1 Historical Reference Points in the Computer Industry and Emerging Challenges in Cybersecurity

THOMAS A. JOHNSON

Contents

1.1 Introduction 2
- 1.1.1 First Generation Computers, 1951–1958 4
- 1.1.2 Second Generation Computers, 1959–1964 4
- 1.1.3 Third Generation Computers, 1965–1971 4
- 1.1.4 Fourth Generation Computers, 1971–1990 4
- 1.1.5 Personal Computers 5
- 1.1.6 Advanced Research Projects Agency Network, Internet, and World Wide Web 6
- 1.1.7 Fifth Generation—Emerging Technologies 8
- 1.1.8 Fifth Generation—Challenges and Game Changers 8

1.2 Dark Side of the Computer: Viruses, Trojans, and Attacks 9
- 1.2.1 Development of Computer Viruses 9
- 1.2.2 Contemporary Threat Landscape 11
- 1.2.3 Threat Attacks 11
- 1.2.4 Botnets and Cyber Crime Applications 15
- 1.2.5 TOR and the Deep Web 17

1.3 Vulnerabilities, Risk Assessment, and Risk Management 18
- 1.3.1 Mobile Devices and Smart Phones 18
- 1.3.2 Web Applications 19
- 1.3.3 Social Media 19
- 1.3.4 Cloud Computing 21
- 1.3.5 Big Data 23

1.4 Emerging Field of Cybersecurity 26
- 1.4.1 Framework for Improving Critical Infrastructure Cybersecurity 27
- 1.4.2 Risk and Threat Assessment 28

1.5 Summary 28

Notes and References 29

Bibliography 30

1.1 Introduction

James O. Hicks Jr. provides a fascinating outline of the early developments in the data processing field by noting the abacus as the first known device capable of making calculations, something so fundamental to the development of today's computer industry. Whereas the Greeks and Romans used the abacus in ancient times, the Chinese made significant improvements to it. The next major introduction into the field of calculations occurred in 1642, when a French mathematician, Blaise Pascal, developed a "gear-driven" mechanical calculator capable of addition, subtraction, and multiplication. Twenty-nine years later, in 1671, a German mathematician, Gottfried Leibnitz, improved upon Pascal's design, and his new mechanical calculator could offer both division and the ability to determine square roots.[1] The concept of performing calculations from beads to abacus to the use of mechanical wheels was fundamental to the modern computer industry's development.

The next major historical contributions occurred in the early 1800s, when Joseph Jacquard developed a loom for production of fabric and clothing. Significant to the eventual emergence of a modern computer industry was Jacquard's use of "punched cards" as the control mechanism in his loom. By sequencing the punched cards, the loom could produce a cast number of patterns and designs. When the punched cards for a particular pattern were repeated, the same pattern would automatically be repeated. Thus, in effect, Jacquard's punched cards were the program for the loom. In 1812, Charles Babbage, an English mathematician, visualized that many of the principles of Jacquard's loom and its use of punched cards could be applied to numerical computation. Babbage's very important observation focused on the use of punched cards as computing steps that were stored on the card in advance of computation, and this allowed a machine to process data totally unaided. Babbage's observation and work were responsible for the first development of the concept of the "stored program" for data processing. This is precisely the capability that differentiates computers from calculators, and Babbage called his first machine a difference engine and designed it to calculate logarithm tables. The major components of Babbage's analytical engine were as follows:

- Input and output devices
- An arithmetic unit to perform calculations
- A memory (punched cards) to store the calculations

As a result of his work, many regard Charles Babbage as the first person to propose the concept of the computer.[2]

An important contributor to Babbage's research was Augusta Ada Byron, the daughter of Lord Byron, the renowned English poet. Ada Byron was

an accomplished mathematician, and she analyzed and improved many of Babbage's concepts. As a result of her work in developing and programming the mathematical tables for Babbage's analytical engine, she has been recognized as the first programmer. In fact, the programming language ADA is named in her honor.[3] It is interesting to note that years later, the U.S. Department of Defense favored a substantial number of their applications to be based in what obviously was an improved ADA programming system.

