.html>
[6] "Online Retail: Press Release 01-20-04." Jupitermedia Corporation. 3 Jan. 2005. <http://www.jupitermedia.com/corporate/releases/04.01.20-newjupresearch.html>

posing as a legitimate company. The email directs unsuspecting victims to a website where they enter their authentication credentials. The attacker then steals the credentials for their own nefarious use.



Source: Anti-Phishing Working Group (http://www.antiphishing.org)[7]

Figure 2: Increasing Phishing Attacks

Growth in the Importance of Information Security

The evidence that shows an increasing awareness of the importance of information security is abundant. In a recent survey conducted by India's National Association of Software and Service Companies (NASSCOM) and the Information Technology Association of America (ITAA), an average of 79% of customers surveyed responded that they were "more concerned [about information security] than ever before."[8]

The same study shows that an average of 79% of companies surveyed believed that information security is a key differentiator, while 70% actually use information security as a critical selling point while marketing their products and services.

[7] Anti-Phishing Working Group. "Phishing Activity Trends Report: November 2004." 3 Jan. 2005. <http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20November%202004.pdf>

[8] NASSCOM-ITAA. "Information Security offers a considerable competitive advantage: NASSCOM- ITAA Poll." 3 Jan. 2005. <http://www.nasscom.org/download/Opinion_Poll_Infosec_Summit.pdf>

Growth in Information Security Staff

In response to the increasing need for information security, the number of people working in the information security field is expected to grow rapidly to 2.1 million people worldwide by 2008 at a compounded annual growth rate of 13.7% from 2003.[9]

Growth in Information Security Products

In addition to the abundant array of products offered by traditional security companies such as McAfee and Symantec, Microsoft has recently announced that it will use security as a competitive advantage.[10] The arrival of its Service Pack 2 for Windows XP includes many security initiatives most notably of which are the Windows firewall, 802.11 wireless enhancements, and a pop-up blocker. These initiatives make a bold statement about the importance of security to Microsoft, and indicate a change in the attitude of vendors in general. Security is now an important component of many companies' overall product offerings.

Paradigm Shift – Value Realized

The mounting importance and attention given to information security is underscored by a paradigm shift in the business world. Executives are beginning to realize that information security is not simply an overhead cost, but rather a vehicle in which the traditional profit equation can be applied. Innovative security initiatives can create a stable environment in which costs are reduced, as well as provide a platform for generating new revenues. A secure product or service translates into increased quality as a response to customer demand.

IV. Case Study: Evolution of Safety in Automobiles vs. Evolution of Information Security

A comparison can be made between the evolution of safety in automobiles and the evolution of information security. The parallels are striking, and there are lessons to be learned from the evolution of safety in the automotive world.[11]

Seat belts, or safety belts, were first invented by Volvo in 1849; however, they were certainly not in widespread use until much later.[12] The attitude that many car manufacturers took was that the motor vehicle accidents causing death or

[9] "Global Workforce Study: Press Release 11-8-04." (ISC)² Inc. 3 Jan. 2005. <https://www.isc2.org/download/PressReleases/Release%20Global%20Workforce%20Study.pdf>
[10] Evers, Joris. "Microsoft to Pitch Security as 'Competitive Advantage'." Network World Fusion. 07 Aug. 2004. 3 Jan. 2005. <http://www.nwfusion.com/news/2004/0708microtopi.html>
[11] Anon. Personal interview. 17 Dec. 2004.
[12] Bellis, Mary. "The History of Seat Belts." About.com. 3 Jan. 2005. <http://inventors.about.com/library/inventors/bl_seat_belts.htm>

injury were solely the responsibility of the driver(s) involved. As the death toll increased, this attitude slowly disappeared.

In the early days of the commercial Internet, security was seen in the same way. As websites grew in number, the onus was on the user to ensure that their systems were not compromised. However, once e-commerce began to grow in importance, the attitude that the user must protect himself or herself began to wane.

