

**PART ONE**

**INTRODUCTION**

CHAPTER 1. IT SECURITY IN THE DIGITAL AGE

## CHAPTER 1. IT SECURITY IN THE DIGITAL AGE

### Introduction

One of the most striking technological developments of the last fifty years has been the emergence of digital technology as a powerful force in our lives.<sup>5</sup> For many of us, this technology is embodied in the digital computer, which has evolved to be an essential tool for our work as well as our personal needs. In 1951, when the first commercial electronic digital computer, a UNIVAC I, was delivered to the U.S. Bureau of the Census, computers were essentially unknown to most people, and were found only in a few research laboratories and universities. They were large, expensive, and prone to frequent failure. In contrast, today's computers are relatively small, inexpensive, reliable, and are found in every country.

Shortly after computers became commonplace at universities, research projects were initiated to link them together so that information could be passed between them. One such early project, the development of the ARPANET, was highly successful and led to what we know today as the Internet. From an initial network of four computers in 1969, the Internet has evolved to the point today where it links over 300,000,000 computers worldwide.

The emergence of the World Wide Web, developed by Tim Berners-Lee and Robert Cailliau at the Center for European Nuclear Research (CERN) in Geneva in the early 1990s, is a powerful service that use the Internet to create a global information system and increased substantially the Internet's utility and attractiveness. Although many people equate the Internet and the World Wide Web, the Web is actually only one service out of many, albeit a major one, that makes the Internet such a powerful tool for information and communication.

Within the past ten years, the Internet has become an important tool for communication in all sectors of society. We depend on it for timely access to information, for private correspondence, and for

commercial business applications of all kinds, including financial transactions. The availability and reliability of the Internet is essential to the continued prosperity of developed countries, and it is quickly becoming important for developing countries as well.

The effects of the computer and the Internet revolution go far beyond their direct uses and these effects are profound.

First, the Internet is capable of radically diminishing the geographic isolation of those connected to it. The Internet is facilitating globalization by providing a communications medium where everyone linked to it, regardless of his or her location, is effectively the same distance away. Search engines underscore this change; search results are based upon content, not distance, so that web sites of firms in developing countries have an equal opportunity to be seen in developed countries.

Second, the Internet is a strong influence towards disintermediation, i.e. the elimination of intermediaries (middlemen) in business and administrative functions. One example is the drastic reduction in the number of secretaries employed in developed countries. The word processor and electronic mail have made it easier for people to compose, print, and send their own messages than to tell a secretary what to type. Similarly, the travel agent industry is currently shrinking, due to the public's new ability to book air and rail tickets and hotel rooms on-line. This is a development that saves the customer time, money, and, with the additional control over one's preferences, may increase the chances of having a pleasant trip. The emergence of companies selling books, music, and electronics on-line has impacted the share of business going to classical off-line retail shops, but at the same time may have increased the size of the overall market in some sectors. While these off-line professions and industries will continue to exist, they are likely to employ fewer people and may their market share erode, and could move to specializing in niche markets rather than providing general services. The effects of disintermediation that have been initiated by technology are likely to continue for a long time and will displace more professions and industries as information technology evolves.

---

<sup>5</sup> See, Digital Tornado: The Internet and Telecommunications Policy FCC Staff Working Paper on Internet Policy (1997), available at: [http://www.fcc.gov/Bureaus/Miscellaneous/News\\_Releases/1997/nrmc7020.html](http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html)

Third, the rate at which we work (our productivity) appears to have accelerated, at least in industries driven by or dependent on information technology. Thanks to electronic mail, it is possible to share information around the globe in seconds, so that worldwide discussions and negotiations can proceed in a very rapid manner. Business once conducted by postal mail, telex, and telephone, is now conveyed through a faster and more effective means of communication, providing reduced cycle times for transactions.

Finally, it is essential to maintain secure information storage and communication links in this new environment. The high-tech industry is actively exploring ways of ensuring the security of its infrastructure; the participants understand that security breaches stemming from insecure hardware and software along the Internet will inhibit some of the major promises of this new medium from being realized. The establishment of trust in sound and safe computers, networks, and stored data in this new environment is as important, if not more important, as it was in an environment based upon face to face interaction.

The lesson for developing countries is clear; organizations that do not have the required level of security in their digital infrastructure and thus do not protect their content and information transmissions satisfactorily will not be trusted and might be left behind in the new global economy.<sup>6</sup>

## The Digital Revolution

Digital technology these days includes much more than just computers. Technological progress in microelectronics has made the micro-miniaturization of complex electronic devices possible, so that you may now carry the equivalent of a roomful of computing and communications equipment in your pocket. Moreover, the improvement in the price-performance ratio for this technology is about 30% per year and likely to stay at that level for another ten years.<sup>7</sup> We expect this technology to

flourish and drive the quest for new areas for commercial exploitation, creating a golden age for digital appliances.

Modern telephone equipment is completely digital in nature; mechanical relay switching devices have been replaced with special purpose computer systems. Since the development of the CD in the early 1980s, music and other sound recordings have been making a transition to digital form. With the introduction of the MP3 music format in the late 1990s, music and sounds have been recorded digitally, even in home environments. Even data dense images are now digitized and cameras that record digital images are rapidly replacing images recorded on photographic film for many applications. Even movies and animation are going digital, as the costs of the relevant production and dissemination technologies are declining. The DVD is starting to replace videotape, movies are made and edited with digital enhancements, and the movie industry is beginning to distribute titles digitally, instead of on reels of celluloid film. Electronic projectors are now in use in some theatres.