Additional improvements in the punched cards were forthcoming by the late 1870s, and Henry Metcalfe discovered a need to reorganize a cost-accounting system that would take records out of the leather board folios in use at the time and allow a more effective way to retrieve information from the ledgers by transferring accounting records from ledgers to punched cards. These cards could be sorted and information more easily and quickly obtained than by the conventional accounting ledgers. Metcalfe developed a coding scheme and unit records to specify the flow of data. Ten years later, in 1880, Herman Hollerith, a statistician at the U.S. Census Bureau, followed Metcalfe's ideas and began experimenting with punched cards for their use in data processing for the 1880 U.S. Census. Hollerith designed a tabulating machine that used the machine-readable punched cards, and within six years, he founded a company that, by 1911, merged with three other companies forming the Computing Tabulation Recording Company, known then as CTR. In 1924, the CTR Company was renamed as the International Business Machines Corporation and emerged as IBM.[4]

The next refinement occurred in 1908 by James Powers, who refined Hollerith's machine by developing a sorting machine with tabulators that were used in the 1910 Census. Powers also formed a company he named the Powers Accounting Machine Company, which, in 1926, merged with the Remington Rand Corporation and then merged with the Sperry Gyroscope Company to form the Sperry Rand Corporation, and they produced UNIVAC computers. Eleven years later, in 1937, the MARK I digital computer was built by Howard Aiken and IBM engineers, and Grace Murray Hopper programmed the MARK I. Grace Hopper became an Admiral in the U.S. Navy and was an important contributor to various computer languages, especially COBOL.[5]

In 1939, at the University of Pennsylvania, John Mauchly and J. Presper Eckert Jr. led a team of engineers who developed the first electronic digital computer named ENIAC. The ENIAC computer was completed in 1946 and used vacuum tubes. The ENIAC weighed over 30 tons and covered 1500 square feet of floor space. In 1945, the binary number system was developed by John Von Neumann, a Princeton University mathematician. This number system used zeroes and ones as on–off and magnetized and not-magnetized as states that ultimately facilitated the design of electronic computers and formed the fundamentals for today's electronic computers.[6]

1.1.1 First Generation Computers, 1951–1958

Included the UNIVAC-1;
Used vacuum tubes for controlling functions;
Used magnetic drums for primary storage;
First generation software used symbolic language for programming; and
Machine language programs were used by the binary forms of zeroes and ones.

1.1.2 Second Generation Computers, 1959–1964

The transistor replaced the vacuum tube and made possible the second generation of computers;
Magnetic tape was introduced and replaced the need for punched cards; and
COBOL and FORTRAN programming languages were introduced.

1.1.3 Third Generation Computers, 1965–1971

Integrated circuits made possible the third generation of computers as incredible numbers of transistors were deposited on a silicon chip, thus introducing the era of miniaturization and increased speed.

The nanosecond (one billionth of a second) became the new standard for measuring access and process time.

IBM's System/360 computers and the first minicomputer by Digital Equipment Corporation were introduced.

Online computers and remote terminals became popular using regular telephone lines from remote locations.

Business applications increased, especially in the airline reservation systems and real-time inventory control systems.

1.1.4 Fourth Generation Computers, 1971–1990

The introduction of large-scale integrated (LSI) circuits for both memory and logic made the IBM 370 mainframe possible by LSI circuits.

The movement to the very-LSI circuits made it possible to place a complete central processing unit (CPU) on one very small semiconductor chip. This resulted in increased computer performance with a phenomenal lowering of the cost of computers. The processing power of mainframe computers in the 1960s costing millions of dollars was now available for use in personal computers (PCs) for less than $1000.

The emergence of the microcomputer or PC was a major advancement, especially with user-friendly software and graphic terminals.[7]

1.1.5 Personal Computers

The evolution of the PC, known as the personal computer, profoundly changed the entire computer industry. While the fourth generation of computing actually made possible the achievement of the PC, its interface was responsible for propelling us into the fifth generation of computing. First, we will review the more salient developments in the era of personal computing, which can be marked by the following developments:

1975—The ALTAIR 8800 became the first PC
1977—The Apple I, II, and Commodore Computers
1981—The IBM-PC Home Computer
1983—Apple Lisa Computer
1984—Apple MacIntosh Computer

The above PCs emerging in this decade required software, and the operating system of most significance was Microsoft's MS-DOS system. However, the interesting feature was how the ALTAIR 8800 computer, which had little to any application capability, did in fact inspire many hobbyists to acquire it. Foremost among these hobbyists were Steve Jobs and Steve Wozniak, and they would, within two years, introduce their Apple I and II computers. This computer proved to be an enormous hit with all those watching this new PC industry; however, some skepticism remained regarding these new PCs, that is, until 1981, when IBM released its new PC-Home computer, and this had the effect of legitimizing this new industry. After all, IBM virtually owned the entire computing industry with its worldwide mainframe dominance. The world took notice of the possibilities of personal computing because IBM entered this market.

