日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

"The IT Revolution and Security Challenges"

Tokyo

December 10-11, 2002

"Information Security: Now and Beyond"

by
Hong Sun Kim
Chief Executive Officer, president, Securesoft Inc., Korea

Information Security: Now and Beyond

Hong Sun Kim

1. Introduction

The Good News of the Internet

Digital economy, *knowledge-based society*, and *e-business* are key expressions used to describe the phenomenon of the explosive growth and advancement in information technology witnessed in the current era. Technological progress in and wide adoption of information technology have spurred the introduction of a number of new, revolutionary business models. Furthermore, information technology is transforming traditional ways of conducting business by making them more information-centric, customer-oriented and global.

Of all the innovations in technology witnessed over the last decade, the *Internet* is clearly the technology that is leading the revolution in information technology. The message the Internet delivers is clear and simple: *freedom from the technological complexities and limitations in managing and communicating information*. All of us benefit from this simplicity provided by the Internet daily in our work and personal lives. Searching for and retrieving information on the Internet is as simple as typing a URL address into a Web browser. When sending an e-mail, it is sufficient to simply know the other party's e-mail address. It is not necessary to have prior knowledge of the computer system, (e.g., type of computer, operating system, or access procedures), where the information resides or is to be delivered. The Internet allows us to navigate websites and share information all over the world in a very simple, efficient and free manner.

Thanks to the simplicity in the communication and transmission of information afforded by the Internet, we can focus our time and energy, instead, on creating value through the collection, processing, management and distribution of that information. Furthermore, the Internet allows greater collaboration among various parties through the elimination of the limitations created by physical distance. For instance, enterprises can now use the Internet to outsource non-core operations and activities to any number of firms in the

world while employees on the road can remain connected to the corporate network from virtually anywhere on the planet. Such benefits in reduced costs and enhanced productivity will continue to fuel the increasing dependence of companies and individuals on the Internet.

The Good Comes With the Bad…Threats Within the Internet

Despite all of this good news, the Internet is still characterized by inherent hazards and threats. The openly accessible nature of this public network provides convenience to users, but also exposes them to various threats ranging from relatively harmless nuisances such as spam e-mails to serious crimes such as hacking, information theft, and viruses. The damages resulting from these incidents can be so devastating that some companies have been tempted to shut down their IT systems altogether. As businesses and individuals become increasingly dependent on the Internet, the potential damages that can result from these events become greater and greater. While we enjoy the benefits of the Internet, we are also placing our business operations and individual privacy at risk.

Importance of Trust in Online Business

In business transactions, integrity and confidentiality are key ingredients in building mutual trust. Similarly, in order to conduct business through the Internet, companies must have the assurance that any information transmitted over the Internet will not be tampered with or stolen, as this will have a devastating effect on the credibility of the business transaction, and ultimately the business relationship itself. Therefore, it is critical for businesses to be equipped with mechanisms to ensure the integrity of digital information and communication to preserve trust within the company and with its customers and business partners. As a result, the advent of the Internet paradigm was followed by significant interest and concern in *information security*. Information security should be regarded as a critical component in the IT infrastructure for establishing *trust* among organizations and individuals. It makes exchanging information over the Internet safe and secure and provide individuals the peace of mind to conduct business online. The Internet is the technology that *enables* online business, but information security provides the trust and assurance that truly make online business possible.

This paper defines the scope of information security and addresses the latest trends within the industry. As we rely more and more on the Internet and the information security technology becomes increasingly sophisticated, it becomes important to understand how security technologies are evolving and how these changes affect the

safety of our data, systems and organizations. One dominant trend in the Internet security industry is the migration from single technology, stand-alone products to more application-specific, integrated solutions. In section 3, we'll discuss how new IT trends and business behaviors are affecting the security industry.

Developments in Internet security are also highly dependant on trends in e-business and e-commerce. It is worthwhile to examine the Korean IT environment, which has experienced tremendous growth, fueled by heavy investments in IT infrastructure and the willingness of the Korean people to embrace the Internet. In Korea, the Internet has now become an integral part of business activity as well as personal life. Korea is an unparalleled laboratory for developing, testing and applying new security technologies in multiple applications and environments. The story behind the development of Korea's IT-rich environment and the competitiveness of security technologies from the region are discussed in sections 4 and 5. The applicability of Korea's experience in information security to the global marketplace and the feasibility of implementing its security technologies worldwide will be analyzed and discussed. Finally, the importance of privacy and cultural issues will be addressed.

2. Information Security Overview: Technologies, Products and Services

Security Risks

Figure 1 illustrates a typical IT network and describes the various security risks common to such environments. These security violations may target a particular service, system, or application. Although an organization's security systems and policies may be optimal at the time of implementation, vulnerabilities can arise due to the constantly changing system environment. A simple software upgrade, addition of new hardware or network reconfiguration can create new vulnerabilities and expose the organization to a host of security threats. The changing work environment also gives rise to new security vulnerabilities. Today, many more employees work out of home, accessing the company's network through broadband connections such as cable or ADSL. Unlike dial-up, broadband connections are "always-on" and always connected, leaving the system particularly vulnerable to an external attacker.

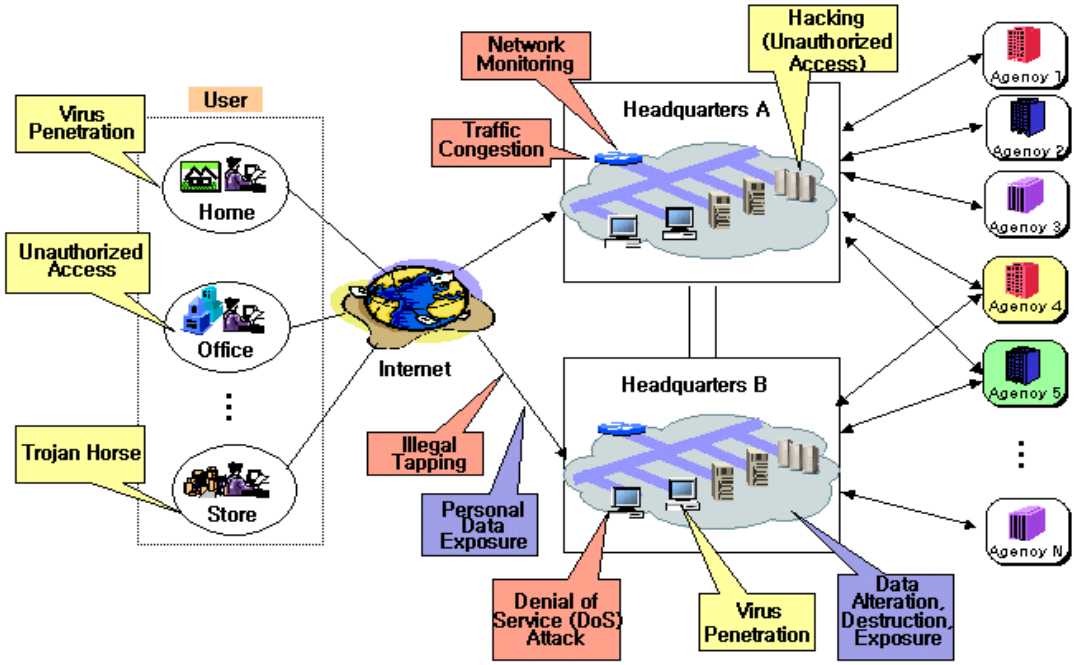


Figure 1. Typical Security Risk

Threats can be categorized as *internal* or *external*, according to the attacker's location, and *authorized* or *unauthorized*, according to the attacker's access privileges. Figure 2 illustrates how one can identify security risks and establish proper countermeasures for those risks. The diagram clearly shows that there are no simple, fix-all solutions to the various risks to information systems posed by the Internet.