In the 1950s, car manufacturers started to offer seat belts as an option in their automobiles. While there was support for the adoption of seat belts by medical communities, the population at large saw seat belts as more of a novelty item, rather than a breakthrough in automotive safety. The interest of the general consumer was focused on car design and the amount of power available to them.

Similarly, while security products such as firewalls and antivirus software were available, the majority of consumers saw them as a novelty item, and did not understand exactly what they were for or why they should use them. It was not until the propagation of worms and viruses that security products became widespread.

By the 1960s, safety in automobiles garnered attention from the government. The United States Department of Transportation was created on October 15, 1966, and a separate, independent organization called the National Transportation Safety Board was created a year later.[13] The creation of these government organizations held automobile manufacturers accountable for the safety of the products they sold.

The world of e-commerce saw rapid growth in the late 1990s and early 2000s. Companies began selling their goods and services online, and many customers began embracing the new and more convenient technology. Information security attracted the attention of government regulators and regulations were enacted to provide security for customers' privacy and proper handling of sensitive information. The Gramm-Leach-Bliley Act (GLBA) ensures that financial data is handled properly while the Health Insurance Portability and Accountability Act (HIPAA) addresses the privacy of health information. More recently, following the Enron and WorldCom scandals, the Sarbanes-Oxley Act in the US, and Bill C-198 in Canada were both passed to address accountability in disclosing financial and accounting information. While none of these regulations are directed solely at electronic information, the implications of these regulations certainly have a great impact on information security. Government regulators are holding companies responsible for the secure handling of private customer information.

[13] Wikipedia. "Car Safety." 3 Jan. 2005. <http://en.wikipedia.org/wiki/Car_safety>

In the 1970s, the availability of seat belts was almost ubiquitous across the board for car manufacturers. New safety innovations were springing forth, and by the 1980s, the safety movement was in full swing. Car manufacturers came up with innovative and effective safety measures such as air bags, side impact beams, anti-lock braking systems, and more recently, traction control systems.

Once the average consumer understood the importance and necessity of safety in the automobile, car manufacturers immediately started marketing the safety of their products. They used safety as a differentiator among their competitors. Companies such as Volvo, Mercedes-Benz, and Subaru have all built their reputation on their safe cars. Safety was built into the corporate brand, and consumers demanded safety in their automobiles.

An important catalyst to fuel customer interest in automobile safety comes from Ralph Nader and the consumer movement. Nader's advocacy for consumer rights prompted customers to take notice, governments to formulate new legislation, and companies to take more responsibility for their products. Perhaps a similar advocate for information security on the Internet would promote quicker action by the public, government and businesses to mitigate losses.

We are at a point in time when the world of information security is coming to the forefront. Consumers are starting to understand the importance and necessity of secure applications in e-commerce. Companies that can successfully market their product as being secure using innovative means will be able to differentiate themselves from the competition and incorporate safety into their brand. Also important to note that while the maturity of automotive safety took several decades, developments in information security have only taken several years. If companies are to take advantage of using security as a competitive advantage, they may only have a small window of opportunity.

V. Achieving Competitive Advantage Using Information Security

Management Strategies

Although the beginning of capitalism as a political system is often debated, for as long as the buying and selling of goods and services have existed, there have been management strategies. Academics, management gurus, and business leaders have all had ideas to improve management techniques. Ideas such as Total Quality Management (TQM), Benchmarking and Business Process Re-engineering (BPR) have all made their mark in the annals of management practices. Unfortunately, many companies adopt the latest concept without seriously considering whether or not the proposed initiative fits with their overall strategy. Then, when the idea produces little or even negative results, questions arise as to why the latest and greatest strategy failed. Companies should examine any idea thoroughly for compatibility with the overall business model

and strategy before dedicating resources to apply the scheme throughout the organization.

Three lessons are to be learned from the business concepts that can be applied to information security. First, information security must be incorporated into the business model and strategy. A traditional clothing retailer whose strategy is to cater strictly to its clients face-to-face will have different information security needs than a large, complex financial institution that transfers millions of dollars electronically to other financial institutions around the world.