IBM's entrance into the personal computing market was made with several major strategic decision failures. First and foremost, IBM made the decision to outsource the development of the PC's operating system, and they offered the contract to Microsoft, which developed the MS-DOS operating system. The second major mistake IBM made was in their failure to restrict the licensing of the MS-DOS operating system to IBM-Home PCs. Even more incredible, IBM possessed the personnel, skills, money, and capabilities by which they could have developed their own operating system and did not need to contract this to Microsoft. A third major mistake IBM made was to use off-shelf parts to construct their PC, and when small new companies discovered this fact, they were able to do the same by simply buying off-shelf parts and then license the MS-DOS operating system from Microsoft, which

had no restrictive licensing to only sell to IBM. In effect, IBM's presence enabled all unknown small companies to enter this market because of the world respect for IBM.

A fourth major error IBM made upon their entrance into the PC market was a total judgment error in terms of the future of the PC. IBM estimated that the total worldwide production of PCs over their entire lifetime would be 250,000 units. In fairness to IBM, they were selling mainframes in the million dollar cost structure to business corporations throughout the world, and they simply could not envision this "hobby or toy" culture emerging to compete with major corporations, especially since at the time of their ill-fated decisions, software applications for the PC did not yet exist. In short order, these software applications did emerge in the form of the following:

1978—VISICALC spreadsheet software
1979—WordStar software

Each of these products was improved by other companies, and Lotus 1-2-3 emerged as an industry-wide spreadsheet. Also, WordPerfect would become an important part of the eventual word processing Microsoft Office Series.

The historical emergence of the computer industry through the 1970s would be propelled by an incredible acceleration of growth as a result of the Internet and, ultimately, the World Wide Web.

1.1.6 Advanced Research Projects Agency Network, Internet, and World Wide Web

The Advanced Research Projects Agency Network (ARPANET) began operation in 1969 with four nodes (sites) as a result of the Advanced Research Projects Agency experiment by the Defense Advanced Research Projects Agency. This experiment expanded to 37 nodes by 1973, and in 1977, it started using the Internet protocol (IP), a universal connector of networks. By 1997, after the ARPANET was founded, the Internet counted over 20 million computers and 50 million users. The Department of Defense began work on an experiment in communications and resource sharing in the 1950s, an era of concern due to the growth of intercontinental ballistic missiles. The Department of Defense was concerned about the ability of the United States to survive a nuclear first strike and decided that research on a communication network should be supported. Paul Baran of the Rand Corporation was the principal designer and force behind the creation of this new communication system and the following features guided its development:

1. Redundant links;
2. No central control;

3. All messages broken into equal size packets;
4. Variable routing of packets depending on the availability of links and nodes; and
5. Automatic reconfiguration of routing tables immediately after the loss of a link or node.[8]

Larry Roberts of the Massachusetts Institute of Technology's Lincoln Laboratory and J.C.R. Licklider of the Defense Department's Advanced Research Project Agency focused on building networks that made sharing of computers and data both economical and cost effective. In 1965, Larry Roberts and Donald Davies of the National Physical Laboratory in England proposed a packet switched computer network using telephone lines to process messages in speeds from 100 kilobits per second to 1.5 megabits per second and switching computers that could process 10,000 packets per second with interface computers connected to mainframe hosts. Leonard Kleinrock of the University of California, Los Angeles produced analytic models of packet switched networks that were critical to the guide design. In 1968, the Advanced Research Projects Agency awarded a contract to Frank Heart at Bolt Beranek and Newman to build the first interface message processors to connect mainframes and their operating systems to the network. The fact that networks now had to be connected together resulted in Vinton Cerf designing a new protocol that would permit users to interconnect programs on computers in different networks. In 1977, Cerf completed his design of what would become the Internet as most people know it. Vinton Cerf designed a matched set of protocols called transport control protocol (TCP) and IP. The IP protocol routed packets across multiple networks and the TCP converted messages into streams of packets, reassembling them into messages.[9]

The massive investment in research by the U.S. government led by both the Department of Defense and the National Science Foundation enabled the creation and growth of the Internet from 1969 until 1989. The work of many research scientists proved both important and invaluable as their efforts resulted in unifying many networks and ultimately provided a stable and valuable community of networks. By 1989, the ARPANET was officially disbanded, and finally, the backbone of the management of the Internet was transferred to commercial Internet service providers (ISPs) from the National Science Foundation in 1996.[10]