Cell phone standards, both *de facto* and *de jure*, are moving to digital, with protocols such as GSM, CDMA, TDMA and their variants and spin-offs displacing the earlier generation of standards based upon analog technology. In developed countries, digital television has been introduced and may eventually displace existing broadcast standards, although this change is likely to come more slowly because of the large base of installed home receivers that depend on the older standards.

Physical security systems are also becoming digital in nature. In hotels, apartment buildings, and offices, physical keys are being replaced by digital access cards. Television cameras used for monitoring security are often deployed on digital platforms, sending digitized images to monitoring stations on a network instead of sending a television signal to a standard video monitor.<sup>8</sup>

<sup>6</sup> Braga, Carlos Prima, Inclusion or Exclusion, UNESCO Courier, available at: [http://www.fcc.gov/Bureaus/Miscellaneous/News\\_Releases/1997/nrmc7020.html](http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7020.html)

<sup>7</sup> This rate of technological advance is a corollary of 'Moore's law,' described by Gordon Moore, the father of Intel, in the 1960's. He observed that every two years (later shortened to 18 months), the technology allowed manufacturers to produce chips with double the capacity for about the same price. This trend has been observed for the past 40 years, and the industry expectation is that it will continue for another 10 years.

<sup>8</sup> Interestingly enough, this particular transformation may well export jobs to developing countries. Once the images are in digitized form and transmitted on the Internet, they can be sent to a monitoring system anywhere on the net. It has been suggested that this security function, which does not require specialized skills, could be set up in developing countries at lower costs, and with equal quality of service. The suggestion is welcome in a development context, but could have physical security implications in that the outsourcing depends upon crossing national boundaries.

Many of the services that we use today would not be possible without computers and networks and the digital technology on which they are based. Airlines would not be competitive without computer based reservation systems and flight and maintenance support systems. Planes themselves depend massively on electronic sensors and digital controls and would be unable to function without them. Even automobiles use microprocessors to function and to assist in their maintenance today. Global Positioning Systems (GPS) permit you to know where you are anywhere on the earth. With this relatively inexpensive device and a computer containing a base of maps, you are able to track where you are going, find important landmarks, restaurants, entertainment, or services along the way, and ultimately to reach your destination.

These digital devices are being networked at a rapid rate. Cell phones 'talk' to the Internet, transmitting initially voice and now pictures. Soon they will have GPS capability, so that people in trouble can be located with great precision when they make an emergency call. Many of the services we use, such as ATM machines for disbursement of money, rely on network access. Inter-bank and international financial transfers have long depended upon financial networks;<sup>9</sup> nowadays, electronic personal banking transactions are accessible to individuals via the Internet.

This explosion of digital electronics and interconnected devices presents many opportunities, but it also has a dark side. It is becoming easier for people to track where you are, to catalogue what web pages you visit, to study what you purchase at stores, and to observe what you read and watch online. If such monitoring is intended for your benefit, you probably won't object to it, but you will want to be sure that such data is collected with your permission and is used only

for the purposes that you understand and agree to. Most individuals value their privacy and many governments have chosen to uphold individual rights to privacy to a certain extent, though the level of protection varies from country to country. The challenge for governments is to assure that we can realize the benefits of emerging technologies and still maintain the values and freedoms that we enjoyed without them. This is a challenge that requires governments to understand the new technologies and evaluate how the devices and capabilities interact with our freedoms. Government must also take proactive steps to ensure that legislation and public policy reflect a lasting commitment to maintaining, if not strengthening, the freedoms that exist currently.

We often refer to the digital world as *cyberspace*.<sup>10</sup> Cyberspace includes all of the computers and other digital devices that are connected to both internal and external networks and can communicate with each other. We can talk about meeting in cyberspace and doing things in cyberspace, as opposed to physical space. For readers of this Handbook, in particular, it is useful to make a distinction between behavior in cyberspace as opposed to the "real world" in which we live, work, and play.

The rapid spread of the personal computer and the Internet to developing countries has brought many benefits to all sectors in those countries. However, the Internet by itself is not necessarily a medium secure from malicious behavior. The opportunity cost of not paying adequate attention to security can be the loss of valuable data needed to run an enterprise or a government agency. Among other things it can include destruction of essential records, identity theft, and theft of financial resources, outcomes that cannot only ruin a company, but that can contribute to a reputation of unreliability for an entire industry in a country.

<sup>9</sup> The interbank financial transfer network has in the past used a special, highly secure, special purpose network, not logically connected to the Internet. This is appropriate, given the high value added nature of the network and the very serious consequences of any compromise of the network.

<sup>10</sup> "Cyberspace" was originally coined by author William Gibson to mean a parallel universe created and sustained by the world's computers. The term cyberspace was actually invented by William Gibson and used in his 1984 novel, *Neuromancer*. "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..." This definition may be useful for literary purposes, but the meaning of the term has shifted substantially from Gibson's usage.

See Intven, *et al.*, Legal and Regulatory Aspects of e-Commerce and the Internet, The World Bank Legal Review, vol. 1 2003, at fn 17. (Kluwer).

As the Internet expands and issues regarding cyber attacks become more widespread, the number of such incidents is increasing:

“Although computers have up to this point been spared a major cyber attack from terrorists or rogue nations, there have been plenty of smaller acts of vandalism by individual troublemakers. The Computer Emergency Response Team (CERT) tracked 52,658 online security incidents in 2001, more than double the number reported in the previous year, and more than four times the number reported the year before that.”<sup>11</sup>

The issue of the security of computers and networks is especially important for developing countries. The Internet can essentially eliminate any disadvantage due to distance or remoteness of location and it can provide access to an enormous amount of content, no matter what the distance is between the person requesting the content and the content repository itself. Together with the World Wide Web, the Internet can place businesses in developing countries on a more equal footing with respect to information about companies, their capabilities, and their products. Furthermore, search engines do not make a distinction between web sites based on geography, so that suppliers of goods and services in developing countries can be seen on a par with suppliers of those goods and services based in developed countries.<sup>12</sup> This is sometimes referred to as the “death of distance,”<sup>13</sup> a phrase which graphically describes what the Internet has accomplished for information and information flows.