Second, information security is an executive level priority. Just as management ideas have gained the attention of senior business leaders, the same level of attention must be given to information security. If information security is deemed to be a vital component of the overall company strategy, commitment must come from the very top to provide resources and to drive the initiatives.

Third, management strategies that have been successfully deployed in organizations morph from being just an idea into a management philosophy that is ingrained in the corporate culture. Similarly, information security is not meant to be a management idea. If it is truly vital to the organization, information security should permeate every aspect of the business.

A note of clarification: the comparison between management strategies and information security was made to gain insight on how information security can be applied effectively. While the management ideas mentioned are generally business or operational concerns, information security has the added component of technical staff assigned to handle technical issues, in addition to business concerns.

C-I-A

Once information security is indeed determined to be an integral part of the overall strategy, and business executives have committed to providing resources, the next step is to identify what we are trying to secure. Traditionally in information security, three aspects of data are to be protected: confidentiality, integrity and availability.[14]

Confidentiality refers to the disclosure of information. In some instances, it is vital that the information is not disclosed in any way to unauthorized sources. Integrity refers to information being kept accurate. That is, keeping the information secure from unauthorized changes or deletion is important. Finally, information or systems must be secured so that they are available when needed.

Each of these three elements may vary in degrees of importance depending on

[14] SANS Institute. Track 1 – SANS Security Essentials. Volume 1.2. SANS Press, Sept. 2004.

the organization, but all are important. For example, availability is most important for an online merchant, while confidentiality is most important in the healthcare industry. Each organization must carefully examine its business and determine how it is protecting the confidentiality, integrity and availability of its information, and focus more resources on the element that is most important to the business.

Risk Assessment

After we understand which aspect is the most important to the business, it is important to prioritize resources. To guarantee 100% security for any given system would be difficult and costly. Consequently, security resources are most effective when they are prioritized according to risk.

Data Classification

One method to prioritize risk is to classify the data that we are protecting. The classification of the data should be based on the impact or damage caused to the organization in terms of confidentiality, integrity, and/or availability. An example of a low risk data class would be the location of a retail outlet. Conversely, an example of a higher risk data class would be the location of a data centre.

A suitable number of data classes should be established for the data. Some organizations such as the government may have multiple classes of data, while other organizations only have a few. Again, depending on the organization it may or may not be useful to have a structured and formalized procedure or policy surrounding data classification. Regardless, all organizations should understand the principle that some data require more security than others.

Threats, Vulnerabilities and Risk

We must protect our data and systems from threats and vulnerabilities. A threat is an external source of danger to the system and/or data that may or may not be a malicious attack. For example, threats include viruses, and worms, but they also include power outages and natural disasters. These are all examples of external sources of danger to the system or data.

Internal sources of weakness are called vulnerabilities. Examples of vulnerabilities include weak physical security and poor patch management. However, although vulnerabilities may exist in any given environment, they may not pose significant dangers. For instance, even if a system was poorly patched, if it was a standalone machine that was not connected to the network and used solely to allow employees to play games, it would not pose a significant risk to the organization.

The combination of threats and vulnerabilities is what causes risk to manifest

itself in an organization. The basic formula for risk is:

Risk = Threat x Vulnerability[15]

According to this formula, even if one of the two variables (threat or vulnerability) was exceedingly great, it would not matter if the other one is zero; there would still be no risk. Only if both a threat and vulnerability were present would there be a risk factor.

Risk Assessment

The best method for effective resource allocation is through risk assessment. The purpose of a risk assessment is threefold. First, the risk assessment allows for the identification of specific areas of risk. Second, it allows us to determine the impact of the risk to our systems and to the business in general should it be compromised. Third, it allows us to identify the controls that are necessary to mitigate the risks.