Tim Berners-Lee of CERN, the Zurich-based Research Center for High-Energy Physics, designed the Universal Resource Locator to name documents and the hypertext transfer protocol (HTTP) to transfer the documents. His design included the hypertext mark-up language (HTML) to identify text strings that were active hyperlinks within a document. He named this system of Internet-wide linked documents the World Wide Web, and it was received in 1990 with wide acclaim and usage. Additionally, Marc Andreeson's work at

the University of Illinois' National Center for Super Computing Applications brought Tim Berners-Lee's World Wide Web into even greater prominence as Andreeson designed the Mosaic browser as a simple, easy-to-use multimedia interface for the HTML documents and the HTTP protocol. In 1992, this design accelerated the Internet throughout the world.[11]

1.1.7 Fifth Generation—Emerging Technologies

The continuing development of technologies and refinement of software have resulted in remarkable advances and inventions. The transition from an analog world to a digital world has provided unparalleled convergence of communications, publishing, entertainment, and capabilities delivered through devices ranging from cell phones to a wide range of appliances and computers. The advance in multimedia, virtual reality, artificial intelligence, and robotics is challenging all aspects of human behavior. In the process of this fifth generation and emerging technologies, we see governments being challenged as their control of information and communication systems is in fundamental change. Additionally, the issue of privacy and its sense of loss to the individual is growing daily by the very presence of social media and the number of applications developed for a range of devices being created throughout the world.

Researchers and scientists are working on a number of interesting technologies, and at the same time, commercial firms are also pursuing their next design for products they hope will be a "breakthrough" revenue producer.

1.1.8 Fifth Generation—Challenges and Game Changers

Big data
Predictive analytics
3-D printing
Cloud computing
Wearable user interfaces
Mobile robotics
Neuron chip sets
Quantum computing
Internet of Things

Each of these items will shape the contours of our future, and each owes its potential to those historical efforts and research discoveries of the past years. Further, each of these items will have a very profound effect on our lives and on the computer industry and its personnel. Our privacy and security will continue to be challenged by these game-changing discoveries.

1.2 Dark Side of the Computer: Viruses, Trojans, and Attacks

A computer virus is computer code that is designed to insert itself into other software and, when executed, is able to replicate itself and propagate with the host software or file. Viruses can be designed to damage the infected host by corrupting files, stealing hard disk space or CPU time, logging keystrokes to steal passwords, creating embarrassing messages, and other activities all performed without the computer user's approval or knowledge. Early viruses were boot sector viruses and spread by computer users sharing infected floppy disks. Other viruses attached to e-mail or a part of the body of an e-mail, and when the code viruses were executed, a message with the virus embedded was sent to other mail clients. In some cases, the code could be designed to provide the scripts access to the user's address book and could, in turn, propagate and use those addresses to further propagate the virus-infected message. Other viruses were designed to be attached to data files such as word documents or spreadsheets. These scripts are visual basic code that can execute when the file is loaded, and once the virus has attached itself to an application, the code in the virus will run every time the application runs.[12]

Eugene H. Spafford notes that the first use of the term *virus* as referring to unwanted computer code was offered by Gregory Benford, a research physicist at the Lawrence Livermore Radiation Laboratory, who noticed that "bad code" could self-reproduce among laboratory computers and eventually got into the ARPANET.[13] However, John Von Newmann actually developed the theory of self-replicating programs in 1949. In 1983, Fred Cohen formally defined the term *computer virus*, and he created an example of the self-reproducing code and named it as a computer virus to describe a program that is created to affect other computer programs by modifying them to include a copy of itself in the program.

1.2.1 Development of Computer Viruses

1981—Elk Cloner virus
1986—The Brain virus
1999—Melissa virus
2000—I Love You virus
2001—Code Red virus
2002—Nimda virus
2003—Slammer virus
2004—My Doom virus

The Elk Cloner virus was written for Apple DOS 3.3 and spread via floppy disks; it displayed a short poem and was activated on its 50th use. The Elk Cloner virus was the first PC virus.

The Brain virus was the first worldwide virus to also spread by floppy disks, and the two brothers in Pakistan who wrote the virus did not intend for it to be a destructive virus, yet despite their intentions, it materialized into one.