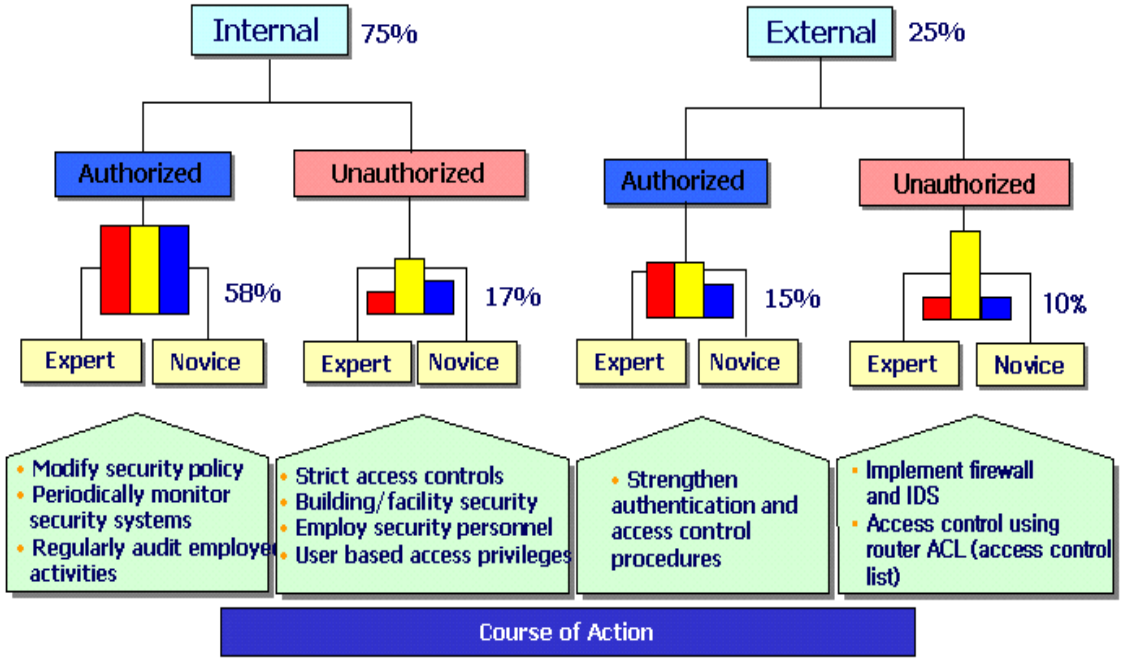


Figure 2. Threats to Information Systems – Types

Security Life Cycle

There is a popular quote that states, *"Life is not a destination, but a journey."* Similarly, the implementation of information security within an organization is not a one-time task, but a continual process. Figure 3 illustrates the conceptual model of the ongoing cycle of information security management. Most security product vendors tend to focus on the implementation phase of the information security life cycle when security products are selected and implemented. Indeed, the product implementation stage is where large investments are made and much of the visible changes occur. The deployment of basic security products such as firewall and anti-virus software are an important starting point in establishing a comprehensive information security system. However, the effectiveness and performance of the products are dependent on the proper maintenance and administration by staff as well as the awareness of the importance of information security at all levels of the organization. Furthermore, since the network environment constantly changes and security risks become increasingly complex and unpredictable, it is wise to follow each step of the cycle on a continual basis.

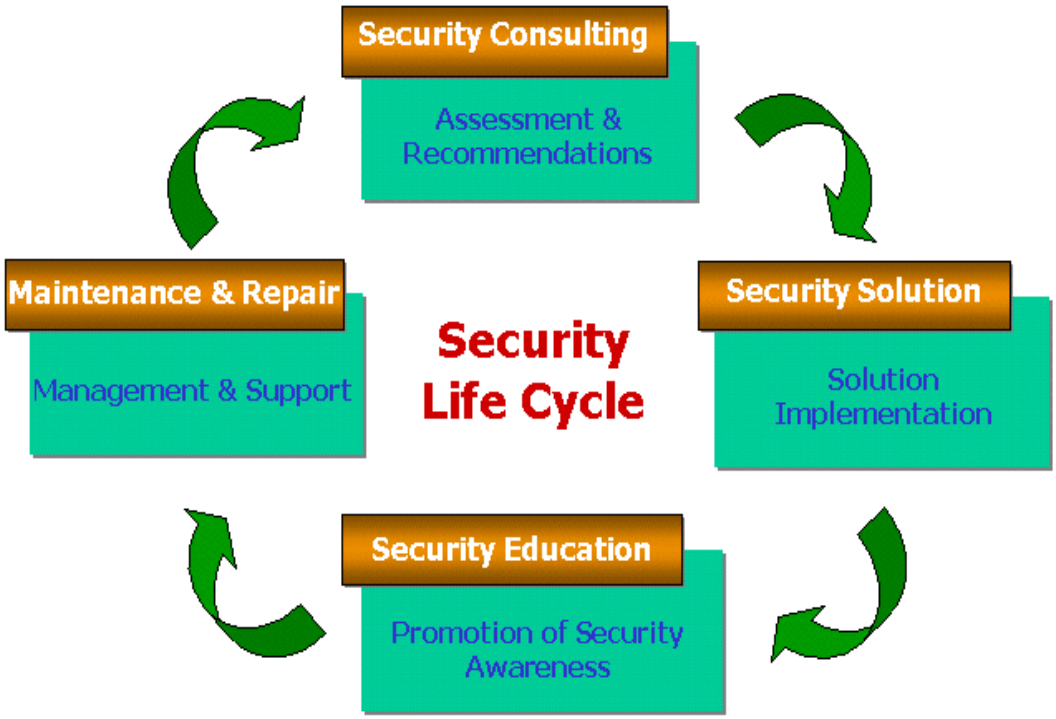


Figure 3. Effective Information Security System

Security Consulting

Information security consulting not only addresses IT systems and equipment, but also analyzes other factors that may affect information security such as operational procedures and access control of equipment and facilities, in producing a comprehensive security solution that maximizes the organization's level of information security. For example, statistics show that more security breaches are caused from within the organization, by employees or others with authorized access, than by external hackers. In addition, a large number of information security breaches are a result of problems in operational procedures and weak access control of the organization's equipment and facilities. Appropriate identification and authorization mechanisms should be implemented in the organization's operations and systems. The goal of information security consulting is to produce a comprehensive security policy that addresses information security through a combination of security technologies, security management, and physical security mechanisms (Figure 4). Inadequate or inappropriate policies in any one of these three areas of security can compromise the security of the organization and its informational assets and expose it to potentially serious threats.