There are several risk assessment methodologies available including SPRINT, OCTAVE and COBRA. Essentially, these risk assessment tools allow the users to:

1. Ask a predetermined set of questions used to identify any risk areas
2. Determine how risky each area is by separating them into high, medium and low categories
3. Establish controls to mitigate the risks.

Usually, several stakeholders are involved in the process including business representatives, IT staff, and information security professionals. This type of qualitative risk assessment is used the majority of the time due to its ease of use. However, since qualitative analysis is somewhat subjective, quantitative risk assessment methodologies are available to provide a more valuable assessment in terms of tangible dollar values.

Quantitative and qualitative risk analysis techniques can be much more advanced and complex than presented here. However, for our purposes, to understand that a risk assessment must be performed to effectively allocate resources to the highest risk areas and to define mitigating controls is sufficient.

Defense-In-Depth

A multi-layered approach called Defense-in-Depth must be taken to secure information.[16] To have a single firewall as the sole method of protecting the organization's systems is not enough. The more layers that are protecting the system, the more difficult it will be for any malicious attack to compromise the

[15] Ibid., p. 23.
[16] Ibid., p. 12.

system. Even if the many layers are not sufficient to protect the information, the multiple layers will slow the attack down. This allows time for the attack to be detected, and hopefully remediation can take place immediately to minimize damages. We will examine some examples of each protective layer but this is not meant as a comprehensive review of how each layer should be secured. Rather, the examples will illustrate how a few good practices will go a long way to ensure Defense-in-Depth.

Network Layer

The outermost layer is the network layer. Here, devices such as routers, firewalls and intrusion detection systems can be employed to drop suspicious packets before they enter.

Data is transmitted across networks using packets. Each packet is made up of bits of data containing address information and the actual data. A router is a perimeter device that connects logical networks used to forward or block packets from entering the network depending on the address of the packet. Since routers determine the various paths a packet can take, placing certain rules on the router will provide the outermost defense against malicious attacks.

A firewall acts similarly to a router in that it also looks at packets and determines whether or not they are allowed in to the network. However, the difference lies in the fact that firewalls do not route traffic. While routers can be analogous to traffic cops, firewalls can be analogous to customs officers at the border crossing. Firewalls examine each packet that comes through, and filters all inbound and outbound traffic, preventing malicious packages from passing through.

Intrusion detection systems (IDS) are used to monitor activity on the network (or host). The tool allows an organization to detect any attacks against their systems but does not prevent the attack from happening.

Host Layer

The second layer is the host layer. Personal firewalls, proper patch management and minimizing services will provide further protection. Since we are taking a layered approach, tools such as IDS and firewalls can be used on the host as well. A firewall or IDS on the host would not monitor traffic on the network, but instead, traffic that is local to the host.

Patches are releases by the vendors that fix a known vulnerability. For example, Microsoft releases updates that fix vulnerabilities found in their Windows operating system. Since these are publicly known vulnerabilities, anyone can take advantage of them to compromise systems. Keeping up to date on the latest patches and managing them correctly will help secure the host.

Network traffic enters a host via open ports; consequently, any malicious attack will enter a host system via an open port before it can access any information. Closing off any unnecessary ports will minimize the chances of a successful attack. Services such as HTTP, Telnet and FTP all utilize ports to connect to other machines. Therefore, identifying which services are essential, and only allowing those services to run will go a long way to increase the security of a host machine.

Application Layer

The final layer before an attack can reach the information is on the application level. Good programming will ensure issues like proper error checking and user authentication are handled correctly, thus providing the final layer of protection.

When coding an application, it is important to provide proper error checking. When code is written without a thorough examination of all areas where something can go wrong, bugs in the program may appear. A malicious attack can take advantage of these bugs and cause a buffer overflow condition resulting in a denial of service attack, shutting down a system. Very simply, every application takes an input and stores it in a buffer (region of memory). If there is no error checking, an attacker can input data that exceeds the allotted buffer space and cause the system to crash resulting in denial of service. Worse yet, the attacker can inject malicious code and trick the system into executing the code.