However, there are the real risks to business of loss of records, denial of service attacks, corruption of information, and other hostile attack effects. For a business to have all or part of its electronic records altered or erased can be devastating. For a country to have a reputation for weakness in IT security can taint its industries, regardless of the actual extent of damage that may have occurred. Lack of attention to security

can result in both real and perceived damages, and can result in business failures in countries which need the confidence of external business relationships in order to prosper. Achieving the Millennium Development Goals depends on developing countries being able to use information technologies effectively and to increase their wealth by becoming integral members of global commerce.<sup>14</sup> The ability to obtain and supply relevant information easily can help countries in all areas of civil society, whether it is education, health care, commercial development, expansion of international markets and trade, or strengthening of local cultures.

Unfortunately, all of the manifestations of human behavior possible, good and bad, have moved into cyberspace and can be observed there. Since it is easy to copy digital content and edit it, it is also easy to falsify information, including the modifying and forging official documents. Because the Internet evolved from a cooperative research environment, where the goal was to share information easily, the underlying structure makes it possible to break into computers and steal confidential information. The motivations of people who exhibit such behavior in cyberspace are similar to the motivations that drive them in the real world, with one significant exception. The environment created by computers and the Internet has brought out tendencies in certain people to prove that they can break into systems or cause other problems. Much of the mischief in cyberspace is caused by “crackers” who simply want to prove that they can defeat any security barriers that may be in their way. The equivalent behavior in the real world consists of someone who demonstrates that he can break into your house but after doing so, leaves. Not only does this generate a profound feeling of insecurity, but it also raises the question of whether anything was taken or changed, or whether the next attempted entry will be more malicious. Just as such behavior in the real world can't be tolerated, neither should it be tolerated in cyberspace. Techniques in this Handbook will help you to guard against such malicious behavior.

<sup>11</sup> Reuters/USA Today, April 16, 2003.

<sup>12</sup> Search engines do differentiate on the basis of language, so that as in the real world, you have to speak in the language of your target market. Search engines may also not have the patience to retrieve web pages at the tail end of slow connections. However, businesses can host their web sites anywhere in the world, so that information can be placed close temporally to target markets. Some businesses mirror their web sites, i.e. create copied in different geographic regions so that customer access time is minimized.

<sup>13</sup> ?, Cairncross, F., *The Death of Distance: How the Communications Revolution will Change our Lives*, Harvard Business School Press (1997).

<sup>14</sup> Information and Internet security are one of the three main topics on which the World Summit on the Information Society will focus at its conferences in Geneva in December 2003 and in Tunis in April 2005. This is additional evidence of the broad recognition that the role of ICT for development is achieving.

Nothing in this Handbook or in cyberspace should make you reluctant to learn about computers and the Internet and exploit them to the fullest. Today's Internet represents the beginning of a wonderful set of transformations of the world's stock of information and knowledge, including the ability to distribute it to the general public inexpensively; information can be efficiently and effectively shared for the good of all. However, in order to realize this goal, we need to take account of possibilities and behaviors that may stand in our way. We're familiar with the concept of being "street smart" in the real world. We must now learn how to become street smart in cyberspace, or "cybersmart;" this Handbook is meant to help you accomplish just that.

### What Is Security?

The notion of security in the real world is an intuitive one for most of us. In prehistoric time, security was defined by the essentials of survival such as security against attack by others or by animals, as well as security of the food supply. Other needs, such as security against the ravages of nature or against sickness were generally not available to them. As civilization progressed, the scope of security evolved to include having a place to live and sleep without harm. Along with the concept of private property came the notion of security of possessions.

Much of what we do in the world involves risk, although most of our actions involve minimal risk. For example, when we travel in an unfamiliar neighborhood, or city, or country, we are conscious of the fact that there are threats to physical security. These threats are more substantial if we are in an unprotected place and we meet someone who may be able to take advantage of us. If we are sufficiently concerned about the risk, we will avoid the location or we may choose an alternative, such as joining someone else to return to a safer location, or taking a taxi.

Some actions involve psychological or financial risk, but not physical risk. When we make an investment of any kind, say in land, in stock, or in a business, we do so with the expectation that we will obtain a

return on that investment that is sufficient to justify it. As we know, some investments provide that return, even handsomely, while others do not. Some investments involve emotional risk. When we commit ourselves to a personal relationship, we hope that the relationship will provide emotional security, though we accept the risk that it may not develop that way.

In some areas, it is impossible to obtain the degrees of security that we would like to have. For example, we would all like to live a long and healthy life and many of us will do so. However, what is true for a statistical average of lifetime expectancy is not true for all individuals; some of us will die at an early age, some will develop debilitating illnesses, and others will live, in good health, to old age. Where risk of this sort is concerned, we compensate for our inability to control our physical fate with insurance that protects us against the financial impact of such events, loss of earnings in the case of illness, for example. Such arrangements highlight a truth about security: absolute security is impossible to achieve in real life and in cyberspace. However, security that is "good enough" is likely to be achievable in almost all circumstances.