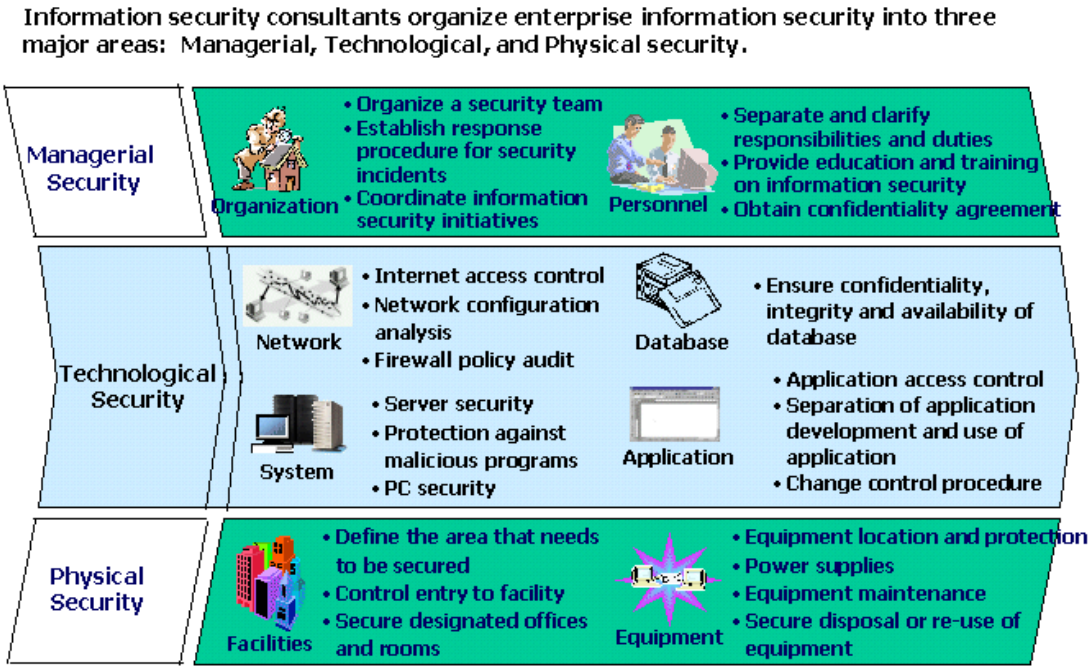


Figure 4. Scope of Security Consulting

Figure 5 illustrates the typical flow of a security consulting project. During the first two phases, the organization's business processes and assets are analyzed and vulnerability assessment is conducted. Based on the results of the vulnerability assessment, a customized security system is designed. The security master plan outlines long-term strategies for security product implementation, employee training and system maintenance. The security policy should be reviewed and practiced by all members of the organization.

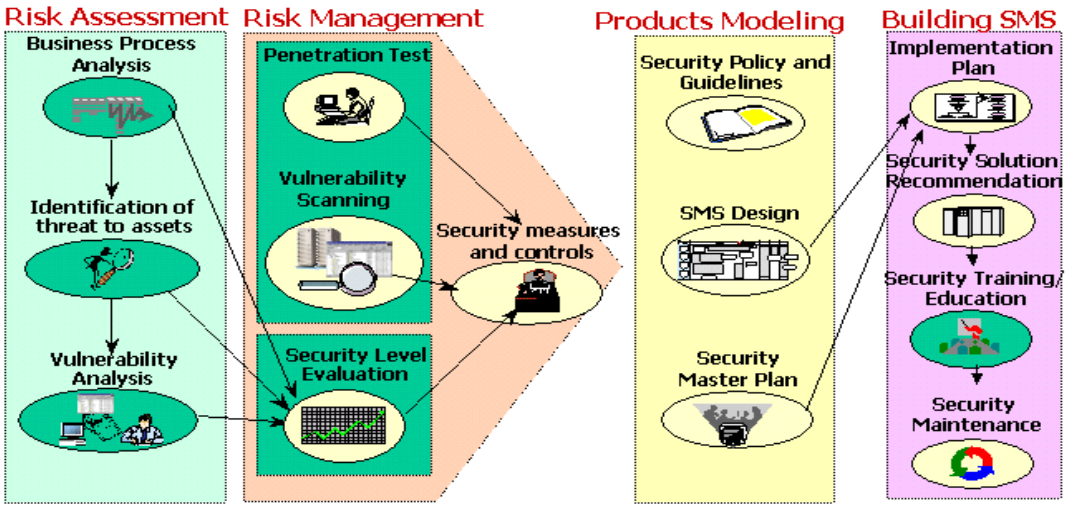


Figure 5. Project Stages of Security Consulting

Security Services

An organization's information security system should feature the following security mechanisms:

- *Authentication*: Verifies the claimed identity of a user. IDs/passwords are the most commonly used mechanisms, but smart cards, one-time passwords, biometrics, or a combination of these methods can be used for stronger, multi-factored authentication.
- *Access control*: Allows access only to individuals with proper authorization and access privileges. Packet filtering or authorization schemes are commonly employed to control access to systems and data. Access control policies are defined in the organization's information security policy.
- *Confidentiality*: Ensures that data is not disclosed to unauthorized parties. Encryption/decryption technologies are used to ensure that information is comprehensible only to the intended recipient.
- *Integrity*: Protects against unauthorized modifications or alterations to data. Data tampering can be prevented with the application of appropriate algorithms or digital signature mechanisms.
- *Non-repudiation*: Prevents both sides of an electronic communication or transaction from falsely denying that they participated in the communication or that the transaction was processed.
- *Availability*: Guarantees that information or data is available to authorized users. A good example of a security threat that can compromise availability is a DOS (Denial-Of-Service) attack, in which the attacker attempts to overload the server causing it to shut down and making server resources unavailable.

Different security products are capable of handling various security risks through a combination of the security mechanisms listed above. For example, *firewalls* allow authentication, authorization as well as data confidentiality and integrity; *digital signatures* ensure integrity and non-repudiation; and *digital certificates* and *IDs/passwords* are used in authentication. An organization must implement an appropriate combination of security products based on the organization's activities and information security requirements.

Security Products

Figure 6 illustrates the classification of security products into two broad categories according to their role in the organization. The left side of the figure lists security tools

used to protect an organization's network and systems against internal/external attacks. For instance, a firewall prevents attacks from the external network and controls system access from internal and external clients, and ESM (Enterprise Security Management) provides integrated, centralized management of multiple security products.

The right side of the figure lists security tools that address application security. Comprehensive application security is achieved through a complex encryption-based technology called PKI (Public Key Infrastructure), but even partial implementation of encryption technologies may be useful in protecting against security threats inherent in various applications.

At the top of the security pyramid is security consulting, the process by which the organization and its security needs are evaluated and an optimal solution is designed using a combination of security tools and procedures customized to the needs of the organization. Recently, a new breed of information security services, (around-the-clock, outsourced information security monitoring services), have come into the market. This service is geared towards small and medium sized organizations, which often lack the resources to to implement comprehensive security systems and procedures internally.