The Melissa virus was based on a Microsoft Word Macro and was designed to infect e-mail messages by sending infected word documents to the first 50 people in a user's outlook list. The Melissa virus was reported to cause more than $50 million in damages to other computer users and businesses.

The I Love You virus infected millions of computers in a single day simply because the attachment stated "I Love You" and people's curiosity caused them to open the infected attachment, which, when opened, would copy itself in different files on the user's hard drive and also download a file that stole passwords from the victim.

The Code Red virus was directed to attack the U.S. White House as a distributed denial-of-service attack, but it was stopped before it could effect the attack. However, this virus did infect thousands of computers and caused over $1 billion dollars in damages. A second version, Code Red II, attacked Windows 2000 and Windows NT systems.

The Nimda virus was one of the fastest propagating viruses to enter the Internet, and its targets were Internet servers; it really worked as a worm and caused significant damage to many users.

The Slammer virus in 2003 was a Web server virus that also roamed through the Internet at incredible speed. Many corporations in both the financial services and airline industries suffered significant losses estimated in the range of several billion dollars.

The My Doom virus used a denial-of-service attack script and sent search engine requests for e-mail addresses, causing companies such as Google to receive millions of requests and severely slow down services and, in some cases, to close down companies.

Worms do not change other programs, but a worm is a computer program that has the ability to replicate itself from computer to computer and to cross over to network connections. It is important to stress that while worms do not change other programs, they may carry other code that does change programs, such as a true virus.[14]

In 2007, the "Storm" worm used social media approaches to fool computer users into situations where they loaded botnets into their computers, and Bruce Schneier reported that millions of computers were infected by this worm, which carried virus code as well.

A Trojan horse is a program that masquerades as a legitimate application while also performing a covert function. Trojan horse programs do not propagate on their own, so they rely on users to accept the executables from

untrusted sources. Consequently, this becomes a major social engineering problem.[15]

1.2.2 Contemporary Threat Landscape

The previously discussed boot sector viruses, file viruses, and macro viruses were some of the earliest targets for virus designers. However, as we move to describe contemporary threat targets, we should also include multipartite viruses, stealth viruses, and polymorphic viruses. In addition to these very difficult viruses, we will also discuss toolkits for distribution of malware and other cyber attack modalities.

Multipartite viruses are a hybrid that can infect files in both the boot sector as well as program files. After the boot sector is infected, and when the system is booted, the multipartite viruses load into the memory and begin the process of infecting other files. As a result of their movement, these multipartite viruses are difficult to remove. If the multipartite virus is both dangerous and difficult to remove, the Stealth viruses are even more difficult to both identify and remove since they are designed to use specific methods to hide themselves from detection. Ankit Fadia describes their method as follows:

> …They sometimes remove themselves from the memory temporarily to avoid detection and hide from virus scanners. Some can also redirect the disk head to read another sector instead of the sector in which they reside. Some Stealth viruses such as the Whale virus conceal the increase in the length of the infected file and display the original length by reducing the size by the same amount as that of the increase, so as to avoid detection from scanners. For example, the Whale virus adds 9216 bytes to an infected file and then the virus subtracts the same number of bytes, that is 9216, from the size given in the directory.[16]

Polymorphic viruses are the most difficult virus to identify because they are designed to mutate or change the viral code known as the signature each time they spread or infect files. Since antivirus software is created on the basis of the signature of the virus, it becomes almost impossible to be protected against the Polymorphic virus unless the antivirus software vendor has provided a new "patch" to guard against it.[17]

1.2.3 Threat Attacks

Spear-phishing
APT's-RSA SecurID attack
Zero-day vulnerabilities; Operation Aurora-Zero Day Malware Attack
Rootkit-Stuxnet; toolkits
Malware—Flame

Mobile malware
Botnets—DDoS; spam; click fraud
Bots—cyber crime applications

Spear-phishing attacks are more focused than the typical phishing attacks since the typical phishing attack is sent to thousands of people and usually displays a fake logo of an individual's bank asking for them to provide some information as to their log-in or to go to the site and change their password. On the other hand, spear-phishing attacks are more focused on specific individuals, usually at an executive level. Since Web pages provide so much information on companies and their personnel, it is available for those who wish to penetrate the corporate structure by studying and doing in-depth research on the potential target employee. Upon acquiring information as to the potential targets interests, hobbies, etc., the attacker begins to formulate an attack methodology so as to acquire the target employee's interest and confidence. For example, if the target employee is an avid sports car or football enthusiast, the attacker would design information that could be incorporated within an attachment that the target might be interested in obtaining further information about, under the expectation that by opening the file or attachment, the information would be provided. This attachment or link, when opened, would then install malware on the target employee's computer. The malware then installed on the host would await instructions from the command and control (C&C) server owned by the attacker. The attacker could take action immediately or could wait for another time, meanwhile having greater access to the entire corporation through the executive level employee. This spear-phishing attack is also useful to acquire information from government or military employees who could be vulnerable to the same type of attack.