There are a variety of ways in which we have historically enforced or provided enforcement mechanisms for enhancing and protecting our security. We have physical mechanisms for ensuring the security of our possessions: sturdy building construction, solid doors, and keys and locks. We may rely on other physical barriers, such as walls and other deterrents. We may choose to keep lights focused on an area of potential entry. Finally, assuming that an intrusion is initially successful, we can use alarm systems to detect it and to notify a stronger deterrent force that we need assistance. If an intrusion has been successful, we have forensic techniques at our disposal to search for clues to the event and to track down the culprit. Most important, we can rely upon civil and criminal laws and a system of enforcement and justice that each of our countries is evolving in response to our national needs.

Often we use multiple methods of maximizing our security so that if one method fails, another may work. If a key has been stolen and the lock in the door is no longer a barrier, the alarm signal may suffice to provide notice of an intrusion. The extent to which multiple barriers are used is, of course, related to the value of what is being protected. The extent to which physical security measures are put into effect is related both to what is to be protected and to the reasonable expectations that it will be attacked.

All of these deterrents and methods have their analogues in cyberspace. We're not as familiar with them as we are with physical security issues, but we need to understand them and know how to use them if we are to live as securely in cyberspace as we do in the real world. In both worlds we need to protect our assets, to defend them if attacked, and to recover if the attack is successful.

The dictionary definitions of security are consistent with conditions we associate with security, such as "the quality or state of being secure, freedom from danger, and freedom from fear or anxiety."<sup>15</sup> However, such definitions do not seem really helpful in the context of cyberspace. Instead, we suggest the following: you are secure in cyberspace when access to your information resources is under your control, i.e. no one can do anything to the resources that are yours without your express permission. The resources include computational, access, network, transaction, process and information resources. Of course, some of these resources may have been provided by others for your use, such as an account on a shared computer or access to the Internet by an Internet Service Provider. While they are never completely secure, you have effective control over having continued access to them to the extent that you follow the rules that the providers set for their appropriate use.

An example of the nature of cyber-security is provided here; the recent discovery of a flaw found in the core of the Microsoft Windows operating system:

"Microsoft Corp. acknowledged a critical vulnerability Wednesday in nearly all versions of its flagship Windows operating system software, the first such design flaw to affect its latest Windows Server 2003 software.

Microsoft said the vulnerability could allow hackers to seize control of a victim's Windows computer over the Internet, stealing data, deleting files or eavesdropping on e-mails. The company urged customers to immediately apply a free software repairing patch available from Microsoft's Web site...

The flaw, discovered by researchers in western Poland, also affected Windows versions popular among home users. "This is one of the worst Windows vulnerabilities ever," said Marc Maiffret, an executive at eEye Digital Security Inc. of Aliso Viejo, Calif., whose researchers discovered similarly dangerous flaws in at least three earlier versions of Windows. Maiffret said that inside vulnerable corporations, 'until they have this patch installed, it will be Swiss cheese – anybody can walk in and out of their servers.'

But four Polish researchers, known as the "Last Stage of Delirium Research Group," said they discovered how to bypass the additional protections Microsoft added, just three months after the software went on sale. Although the Polish researchers created a tool to demonstrate the more serious vulnerability and break into victim computers, they promised not to release blueprints for such software onto the Internet ...

Some experts said they expected hackers to begin using this new vulnerability to break into computers within months. Even without detailed

---

<sup>15</sup> Merriam-Webster OnLine Dictionary.

blueprints from researchers, hackers typically break apart the patches Microsoft provides for clues about how to exploit a new flaw.”<sup>16</sup>

As individuals and employees within organizations we have no control over the code contained in proprietary programs like Microsoft Windows. We trust that software vendors have a strong interest in making their programs error free and secure. However, few large programs are completely error free. In response, we can take action when such problems are reported by making an informed judgment whether to download and install the vendor's 'fix' for the error. This is the extent of control that we have.

In real life, we are already knowledgeable about how we protect our information resources. We understand that some information needs to be kept private while other information can be freely circulated. We lock file cabinets and office doors and may store copies of critical information off-site to guard against loss through fire and natural disasters. We know that some information should only be circulated to a limited number of people and we trust different people to different extents depending upon the confidentiality of the information at hand.

The nature of threats to security in cyberspace is conceptually no different than the nature of threats in the real world. The differences come from the characteristics of the electronic space in which the threats appear and the manner in which they can be thwarted, avoided, detected and resolved.

The notions of privacy and confidentiality are related to security. Information that is meant to be private can only be kept private if it is stored in a secure manner. With information in the real world, that may be accomplished by acting as if the information does not exist; such a security policy might be termed “security by obscurity.” Similarly, information that needs to be confidentially shared requires that it be kept secure from those outside the group who are sharing it. If the group is not all in the same place, adequate security policies must include a way of keeping the information secure when it is transmitted among members of the group.

Similar situations exist in the world of cyberspace. However, given the nature of cyberspace and the interconnectedness of the computers within it, the policy of security by obscurity is weak policy and should be avoided. This Handbook will provide details on the special security measures required in electronic space (cyberspace) at several levels.

## Emergence and Growth of the Internet

The computing and networking environment from which today's Internet evolved had its origins in a cooperative research and education culture. When the ARPANET, the predecessor to the Internet, was first implemented, the main goal was to share resources among groups of researchers in different geographical locations.

The groups had compatible goals and worked toward sharing both computing resources and data. Access to the network was restricted to members of the group, so there was no need to be concerned about security at the time. The intent and design of the World Wide Web exemplifies this; it provides substantially better tools for discovering information resources and for making one's own information available to others, without any mechanisms for obtaining permissions or facilitating financial settlements.

The culture of sharing among researchers and academicians that was born in and nurtured by the ARPANET lasted well into the 1990s, and there are still vestiges of it today. It included the notion of making information as available as possible, and that tradition still exists in the form of the World Wide Web, where content of all kinds is being provided, almost free of charge, to hundreds of millions of people around the world. It was a strong culture, and it was responsible in large part for why the Internet has grown to such an enormous size today. Its ethics are reflected in the words of people who are Internet “evangelists,” who see the power of the medium for development, and who work to make it happen. Sometimes called the spirit of the Internet, it is reflected in the mantra that “information wants to be free.”