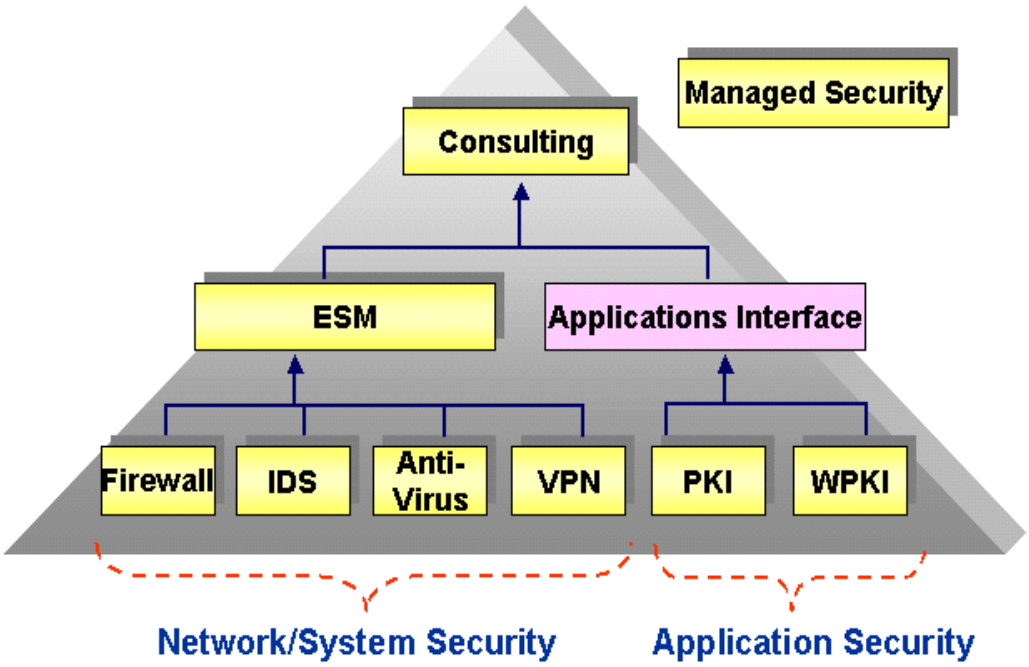


Figure 6. Technologies, Products & Platforms

3. Trends in Information Security

As the advancements in information technology create a paradigm shift in the way business is conducted, the requirements of information security are also changing hand in hand. The following are the current trends affecting the changing requirements of information security:

- **Organizations are becoming increasingly virtual and global.**

The Internet allows companies today to transact business with virtually an unlimited number of organizations and individuals worldwide rather than being limited to the domestic market. As a result, enterprise today are becoming more operationally and geographically decentralized. This trend is not limited to large corporations. Even small companies with less than 100 employees are globalizing their operations with the help of the Internet.

The Internet provides the benefits of rapid and efficient communication between customers and business partners worldwide which translates into tremendous revenue and cost-savings opportunities. However, these benefits come with a host of complex problems from an information security perspective. When an organization and its systems are centralized, a tall wall is sufficient to protect it against outside attacks. However, when the organization is dispersed across multiple geographic locations and business transactions are conducted over the Internet, all communications and exchanges of information become vulnerable to theft and tampering. Therefore, it is necessary to design and implement a comprehensive security policy to ensure the reliability and security of business activity on the Internet. An organization should pay particular attention to *authorization* and *access control*, the two most fundamental elements of information security. This requires a thorough examination of the enterprise and its operations, and the implementation of encryption and digital-signature mechanisms in the company's network environment. Security consultants are instrumental in performing the necessary analysis of the organization, including identification of vulnerabilities and potential threats, designing the optimal security policy and systems, and in implementing the various phases of the security life cycle

- **Networks are becoming faster and more sophisticated but organizations are demanding easier management**

The demand for increasingly faster network performance is never satisfied. As networks

become faster and more advanced, increasingly sophisticated services that take advantage of the increased network and computing power, such as streaming multimedia, are being offered. This cyclical pattern of advancements in computing technologies fueling the proliferation of sophisticated services and the increasing sophistication of services, in turn, fueling the advancement of computing technology will continue in the foreseeable future until a balance is eventually reached. It is not necessary to study Moore's law to recognize that computing hardware performance is getting better while prices are continuing to fall. Higher performance combined with greater affordability is fueling the rapid increase in the adoption of the Internet. This drastic rise in Internet traffic at home and work has caused network security product vendors to shift their focus from software functionality to performance and reliability in high-traffic environments. The significant majority of U.S. Fortune 500 companies, and a growing number of small and medium enterprises, have implemented firewall appliances in their corporate networks to increase the security of their networks and provide a greater level of trust and reliability in their online business activities. The development of such hardware security products is progressing in two directions: high-end products for multi-gigabit environments and low-end products for small organizations.

In addition to higher performance, the demand for greater simplicity has spurred the latest trend in information security products: the integration of separate security components into a single product. Integrated security appliances featuring firewall, VPN and anti-virus components on a single device are now widely available in the market. The August 2002 issue of *Information Security* magazine featured interviews with leading IDS (Intrusion Detection System) experts. Most agreed that firewall and IDS features will continue to be further integrated in the future. This integration is driven by the desire to achieve better performance and simpler, efficient management of security systems. Due to the increasing complexities of the network environment and information security technologies, and the ever growing number of security products on the market, organizations are stressing the importance of convenient implementation and ease of management in selecting security products. Many organizations accomplish this through ESM, middleware designed to manage the multiple security devices as well as other equipment on the network.

- **Security becomes application-specific and business-oriented**

Many security technologies have already become commodities. As discussed above, security products are being transformed into high-performance, multifunctional

products that are integrated with multiple security components. Another trend within information security is the embedding of core security technologies into other components or software applications. On the application security side, we are witnessing a strong trend toward vertical integration of security technologies and services. For instance, PKI vendors are now expanding their scope to include EAM (Enterprise Access Management) and application development services, (for applications requiring sophisticated security features). These trends indicate that security technologies are gradually evolving from stand-alone products to integrated parts of applications and other system components.

Security implementation requirements are also determined by an organization's particular business activities and security requirements. Enterprises with complex business operations and diverse e-business applications are unable to establish an effective security system through the simple installation of security products on their networks. A great deal of effort in customization accompanied by a clear understanding of the organization's operations and security requirements is required. Customization is performed during the implementation phase of the security consulting project. Prior to customization, the organization's operations and security requirements are analyzed by the security consultants. As a result of the growing complexities in information security and security products, information security consulting and product integration firms are seeing an increase in demand for their services.

4. The Korean IT Environment

During the last five years, Korea has undergone tremendous societal, economic and technological changes. In November 1997, the Korean government accepted assistance from the IMF on the basis that it would accept the IMF's strict requirements for economic reform. This was a big turning point towards achieving greater globalization and reform of business practices. Prior to this era of reform, a handful of large business conglomerates dominated the Korean economy with bureaucratic and noncompetitive business practices. In the last several years, many of the conglomerates, due to diminished competitiveness and poor financial management, have either gone bankrupt or have been radically restructured.