Proper access controls will also help secure the system. Access should only be granted to users who have the proper authority. In addition, users should only be given the minimum level of access that is needed. This is known as the Principle of Least Privilege. One common method of access control is through the use of passwords. In addition to a strong password policy, the application itself can check for proper passwords. Some generally accepted rules for passwords are:

- Account lockdown after 3 unsuccessful attempts
- Passwords should contain alphanumeric and special characters
- Passwords should be changed at regular intervals (at least every 60 days)
- None of the previous 5 passwords can be re-used[17]

The broad array of techniques or good practices discussed is simply scratching the surface on how to employ Defense-in-Depth best. Each layer contributes to the overall security of the system and information. Although information security is very much still in its infancy, to postulate that information security will evolve into an independent discipline, with its own set of theories and body of

[17] Ibid., p. 143.

knowledge, would not be out of line.

Security Awareness Training

Despite fostering a secure environment via Defense-in-Depth, the best plans may fail if people refuse to take ownership of security. Security is everyone's responsibility. For example, despite the best security, a customer may fall victim to a phishing attack. If uneducated, staff may fall prey to social engineering attacks, where attackers will use lies and deception to gain access to information. Lack of security knowledge is often the weakest link in any system. In order to strengthen this link, a good security awareness program should be put in place to train both staff and end customers alike. Simply being aware of the risks and dangers will help a great deal in deterring attacks directed at naïve users.

Security Policy

A good security policy will complement security awareness training. Security policies are meant to protect both information and people. Instead of being a set of rules and regulations, a security policy should be written to enable and empower employees to protect information: it details what must be done to protect the information and allows employees to carry it out.

Good security policies are concise and easy to understand. Although security policies will cover some technical issues such as authentication, acceptable use and disaster recovery, the security policy should also be supportive of the overall business strategy. A security policy should be a natural extension of the security conscious culture adopted by senior management.

VI. Examples of Competitive Advantage Using Information Security

Although the information security field is not yet mature from a business perspective, it is vital to "use good security to promote the brand."[18] A recent study conducted by Interbrand, and published in BusinessWeek Magazine lists estimated values for the top 100 global brands.[19] These valuations emphasize the need to protect the brand by having good information security practices. After all, any security breach would have a direct impact on any organization's reputation and brand.

Short Message Service (SMS) authentication is in place at a financial institution in Singapore where a short text message is sent by the customer's cellular phone to authorize important transactions such as fund transfers. In alignment with our Defense-in-Depth approach, SMS authentication is used in conjunction with other authentication schemes to provide two-factor authentication.[20]

---

[18] Anon. Personal interview. 17 Dec. 2004.
[19] Interbrand. "Cult Brands." BusinessWeek. 9-16 Aug. 2004. 3 Jan. 2005. <http://www.ourfishbowl.com/images/surveys/BGBleaguetable_final_.pdf>

In all areas of the world, a major global bank has instituted policies to address customer authentication.[21] Variants of the virtual keyboard and random character challenge have appeared in the UK, France, and different areas around the world in an effort to provide robust authentication. Virtual keyboards are graphic user interface (GUI)-based keyboards that prompt customers to enter their authentication information using a mouse to click characters on a screen rather than on a physical keyboard. This discourages any keystroke logging (programs that record characters typed on the physical keyboard) and shoulder surfing (people watching the victim over their shoulder to see what they are typing) attacks. Random character challenge is an innovation that puts a twist on the traditional password. Instead of entering their full password, the system will prompt the user to enter specific characters within their password. For example, the system may ask the user for the 4th, 8th, and 1st characters in the password. The next time the user logs in, the system may ask for the 1st, 2nd, and 6th character. This is an added security feature to make it more difficult to crack the authentication credentials.