An alternative way of describing this situation is that the early Internet was based on trust; the community of users trusted each other implicitly to work for the

---

<sup>16</sup> Ted Bridis, The Associated Press July 16, 2003.

common good. As the Internet has broadened its reach and included more and more people with diverse interests and objectives, the trust model has become insufficient. One of the major challenges for today's Internet is to develop a new trust model that is realistic, easy to implement, and effective in its application.

The Internet is different from earlier communications systems in a variety of ways, but several are particularly important. Some differences are best understood when compared to the public switched telephone network (PSTN) that is used worldwide on a daily basis.

The Internet is based upon a model of information transmission called *packet switching*. Every time information is transmitted over the Internet, it is broken up into packets of binary data. The packets are encoded and sent independently over the network, possibly by different routes, and the information is reassembled at the receiving end. This mode of transmission is called packet switching, as opposed to circuit switching. The public switched telephone network uses circuit switching, in which each telephone call is allocated a single circuit for the duration of the call, no matter how much or how little sound is being transmitted at any given moment.

The Internet is “stupid”<sup>17</sup> in that all it knows how to do is to deliver packets from an origin connected to the network to a destination connected to the network. All services originate at the edge, or the boundary, of the Internet in the computers attached to it. This is in contrast to the PSTN where the intelligence is at the center of the network (at the switch), and the user instruments at the edge have little functionality other than being used for speaking and listening.

The Internet is global. It connects many countries, and information generally flows freely across national borders. This characteristic raises interesting policy concerns not necessarily directly concerned with security. The PSTN is also global, but the methods of accessing phones in different countries are not as opaque as they are with the Internet. The user knows that he is dialing a foreign country, for example, whereas he may access a website without knowing where the servers are located.

The Internet is open. Formally defined as a network of networks, any network that conforms to a family of protocols known as TCP/IP (Transmission Control Protocol/Internet Protocol) can connect successfully with it and become a part of it. The standards defining this family of protocols come from the work of the Internet Engineering Task Force (IETF), an informal technical body based on technical meritocracy and the creation of implementable consensual standards.

The Internet is decentralized. There are no system-wide gatekeepers. If you obey the “rules of the road,” i.e. the TCP/IP standards, you can connect your computer or your network to the Internet.

The Internet is abundant. The barriers to entry are low and the amount of bandwidth, (i.e. how fast you can transmit data through it) depends upon the carrying capacity of the copper wires, fiber links, or satellite channels that are in the path. No scarce electromagnetic spectrum is involved for the Internet backbone. Where radio spectrum is used, for example in the deployment of local area wireless networks, often called “Wi-Fi,” the relevant protocols or rules implement a sharing arrangement for the available spectrum rather than a rigid allocation that ultimately denies access to the network.

The Internet is relatively inexpensive for the average user in parts of the world where local calls are free. The price of access over dial-up lines and at cybercafés and other public Internet access points is descending in such countries, so that access is becoming broadly affordable for a greater percentage of the world's population.

The Internet erodes the traditional barrier between author and publisher; you can become a publisher or establish a network service on your computer if it is permanently attached to the Internet. You can advertise the services and, subject to permissions that you establish, anyone else connected to the Internet can connect to your computer and use those services. The Internet is by and large user-controlled. In many countries, you can choose whether your messages and other transmissions should be encrypted or not.

---

<sup>17</sup> See, Lessig, L, *The Future of Ideas*, Random House (2001).

In addition, filtering of messages for whatever reason is under your control, although you may wish to have an external source do it for you, such as instructing your Internet Service Provider (ISP) to filter out spam messages according to rules that you set up.

The Internet is interactive. You can move quickly and easily between access to multiple content providers and sending and receiving electronic mail with many people. While waiting times for on-line services depend upon the size or bandwidth of your connection to the Internet, it is often possible to get response times that support your activities.

The Internet can be vulnerable. Based initially upon a concept of providing services to a relatively homogeneous, cooperative group of people, certain aspects of trust were assumed rather than required to undergo strict verification. This Handbook addresses the Internet's vulnerabilities and provides you with a set of best practices in security that will help you to minimize your vulnerability.

Based on the above characteristics, you should be getting a picture of an Internet that is supportive and permissive of many kinds of activity, rather than one that is restrictive and controlled. This openness strongly reflects the academic and research roots of the Internet, and is responsible for its usefulness for all of us. The Internet was not designed to maximize security, but instead to maximize the fruits of collaborative work; such a degree of openness has provided opportunities for some people to misuse the network in ways that are harmful to others. We need to understand what those misuses are and guard our networks against them.

## Information Security Issues

The concepts of computer, network, and data security in cyberspace are similar to issues in the real world, however, the mechanisms are different. For example, in place of keys (physical or electronic), we have passwords to accounts that allow access to information and services. In place of sealed envelopes, we are able to encrypt information so that it is not readable by others

who cannot unlock that information with the right key.

In comparing the real world with cyberspace, we also observe some of the same violations of trust and confidentiality. In both worlds, it is possible to forge a false return address and even a false signature. In both worlds, it is possible to provide misleading or erroneous information. In both worlds, it is possible to deluge someone with information, either accidentally or deliberately, making it impossible to determine which information is important and relevant.<sup>18</sup> And in both worlds, it is possible to gain access to confidential information and use it in unintended or illegal ways.

There are, however, three important differences.