A significant number of people lost their jobs and many young graduates of the nation's top universities had difficult times finding employment. In the midst of these events, the Internet became widely available while early stage, high-tech companies utilizing the Internet to provide never-before-seen, products and services were receiving much attention from the technological, financial and political communities. What followed was a tremendous migration of human resources and financial capital from the big conglomerates to small, start-up IT companies. The Korean government, led by MIC (Minstry of Information and Communication), played a pivotal role in the nationwide deployment of the world's most advanced IT infrastructure. From 1999-2001, tremendous public and private-sector investments in the IT infrastructure, made high-speed access to the Internet virtually ubiquitous. Along with the surge in Internet usage, a proliferation of small, entrepreneurial IT companies dominated Korea's economic scene. The wave of IT entrepreneurship in Korea resulted in products and technologies that have made significant contributions to the development of global information technology and has forever established the importance of IT to the Korean economy and society.

The following is a review of information technology in Korea:

4.1 Korea's IT Infrastructure

Korea features the fastest, most accessible and cheapest broadband Internet connections in the world. Two of the driving forces responsible for the creation of this environment were the rapid deployment of ADSL and cable for general households and the explosive growth of business establishments known as Internet cafés. Interestingly, despite the widespread use of ADSL and cable broadband Internet services, there is still a

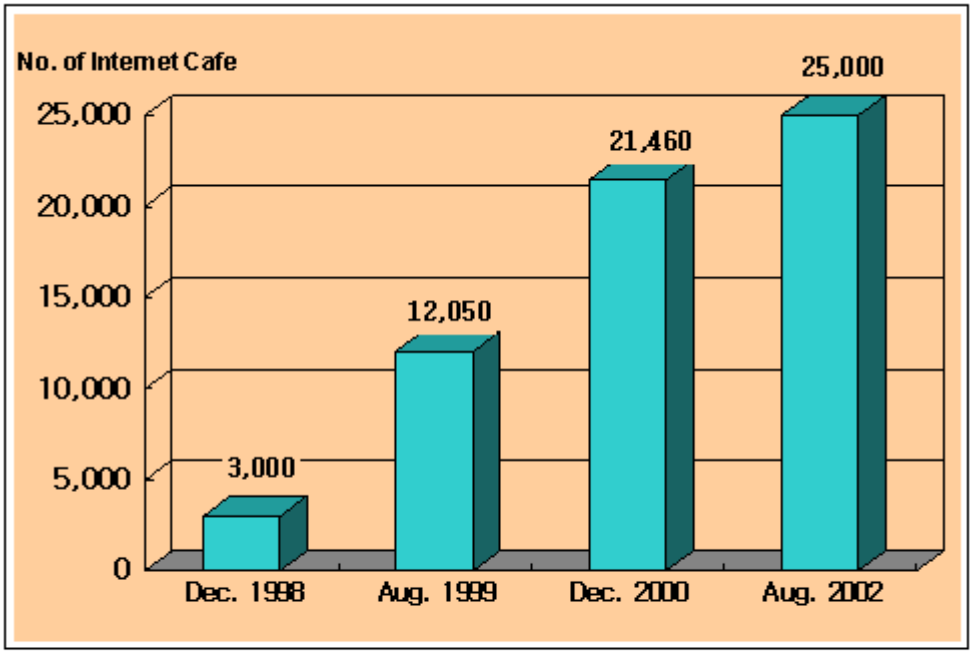
significant and growing demand for wireless and mobile Internet access.

Statistics on broadband services

According to KISDI (Korea Information Society Development Institute), as of the end of 2001, approximately 7.8 million households, equivalent to 53% of total households in Korea, had broadband access. That number has increased to more than 10 million households as of October 2002. By the end of 2007, that number is expected to reach 14 millions households, or 88% of all households in Korea. Since 2000, the average price of ADSL and cable Internet access have fallen to under US$30 dollars per month and continues to decrease. Also, VDSL service, with speeds of up to 13 Mbps, almost 10 times the speed of ADSL, was launched in July 2002. VDSL is expected to quickly replace a substantial portion of the ADSL market, as it is priced at a highly competitive rate of US$40 dollars per month for a full speed package. According to KRNIC (Korea Network Information Center), more than 25 million individuals, or 58% of the Korean population, use the Internet. These factors have raised the Korean consumer's expectations for higher Internet access speeds and more reliable services.

Game-Bang (Internet Café)

Another exclusive feature of Korea is the emergence of Internet cafés, also called *game bang* or *pc bang*, which means 'game room' or 'PC room' in Korean. The introduction of the game bang was motivated by the growing popularity of on-line, network computer games. Fast Internet access, a necessity in playing on-line, network games, was available for less than $1 per hour, and these establishments quickly attracted a large number of on-line game fanatics, in addition to ordinary computer users. This attributed to the huge growth in number of Internet cafés during 1999 – 2001 (Figure 7). Although online games were the driving force behind the initial success of Internet cafés, these *game bangs* have now become public places for Internet chatting, e-mailing, Internet banking, online stock trading, and other Internet services.

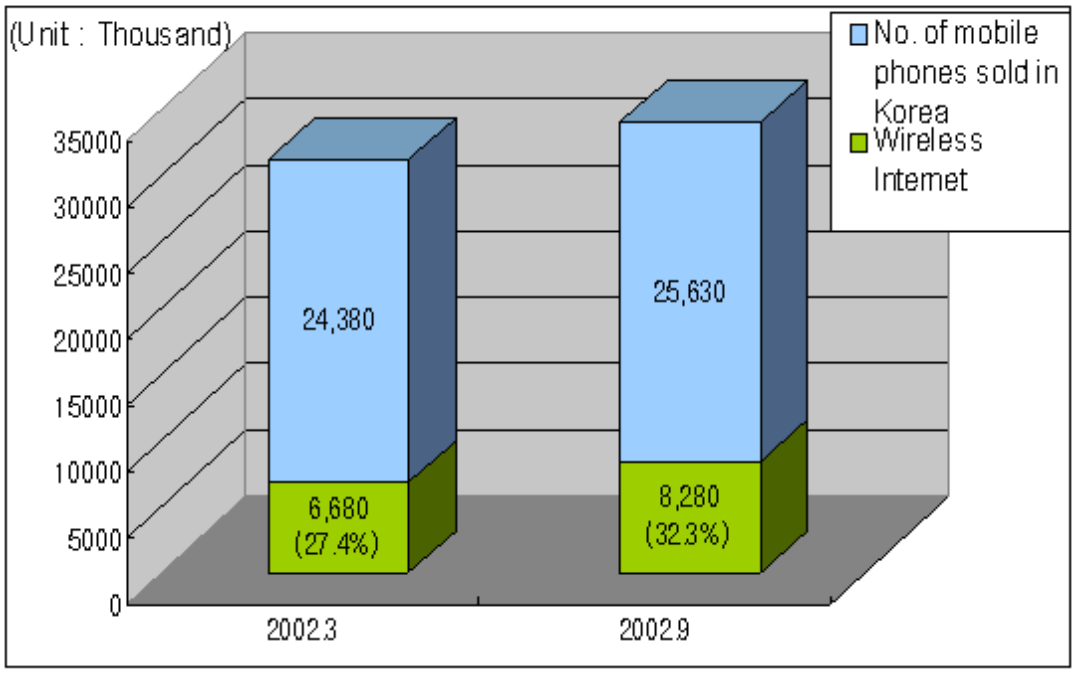


(Source : Internet PC Culture Association)

Figure 7. Number of Internet Cafe in Korea

Mobile Communications in Korea

The high penetration of mobile communication services is another important element of Korea's societal, economic and technological environments. Like Japan and Europe, Korea has experienced a substantial growth in the number of mobile communication users (Figure 8). With a population of approximately 45 million, the data in Figure 8 indicates that about two-thirds of the entire population own a cellular phone. There has also been a sharp increase in the number of mobile Internet users. Latest statistics show that younger users tend to spend more time on data communications than voice communications on their mobile phones. This trend is expected to continue as full-fledged mobile commerce and services are launched in Korea.