One executive for a bank in Brazil has implemented some of the most innovative security solutions in the financial industry.[22] In Brazil, Internet banking fraud is in the news frequently, and the general population is very conscious of the risks. In the past year alone, Internet fraud has increased fourfold. In response to this increase in malicious activity, and to increase customer satisfaction, the Brazilian bank has stepped up its efforts to protect its customers.

Virtual Keyboard

Initially, the virtual keyboard was implemented to discourage keystroke logging attacks. Unfortunately, the latest keyloggers all come equipped with screen capture capabilities, where a picture of the screen is captured as the user is authenticating to steal login credentials. In response, the Brazilian bank has implemented the codified PIN. Instead of clicking the actual PIN on the virtual keyboard, the customer types in a letter from the randomly generated table that changes with each login:

[20] Anon. Personal interview. 17 Dec. 2004.
[21] Anon. Personal interview. 17 Dec. 2004.
[22] Anon. Personal interview. 30 Dec. 2004.

0 = W
1 = E
2 = M
3 = T
4 = O
5 = D
6 = X
7 = S
8 = Z
9 = B

Figure 3: Sample Codified PIN Table

In this example, if the customer's PIN is "1234", they would click "EMTO" on the virtual keyboard. Asterisks appear each time a character is clicked to further protect the privacy of the PIN. The virtual keyboard also appears randomly on the user's screen each time they log in. This feature along with the codified PIN will foil any attempted screen capture attacks.

Digital Stamp

The digital stamp was applied by the bank to combat the increasing frequency of phishing attacks. Each customer account is issued a digital stamp. The stamp is an image unique to that account. It appears when an account number is typed during the Internet banking login process. Clients are instructed to input their password only if they recognize their digital stamp. Once they have confirmed that the digital stamp is correct, the virtual keyboard will be displayed. Since only the bank has access to each account's digital stamp, this will prevent phishers from conning customers successfully. These stamps vary in shape, size and color and can be marketed in such a way as to attract new customers. Customers can be allowed to create their own stamps or special edition stamps with different themes can be created.

One-Time-Password Token

One time password (OTP) tokens are distributed to all of the bank's commercial clients in Brazil, and they are mandatory if the customer would like to perform financial transactions online. The token is a physical piece of hardware given to each client that will display a new password that changes at set time intervals. Every time the client wants to login, the system will prompt the user for the password displayed on the token. This ensures that the password is used only once which secures against stolen or hacked passwords. The tokens are used in conjunction with the standard username and password combination to provide two-factor authentication. The combination of authenticating the user via something they know plus something they possess increases the level of

security. The success of these tokens in Brazil has translated into a dramatic decrease in the number of fraud cases, and increased customer satisfaction and confidence in the bank. In fact, the Brazilian bank's move towards mandatory OTP tokens has prompted their customers to demand other banks to issue similar tokens.

Customer Authentication

Through such initiatives, the financial institutions profiled have demonstrated their dedication to providing secure innovative solutions that are of high quality and efficient in response to customer needs. However, most innovations in customer authentication are largely dependent on customer awareness and acceptance of the technologies. This underscores the importance of security awareness training, not only for staff, but for customers as well.

Customer authentication is one area of information security that is becoming increasingly competitive. In September of 2004, AOL announced that they will offer OTP tokens to its customers as an added security feature to protect from fraud and identity theft,[23] marking the first time such services are offered to end consumers in the United States.

Australia's Bendigo Bank is also offering OTP tokens to its customers and making the tokens mandatory by July, 2005.[24] These examples clearly show that organizations are starting to understand the importance and need for information security. If companies are willing to embrace the concept that information security is a business driver as well as technology, they may have an advantage over their competitors.

Conclusions

In a paradoxical time where the return on investment in information security spending is uncertain, trends suggest that information security will be increasing in importance. Significant opportunities exist for organizations to capitalize on using information security as a competitive advantage. Once embraced by executive management, a security-conscious organization can play a vital role to promote quality, efficiency, innovation, and even customer responsiveness.