First, violations of security of all types of cyberspace can take place very rapidly. That means that by the time you understand what is happening to your information assets, it may be too late to prevent damage. Of course, not all violations occur quickly; some attacks are observable as they occur and take time to execute. The lesson to draw from this is that preventive measures taken to protect against violations are far superior to detecting a violation while it is happening or after it has been completed.

Consider the following account of the 'Slammer worm,' which severely disrupted the Internet early in 2003. All continents and many countries were affected, including many developing countries.

"Slammer (sometimes called Sapphire) was the fastest computer worm in history. As it began spreading throughout the Internet, the worm infected more than 90% of vulnerable hosts within 10 minutes, causing significant disruption to financial, transportation, and government institutions, and precluding any human-based response ... "

"Slammer began to infect hosts slightly before 0530 UTC on Saturday, 25 January 2003, by exploiting a buffer-overflow vulnerability in computers on the Internet running Microsoft's SQL server or Microsoft SQL server Desktop Engine (MSDE) 2000. David Litchfield of Next Generation Security Software

<sup>18</sup> The S.S. Titanic used relatively primitive radio to communicate from ship to shore. On its first voyage, the radio operator was so deluged with congratulatory and personal messages that a critical message, warning of significant icebergs in its path, was not identified as important or acted upon. The ship struck an iceberg and sank several hours later.

discovered this underlying indexing service weakness in July 2002. Microsoft released a patch for the vulnerability before the vulnerability was publicly disclosed ([www.microsoft.com/security/slammer.asp](http://www.microsoft.com/security/slammer.asp)). Exploiting this vulnerability, the worm infected at least 75,000 hosts, perhaps considerably more, and caused network outages and unforeseen consequences such as cancelled airline flights, interference with elections, and ATM failures.<sup>19</sup>

Second, you do not have to be physically present at a location, or even in the same country, to commit a security violation in cyberspace. This means that someone in Europe, for example, can probe the security of computers in India just as easily as a person located across the street from the target. In cyberspace, the threat can come from anywhere on the network. It may be directed at a known target, the target may have been selected at random, or it may have been chosen because its Internet address was in a range of addresses being probed as a unit. This omnipresent threat should change the way in which we think about security and the profile of our possible adversaries. It is worth noting that the Digital Millennium Copyright Act makes it illegal to design software that decrypts encryption software; national and global copyright regimes on this and other matters related to copyright and data protection are in active development at the present time.<sup>20</sup>

Third, cyberspace provides a powerful but complex environment, in which the responsibility for security is divided among multiple players. If you are a user of computing and network services, there are a number of ways to protect yourself and your personal computer. However, you cannot control your ISP's security policy or its implementation. Nor can you control your client's software, even if you are closely linked with their systems. Thus you need to assume a protective stance over your own assets, while being aware that the connections you are making with the outside world prevent you from eliminating all vulnerabilities on the network.

What are the possible risks in cyberspace? If you take no security precautions at all, here are some of the possible consequences:

Information destruction. The data stored on your computer could be deleted. It might be possible to recover it, but it could take time and the recovery might not be complete. If you are a government agency, your ability to perform your functions during this period may be compromised.

Information theft, and loss of privacy. You may or may not be aware of the theft immediately (or ever) and it is unlikely that you will know who took your data, what was taken, or what will be done with it. If a great deal of your personal information is taken, the thief might be able to steal your identity with unknowable, but probably serious, consequences.

Loss of information integrity. The information on your computer could be modified without your knowledge. Depending on what kind of information you keep, the consequences could range from trivial to disastrous.

If the data include enterprise financial records, customer information, order status, or personnel files, your business dealings could be adversely affected,

Loss of network integrity on other systems and/or networks. Although you may not be attacked directly in this case, other computers to which you have access may be attacked with trickle down consequences to you. If you are a financial institution, you may not be able to complete financial transactions during the recovery period.

Keystroke capturing. Hidden software could be installed on your computer that would capture your keystrokes and send them to another computer. This could compromise your access to external sources, such as a protected web server, an e-mail server, financial transactions, or confidential information. Authentication tokens such as credit card numbers and passwords could be obtained by the thief and used in later transactions for his or her personal gain.

<sup>19</sup> Moore, Paxson, Savage, Shannon, Staniford and Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy*, Vol. 1, No. 4, July/August 2003, pp. 33-39.

<sup>20</sup> For an overview of recent thinking on the Act, see the U.S. Copyright Office Digital Millennium Copyright Act Study at: [http://www.copyright.gov/reports/studies/dmca/dmca\\_study.html](http://www.copyright.gov/reports/studies/dmca/dmca_study.html)  
The DMCA itself is available as a pdf file: <http://www.copyright.gov/legislation/hr2281.pdf>

Denial-of-Access. You could be denied access to your own information, even though it has not been erased. It might appear in encrypted form, where only the intruder has the decryption key.

The cost associated with recovering from any of these attacks is likely to be substantial, and the recovery process is likely to be inconvenient at the least. If you are the director of an enterprise with a critical dependence on your electronic data resources, an extremely malicious attack could lead to the demise of your enterprise. Note that the Slammer worm was indifferent to which countries it invaded and which organizations and computers it disabled; any computer that did not have a Microsoft patch installed was attacked.

One noteworthy security breach that succeeded for more than a year illustrates the novel ways in which security can be compromised in cyberspace:

“NEW YORK (AP) - For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords. Jiang had secretly installed, in at least 14 Kinko's stores, software that logs individual keystrokes. He captured more than 450 user names and passwords, using them to access and even open bank accounts online.