(Source : KRNIC(Korea Network Information Center), 2002.9)

Figure 8. Number of Wireless Internet Users in Korea

4.2 Korea's Internet Culture

As Internet access has become widely available, the number and variety of Internet-based services has also grown. Much of this was due to the willingness of Korean businesses to accept the new business paradigm presented by the Internet and information technology. The following are representative examples.

Financial services

Internet banking and online stock trading are extremely popular in Korea. While online trading comprised only 1.8% of total stock trades in 1998, by 2001, it had grown to an astounding 67.4%. Large firms such as Samsung Securities, LG Investment and Securities and Daishin Securities Co., Ltd. account for about 80% of the total online stock trades. Given that online financial applications are extremely attractive targets for attacks, the widespread use of online financial services must be accompanied by implementation of security infrastructure. According to KISA (Korea Information Security Agency), licensed certificate authorities have already issued certificates for more than 4 million users. Compared to Germany's 27,000 certificate users and 19 licensed certificate authorities, Korea's numbers indicate a strong and rapid growth in Internet based services. In 2003, digital certificates issued by licensed certificate authorities will be required by law to conduct online financial transactions in Korea.

Due to this new legislation, the number of digital certificates issued is expected to reach more than 10 million users in the near future.

Online shopping

Although home shopping has been popular in the United States for many years, home shopping was not widely adopted by Koreans until approximately several years ago. In Korea, most shops and stores are located in close proximity to residences and most of the population live in cities where shopping is not a significant inconvenience. Customers were also hesitant to purchase products without first seeing and touching them in person. Payment and delivery were also concerns that contributed to the slow adoption of home shopping. However, this has changed quite a bit during the last 2-3 years, and many large Internet shopping malls emerged as consumers' reluctance to purchasing products from non-brick-and-mortar retailers were overcome by the convenience and the distinct advantages of shopping online (Figure 9(a)). Daum Communications Corp., one of the leading portals in Korea, was struggling in 2000. However, a substantial growth in online sales revenue, as shown in Figure 9(b), has placed it in a strong market position. Today, every imaginable product is available for purchase online, and online retailers pose a significant threat to their off-line counterparts.

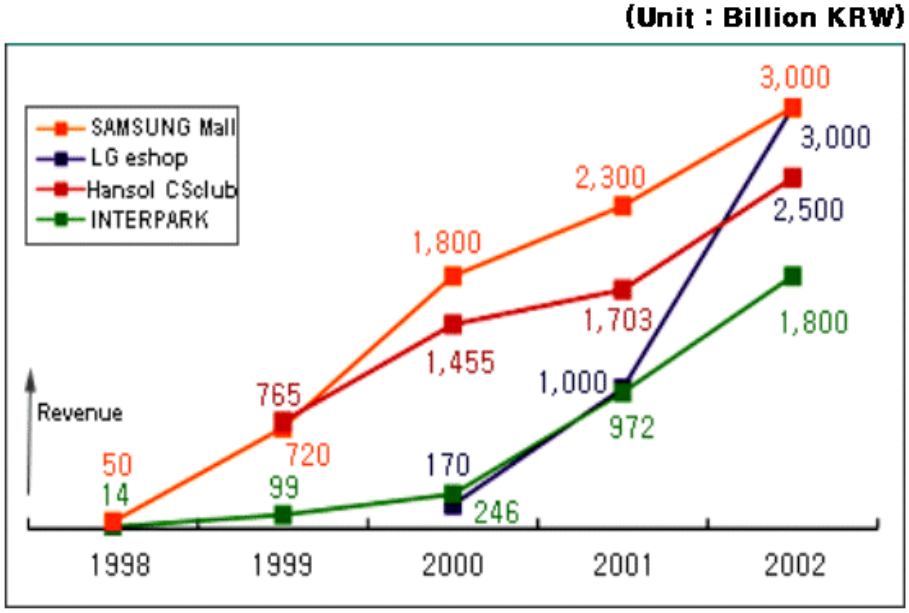


Figure 9.(a) Yearly Revenue of Major Internet Shopping Malls in Korea

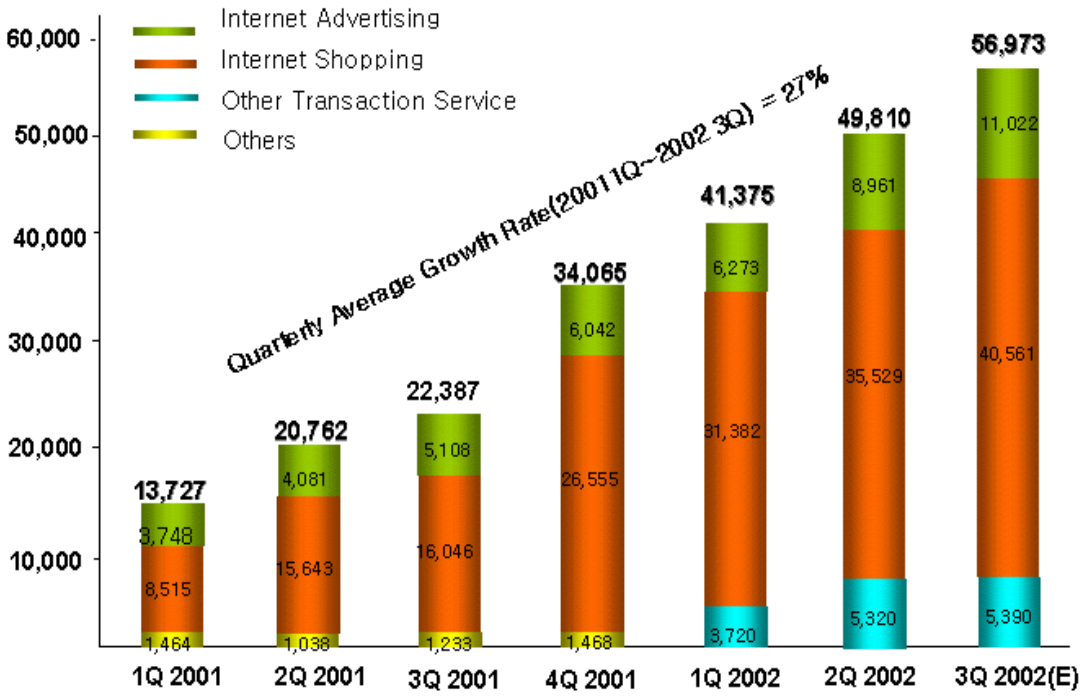


Figure 9.(b) Daum's Historical Revenue Performance

Online games

As explained earlier, *game bangs* are public Internet cafés that provides low cost, high speed Internet access for playing games and conducting other activities on the Internet. *Game bangs* have contributed significantly to the growth in number of on-line gamers from young children to people in their 30's and 40's. Most online game makers made profits ranging from $8M - $38M for the first three quarters of 2002. This equates to profit margins of 35% - 58%. However, as online games become more violent and gamers become more emotionally and psychologically involved with these games, many social problems are being attributed to online gaming. Virtual game pieces for online games are being traded online or offline, with some rare, powerful weapons, tools or characters going for thousands of dollars. The significant monetary value of these virtual game pieces and the tendency for some gamers to get emotionally involved in the games are becoming a source of various crimes, including malicious cyber attacks. It has therefore become crucial to safeguard online game sites against such threats and to promote a positive gaming culture.