Through the use of Defense-in-Depth, risk assessments, security awareness training, and good security policies, organizations can achieve gains in quality, efficiency, innovation, and respond to customer needs. Information security is as much a business need as it is a technical need.

---

[23] Roberts, Paul. "AOL Offers Added Security." PC World Magazine. 21 Sept. 2004. 3 Jan. 2005. <http://www.pcworld.com/news/article/0,aid,117873,00.asp>

[24] Crawford, Michael. "Bendigo Bank Adopts Tokens for Online Security." ComputerWorld Magazine. 28 Jul. 2004. 3 Jan. 2005. <http://www.computerworld.com.au/index.php/id;1580450875;relcomp;1>

Regulations such as HIPAA, GLBA, Sarbanes-Oxley, and the California Privacy Act were passed in response to meet the privacy and integrity needs of customers. Aside from sending a strong message to the business community about the importance of protecting information, the regulations have also accelerated the pace at which secure solutions are needed.

As this field is still in its infancy, organizations that can instill the need for information security within its corporate culture and deploy secure solutions will be able to differentiate themselves from competitors and create a competitive advantage.

List of References

Anon. Personal interview. 17 Dec. 2004.

Anon. Personal interview. 30 Dec. 2004.

Anti-Phishing Working Group. "Phishing Activity Trends Report: November 2004." 3 Jan. 2005. http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20November%202004.pdf

Bellis, Mary. "The History of Seat Belts." About.com. 3 Jan. 2005. http://inventors.about.com/library/inventors/bl_seat_belts.htm

Crawford, Michael. "Bendigo Bank Adopts Tokens for Online Security." ComputerWorld Magazine. 28 Jul. 2004. 3 Jan. 2005. http://www.computerworld.com.au/index.php/id;1580450875;relcomp;1

Evers, Joris. "Microsoft to Pitch Security as 'Competitive Advantage'." Network World Fusion. 07 Aug. 2004. 3 Jan. 2005. http://www.nwfusion.com/news/2004/0708microtopi.html

Global Information Security Survey 2004. Ernst & Young. 3 Jan. 2005. http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf

"Global Workforce Study: Press Release 11-8-04." (ISC)² Inc. 3 Jan. 2005. https://www.isc2.org/download/PressReleases/Release%20Global%20Workforce%20Study.pdf

Hill, Charles W. L., and Gareth R. Jones. Strategic Management: An Integrated Approach, 5th ed. New York: Houghton Mifflin Company, 2001.

Interbrand. "Cult Brands." BusinessWeek. 9-16 Aug. 2004. 3 Jan. 2005. http://www.ourfishbowl.com/images/surveys/BGBleaguetable_final_.pdf

NASSCOM-ITAA. "Information Security offers a considerable competitive advantage: NASSCOM- ITAA Poll." 3 Jan. 2005. http://www.nasscom.org/download/Opinion_Poll_Infosec_Summit.pdf

"Online Retail: Press Release 01-20-04." Jupitermedia Corporation. 3 Jan. 2005. http://www.jupitermedia.com/corporate/releases/04.01.20-newjupresearch.html

Porter, Michael E., Competitive Advantage: Creating and Sustaining Superior Performance, New York: The Free Press, 1985.

QuickMBA.com. "Competitive Advantage." 3 Jan. 2005. http://www.quickmba.com/strategy/competitive-advantage/

Roberts, Paul. "AOL Offers Added Security." PC World Magazine. 21 Sept. 2004. 3 Jan. 2005. http://www.pcworld.com/news/article/0,aid,117873,00.asp

SANS Institute. Track 1 – SANS Security Essentials. Volume 1.2. SANS Press, Sept. 2004.

United States. United States Census Bureau. Department of Commerce. Quarterly Retail E-Commerce Sales 3rd Quarter 2004. 3 Jan. 2005. http://www.census.gov/mrts/www/current.html

Wikipedia. "Car Safety." 3 Jan. 2005. http://en.wikipedia.org/wiki/Car_safety