The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments. “Use common sense when using any public terminal,” warned Neel Mehta, research engineer at Internet Security Systems Inc. “For most day-to-day stuff like surfing the Web, you're probably all right, but for anything sensitive you should think twice.” Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals remotely access their own computers from elsewhere. The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around the screen and files open as if

by themselves. He then saw an account being opened in his name at an online payment transfer service. Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as Feb. 14, 2001.”<sup>21</sup>

This Handbook is about security as applied to users, both in the home environment and in small to medium-sized businesses. Therefore, it contains extensive information on security issues, including threats and outcomes of attacks, approaches to protection of your computers, networks, and data, and also policy issues that must be considered before an effective security strategy may be implemented. The ultimate purpose of this Handbook is not to frighten users away from resources offered by the new digital environment, but to empower users to take advantage of this exciting new world in a safe and secure manner. The objective is to develop an in-depth and realistic understanding of what the security problems are, in order to minimize vulnerabilities and reap the benefits from the many positive and powerful aspects of ICTs.

## What Motivates the Security Violators?

In real life, there are a variety of motivations for crimes against personal or organizational security. Financial gain is a major incentive, as is revenge against someone or something that a person feels has wronged them in some way.

The same motivations exist in cyberspace, but there is an additional motive that is apparently quite compelling. Cyberspace is seen as a challenge by one group of people, often called “crackers,” who regard the ability to break into accounts and be mischievous as a game or sport. In other words, they consider it an achievement to be able to break into computer accounts, databases, and network equipment just because it is there, whether or not someone has protected it. This type of behavior does not have a significant analog in the real world.

Crackers generally regard their activities as a victimless crime. What does it hurt, after all, if an account or a

---

<sup>21</sup> Associated Press bulletin, July 23, 2003.

database is broken into, and nothing is altered or stolen? They discount the legal implications and the consequences of such actions. They also disregard the victim's feeling of insecurity that such actions are likely to generate. The analogue in the real world is knowing that someone has broken in to your home and can do so again anytime; it is an intolerable feeling.

Ironically, the Internet aids would-be security violators in an unfortunate manner. Some crackers build "break-in kits" that provide novice crackers the ability to employ sophisticated tools in their efforts. Such tools are often posted in well-known Usenet News Groups, where they can be inspected and downloaded by anyone with access to the Internet. While many of these kits may be harmless, one is never sure, and it is certainly possible to modify a so-called harmless kit to do real damage to the computers and accounts that are accessed with the kit. Here is a recent example of such activity:

"CERT Advisory CA-203-18 documents the latest critical Windows security hole, while CNet reports that a Windows exploit for another flaw could pave the way for a 'major worm attack':

A hacker group released code designed to exploit a widespread Windows flaw, paving the way for a major worm attack as soon as this weekend, security researchers warned. The warning came Friday, after hackers from the Chinese X Focus security group forwarded source code to several public security lists. The code is for a program designed to allow an intruder to enter Windows computers.

The X Focus program takes advantage of a hole in the Microsoft operating system that lets attackers break in remotely. The flaw has been characterized by some security experts as the most widespread ever found in Windows."<sup>22</sup>

This trend toward attacks of increasing power by relatively unsophisticated people is a long-term trend.

Not all security violations involve computers and the Internet. Automatic teller machines (ATMs) have been used for theft of confidential information. In one case, (in the State of Connecticut in the United States)

thieves installed what looked like an ATM machine in a shopping center. When people tried to obtain money from it by entering their card and numeric passcode, the machine reported that it was unable to complete the transaction. However, it recorded the card number and passcode so that unauthorized withdrawals could be made at a later time. In a variant of this method, thieves tapped legitimate ATM machines so that they could record the information as transactions were being completed. Later, the information was used to make unauthorized withdrawals.

Although most visible cyber crimes have been traced to individuals, organizations including governments, are also capable of manipulating aspects of cyberspace for their own purposes. Organized crime may well have an interest in manipulating the network so as to cause results that are in their interest but also represent criminal activity against others. For other organizations, it may be in their interest to manipulate the results of a poll, or even an election, to obtain falsified but favorable results for themselves. Some such groups are well funded and organized, and could in theory pursue such strategies intensively.

It's clear that the potential benefits of our new digital era are enormous. It's important that we protect those benefits by securing our physical environment, our infrastructure, our computers, our communications links, and our information resources. The first step in doing this lies in understanding enough of the technology to make wise decisions on how to provide the required level of security. Many of us have multiple roles: we may use these resources as individuals, we may have a responsibility for the digital systems and services in an organization, and we may be participating to help government adopt and implement policies supporting adequate security.

In each of these roles, we have a responsibility to ascertain that adequate security exists. Unfortunately, security in a complex environment is often only as strong as its weakest link; we must work to ensure that the components over which we have some control are sufficiently robust to defend against the threats that we believe exist.

<sup>22</sup> CNet News.com, July 25, 2003.

## Importance of Security for SME's in Developing Countries

While security is important for everyone, it is of special importance for small and medium enterprises in developing countries. The rewards of being able to move into global markets with the assistance of ICTs can be significant, but the risks of doing so in an insecure manner are substantial.

Many businesses have already made the transition from manual operations to computer-assisted management of the business. Stand-alone computers have been used in many aspects of business in developed countries for some time. Along with the introduction of new computer resources, managers have had to learn about operational issues such as backup, maintenance, software updates, and computerized audit trails, all of which have implications for computer, network, and data security.

With the introduction of network connections, and the possibility of engaging in e-business, the systems and management processes deployed need to be viewed differently. Stand-alone systems are generally product-centered or process-centered, including inventory, ordering, and/or processes such as manufacturing, general ledger, and accounts payable and receivable. Successful on-line e-business systems are organized in a different way; in order to succeed, they need to be designed as customer-centric, with the system tracking the customer's progress through a search for and evaluation of products, placement of an order, completion of the financial transaction, and tracking of the sale shipment. Product and process issues are still important, but now they are subservient to the primary need to track the customer's journey through the business's web site and to assemble and execute any transactions that the customer specifies and submits on-line. Such a redesign is essential for success, but requires an alternative approach to customer transaction management, an approach that, if implemented without caution, may open the door for new forms of security breaches.