4.3 Korea's Internet Security Industry

National security has always been a high priority in Korea. Security technology has always been associated with concerns regarding national security. Information security

is currently an important element in Korea's national security agenda. In 1997, MIC (Ministry of Information and Communication) publicly announced a master plan to promote the information security industry. MIC's agenda regarding information security is reflected in the new legislation entitled *The Critical Infrastructure Protection Act.*

The Critical Infrastructure Protection Act was passed in December of 2000. This law requires institutions deemed critical to the nation's information and communications infrastructure to conduct vulnerability assessments of their networks and systems. Government institutions, telecommunications facilities, and financial institutions fall under the requirements of this new law. In addition, the government grants licenses to qualified companies, following a thorough examination, to provide security consulting, vulnerability assessment and security service to the institutions listed above. This act has contributed to an increase in the number of public contracts for security consulting companies in Korea.

The security technologies developed in Korea were not purely "first-mover" technologies. Instead, information security products featured an amalgamation of existing security concepts and technologies tailored for the requirements of Korea's unique IT environment. Korean security firms have generally done well in the domestic market due to this understanding of the unique IT conditions and organizational requirements in Korea. It is not surprising, therefore, to see that many foreign companies, without this understanding and accustomed to a far different IT environment, have not performed well in the Korean market.

To date Korean security companies have generated most of their revenues from the domestic market. However, since a few years ago, several domestic companies have introduced more advanced, next-generation security products with global appeal and have made efforts to expand into foreign markets. While the history and presence of Korean security companies in the global arena are limited, they enjoy the advantage of proven technologies tested within one of the most advanced and demanding IT environments in the world. Korean security companies are therefore well poised to make a significant impact on the global information security market, and global IT at large.

5. Competitiveness of Information Security Technologies

We have all witnessed the impact the Internet is making on the lives of individuals and on business activity. Despite the bursting of the Internet and the broken promises of many dot-com companies in the last few years, the increasing penetration of IT in business and society will continue. Nor does the temporary reduction of IT budgets signify the suspension of the e-businesses and e-commerce paradigm.

Basically, information security delivers products and technologies to organizations or individuals pursuing e-businesses. Most products such as firewall, VPN, anti-virus, have already become necessary commodities in today's paradigm. However, security products are no longer viable as single technology products, and many vendors are now moving toward all-in-one products that integrate several key technologies. As addressed in the previous section, information security is moving away from being packaged products to become tools or methodologies that are customized applied to various applications and business models.

Korea is a unique and ideal environment in which security technologies can be developed and tested under rigorous, real-world conditions. The high rate of Internet penetration due to an unparalleled broadband infrastructure, and the tremendous level of Internet traffic due to the heavy reliance of the Internet for business and personal activities make Korea an ideal laboratory for developing and testing IT technologies and products. Many foreign IT firms are coming to Korea to test their products and develop reference sites. The following is a case study of the recent application of a Korean security technology in a new business application.

SK Telecom, the leading wireless carrier in Korea, launched a full-featured mobile commerce service in December 2001. Mobile commerce services allow users to conduct various types of e-commerce transactions such as catalog shopping, Internet banking, and online gaming over cellular phones, PDA's, and other mobile devices. Mobile transactions are secured end-to-end using public-key algorithms, digital signatures, and 128-bit symmetric algorithms. SK Telecom's mobile commerce services, called the MONETA service, uses an integrated smart card that serves simultaneously as a credit card, traffic card, and digital cash. As shown in Figure 10, the system entails sliding a card into the slot of a phone, or using a smart card chipset that is embedded into a phone. In addition to a variety of features mentioned above, the MONETA service features an underlying end-to-end security mechanism that ensures

the security and reliability of the mobile transaction. The government of Korea is planning to approve and support licensed digital certificates to be used in mobile commerce services by the end of 2002.

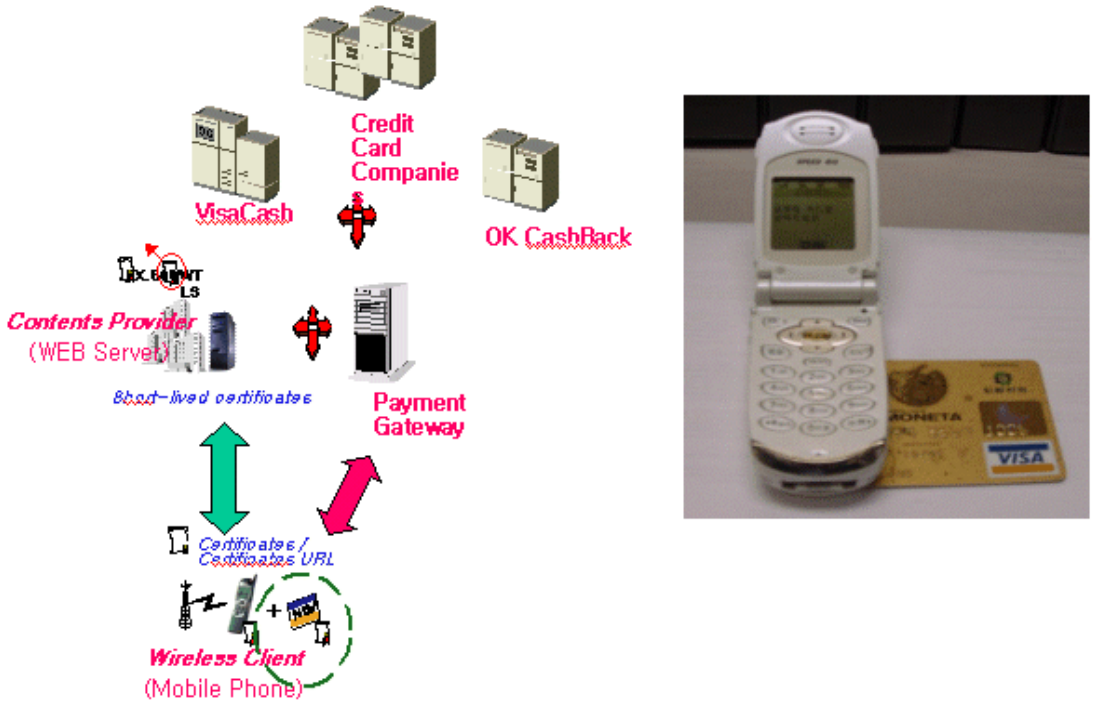


Figure 10. MONETA Service

This service demonstrates an example of an innovative information security technology developed within Korea to meet the demands of an advanced IT marketplace. Despite the many advancements in mobile communications, many consumers feel that the wireless environment has yet been disappointing due to the low processing power and limited memory of wireless devices, and the small communication bandwidth and lack of a uniform standard. Small storage space on mobile devices is a significant limitation in embedding critical security codes and encryption algorithms. Additional hardware chipsets cannot be embedded into wireless devices. Regardless of the limitations, mobile users are demanding reliability and speed in their mobile communications and commerce activities. The primary technology available today for securing the mobile transaction is *wireless PKI*, which requires interaction with other modules such as payment gateways, smart cards, and application interfaces. Moreover, it has to be seamlessly incorporated with other wireless services and business entities. There are two reasons why this security technology was first commercialized in Korea: (i) the domestic development of the core wireless PKI technology motivated by (ii) the readiness (in terms of infrastructure and consumer mentality) and demand of the marketplace for mobile commerce.