Small and medium enterprises should be aware that the reorientation of business systems for deployment on the Internet involves new types of risks. One type of risk, in particular, is new: the possible compromise or theft of

intellectual property assets that are held (and perhaps sold) by the firm. To the extent that goods and services sold are information products, there is the possibility that they will be replicated illegally and distributed either for free or in the gray markets, where profits accrue to the thieves and not the firm that produced the work.

The most obvious example of illegal copying today can be observed in the music industry, which is fighting the distribution of "pirated" recordings, often in CD format. The protection of digitally recorded intellectual property is an unresolved issue at the moment, though there has been considerable effort in the industry to come to grips with new technology and distribution issues, both in the United States and around the world. As long as near-perfect digital copies of information products can be made easily and their origin is not traced back to a specific sale, the gray market for entertainment products will exist. The technology used in music piracy could also be deployed in other circumstances; trade secrets or other confidential information could be lifted and distributed in ways that could damage a business severely. Valuable assets require adequate protection. It is possible to provide this protection, but the risks and methods will be different for a firm in an e-business mode than they were for the firm operating as a traditional business, before e-commerce evolved.

## Towards a New Model of Trust

The new digital environment requires us to re-evaluate our notions of trust. In the real world we use a variety of measures to decide how much to trust a person, a process, or an organization. We have our intuition, which is based upon past experience and match what we observe with what we have experienced. In making such decisions, we assess a person's words, absorb non-verbal communications, and observe events in a rich environmental and informational context. In an exchange of information in cyberspace, most non-verbal elements of communication are missing. When we receive a piece of electronic mail or read a web page, we cannot always tell if the information is accurate and if we see that it is not correct, we do not know whether the errors are the result of negligence or whether there is a deliberate effort to deceive us. In the absence of other information, we do not know if the author is the person that he or she claims to be.

Deception occurs in the real world too, of course, but it is generally easier to determine the truth of a situation with physical actors and real locations.

Fortunately, some help is on the way in cyberspace through the concept of a certification authority. This is an authority that is formally recognized as providing authentication for the identity of an individual or organization. This concept exists in the real world as well; if you hold a national passport, your government presumably has authenticated your identity and the passport is the token that you can present to prove it. Similarly, if you have a license to drive a motor vehicle, a regional or national agency of your government has issued the license, both authenticating you and also granting you the privilege of driving a vehicle. Credit card companies authenticate you through the issuance of credit cards. Your employer or school may authenticate you through an identification card. This card may authorize your access to certain services that they are providing for employees or students in their domain. Clearly, there are quite a few certification authorities in the real world. Generally each of these authorities has a special purpose in authenticating you, although the proof of authentication may be used for broader purposes. The thoroughness of the authentication differs from authority to authority; some may require detailed proof of your identity, while others may accept what you say without validation.

Certification authorities in cyberspace share these properties. Various levels of certification provide for different degrees of assurance that the certification is correct. Multiple certification authorities exist in cyberspace, although it's more likely that one certification will be sufficient for most or all purposes. In addition, with electronic certification, certificates can be 'signed' electronically in a way that provides certainty that the certification transmitted is genuine and accurate. Such a system of certification is more formal and quantitative than the intuitive and experiential methods used in the real world. In the digital world, we need to rely on more formal methods to establish the trust required to support business and financial transactions conducted over electronic networks.

Governments have a role in ensuring that adequate mechanisms exist so that new trust models are viable and helpful for its inhabitants. Small and medium sized enterprises, in particular, depend upon the existence of trust when doing business electronically. In some countries, governments believe that government agencies should act as certification agencies, either exclusively or not. In other countries, governments believe that the certification authority function should be left to the private sector. Regardless of the specifics of the implementation, the goal is clear. Government policy can facilitate trust mechanisms that will enable its inhabitants, individual and organizational, to participate in e-commerce activities on an equal footing with other countries.

## Summary

Digital technology provides us with exciting new tools that can have a major impact on education, health, commerce, and other sectors of civil society. This technology benefits all countries and people, but has a special attraction for developing countries in that it can help to accelerate their integration into the world economic community. The technology is still in its infancy, but it is developing rapidly. Unfortunately, as with other technology developments, the Internet can be used for good or evil. As we have seen, there are crackers and cyber criminals using it to attack individual users and all types of organizations.

The notion of safe computing, or being "cyber safe," is an important one. The examples in this chapter, the rate of incidents reported to the CERT, and the new incidents reported in the press on a daily basis, show why it is important to be aware of security issue and why you should take steps to ensure that your business and personal computers and data are protected. This Handbook contains a set of current "best practices" in security that may assist you in implementing the policies and procedures that are relevant to your specific situation. In addition, this Handbook also includes ample references to other materials, both electronic and print, that cover specific aspects of IT security. There are links to professional organizations that focus on IT security issues as well; all of these resources will be useful to individuals and organizations seeking to deepen their knowledge of security in a networked world.

The stakes are high for developing countries. Foreign direct investment, confidence, and trust in a developing country depend upon a secure and effective implementation of technology and infrastructure. Governments, organizations, and individuals all have a part to play in assuring the security of the country's electronic and information assets. Knowledge of the threat is paramount; appropriate action based on such knowledge should produce an environment of trust that is conducive to progress and to realizing the benefits of the new digital age for as many inhabitants of Earth as possible.