Competitiveness of Korean security technologies

The competitiveness of Korean information technology lies in the combination of the ability to develop core technologies and the strong e-business platforms and IT infrastructure available in Korea (Figure 11). Internet security is one of the core areas of this advanced IT infrastructure. Along with the benefits of an advanced IT infrastructure and high rate of IT adoption come the demands and risks of that infrastructure.

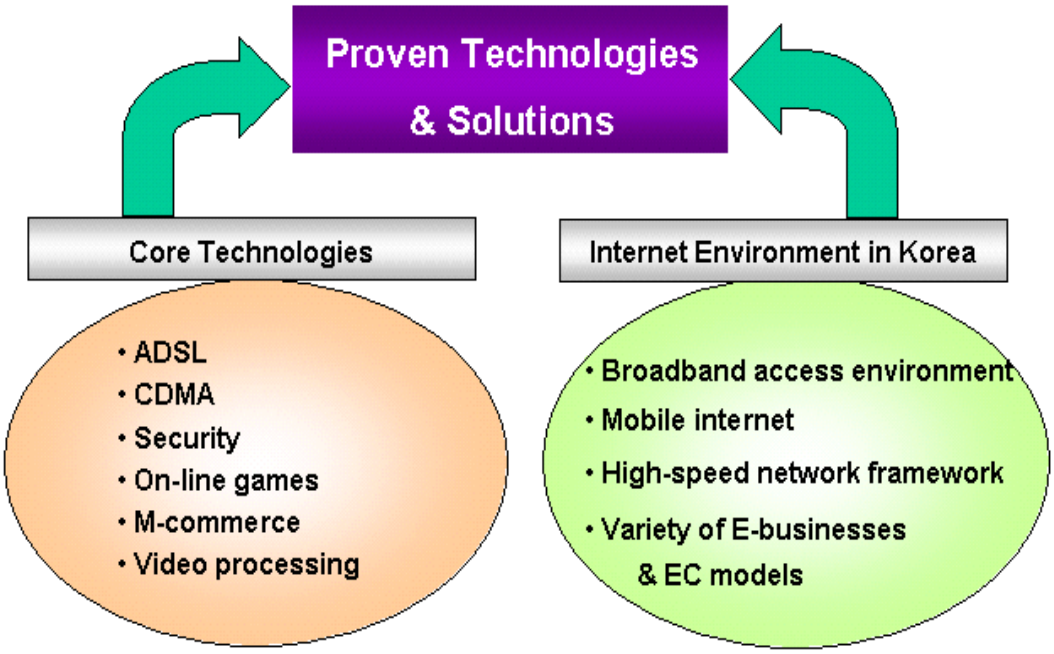


Figure 11. Competitiveness of Korean IT Technologies

New and changing business models are critical reasons for the improvement of security technologies. New business models and applications of information technology require us to analyze the risks posed by these applications and to create counter measures to maximize security. For example, *cyber apartments* or *intelligent buildings*, (residential or commercial facilities featuring appliances, and various equipment networked through a high-speed Internet connection), provide a tremendous array of new services and conveniences never before possible, but also expose the consumer to a slew of potential risks and disturbances from interruption of services or other damages caused by a security breach of the home or office network.

Information security technologies and products are at an inflection point. Once a stand-alone product deployed as a part of the corporate e-business infrastructure, information security technologies are now being integrated into specific applications and services. As with any technology, the value of new information technologies will

depend on their applicability in real-life applications. In this regard, Korean security vendors are in a strong position due to its great business platform. The challenge for Korean vendors in the future will be to bring their innovative, tested technologies to the global marketplace.

6. Cultural and Privacy Issues

Information security plays a critical role in the protection of personal privacy and the adoption of an IT-centric culture.

Privacy concern

As more information is shared and exchanged, the privacy concern becomes more critical. In particular, a person's life and reputation can be greatly affected if personal information such as one's medical record or financial information fall into the hands of criminals. If a person's residence or workplace is networked, such as in the case of cyber apartments, a number of potential privacy issues arise.

In a sense, there are trade-offs between privacy and protection when one implements a security system. An organization should address these conflicting issues. The method of addressing these issues differs depending on the geographical region. For example, Asian culture is quite different from the US culture when it comes to privacy matters. However, one clear proposition is that the protection of organization's valuable resources should not be compromised.

Public countermeasures

Security threats may come from many different sources. Once the security threats are detected, such information should be communicated to appropriate authorities immediately and appropriate actions should be taken. These days, a security device such as an alarm system is important not only to private entities but also to the government. The Government should play an active role in legalizing security issues available in the market place. Also, the government should manage and maintain the security of its people and the nation.

Culture

Internet security cannot be maintained without cooperation between individual consumers and organizations, computer and security equipment vendors, service providers, and regulatory agencies. Product vendors and service providers are primarily concerned about products and services they deliver. However, if a user ignores a certain guideline, security solution will become ineffective. We need to create a new culture where broad knowledge and responsibility are stressed.

A well-managed security solution involves participation of all these parties. First of all, the top management should be committed to building a secure organization. Once the

security policy is established and effective solutions are adopted, all employees must follow such rules and guidelines. A mistake from a minor task may cause a cascading effect on the organization. Everybody within an organization should be committed to security and the management must create such culture within the organization. Continuous training and education ensure enhancement of security within the organization.

Information security is a critical component of e-business and e-commerce. As more business models are developed and IT infrastructures continue to improve, security technologies will evolve as well. It is safe to view information security as a new culture in the IT industry. Users should be patient and ready to accept this culture. Product suppliers or service providers are required to continue looking into new threats and develop corresponding technologies to safeguard corporate or individual assets. They have to be adaptable to new business models and IT environments. Government and public institutions have to establish legal policies and preventative mechanisms. Moreover, global cooperation is needed.

As our global society becomes increasingly e-centric, and we continue to rely on the Internet in our business and personal lives, information security will continue to be an important issue. Regardless of what technology can enable us to do, *trust* and *security* are fundamental requirements for a technology to be truly useful. Information security is not just an issue of protecting one's information assets, but of establishing a safe and reliable informational society. In order to build a safe society and realize all of the potential benefits the Internet and information technology can provide, a global consensus that information security is the foundation of a e-society must be reached.