APT attacks, or Advanced Persistent Threats, are sophisticated network attacks in which the attacker seeks to gain information and remain undetected for a substantial period of time, thus acquiring a great deal of information and knowledge on the target. It is certainly possible that a spear-phishing attack might provide the attacker this presence and opportunity. APT attacks are not designed to do damage, but to acquire information or modify data.

Zero-day vulnerabilities that may, at some point, become a zero-day attack are operationalized and successful when the attack is targeted against a software or hardware system's unknown vulnerability. Since the vulnerability is not recognized, a software patch or hardware fix has not yet been offered. The attacker seeks to discover the potential vulnerability, and if discovered, the attacker will keep this program vulnerability private until the time for the attack is determined to be most provident. In short, this search for an exploitable opportunity is to locate something new and totally

unknown and to keep it secret until a future attack or decision to sell this information to other cyber criminals.

Rootkit is a set of tools that enable root- or administrator-level access to a computer system. The term *rootkit* has become synonymous with malware and is used to describe malware with rootkit capabilities. However, rootkit can be used for legitimate purposes as well as for malicious purposes. If rootkit is coded with malware to gain root access and take complete control of the computer's operating system and its attached hardware, and then to hide its presence in the system, we then have a very complex toolkit. The Stuxnet incident against the Iranian Natanz uranium enrichment facility was accomplished through the use of a rootkit that permitted entrance into the computer system and the planting of a very sophisticated computer worm used in the attack, which clearly fit the definition of an APT attack, since the attacker had to possess expertise in cyber intrusion methodologies and also was capable of designing state-of-the-art exploits and tools.

The RSA SecurID attack was also an Advanced Persistent Attack in 2011 that compromised RSA's two factor authentication token devices. Several Department of Defense contractor corporations were victimized by this attack, and depending on how long the attackers were inside their systems, we have no idea as to the level of data ex-filtration or knowledge that may have been collected by our adversaries responsible for this APT attack. It is generally assumed that Chinese People's Liberation Army authorities were responsible for this action.

Flame was perhaps one of the most serious attacks occurring in 2012, and it utilized C&C channels installed on servers to download very high-tech malware estimated to be 20 megabytes in size or at least 30 times larger than a typical computer virus. This APT attack was launched against the Iranian oil terminals to collect intelligence in preparation for cyber-sabotage programs designed to hamper and impede Iran's ability to develop nuclear weapons.[18]

Toolkits that are emerging as attack toolkits are software programs containing malicious code designed for both the novice and more experienced cyber-criminal to facilitate their ability to launch attacks against networked computers. An example of an attack toolkit that has been most effective in allowing cyber-criminals to steal bank account numbers from small businesses is named ZeuS, and in 2010, one group of cyber-criminals used ZeuS to acquire $70 million from online banking and trading accounts in an 18-month period. These attack toolkits are often sold on a subscription-based model with regular updates that extend both the exploitable capabilities as well as support services for the attack toolkit. The demand for these attack toolkits has increased since 2006, when some kits were sold for $100 or less. In 2010, ZeuS 2.0 was selling for $8000. Symantec's Security Technology and Response Team discovered 310,000 domains that were found to be malicious

and resulted in 4.4 million malicious Web pages per month and 61% were attributed to attack toolkits.

The most prevalent attack kits are the following:

- MPack
- Neosploit
- ZeuS
- Nukesploit
- P4ck
- Phoenix

These attack kits are easy to update and are able to tell their cyber-criminal customers they can target potential victims before security vendors can apply the necessary security patches to prevent the attack.[19]

Mobile malware is now one of our most perplexing problems to address, particularly since more smart cell phones were sold in 2012 than computer laptops. The growing number of people using cell phones or tablets has created enormous problems for corporations as the BYOD (bring your own devices) has virtually overcome corporate Chief Information Officers (CIOs) to maintain any semblance of security for their information and data systems. Quite simply, the introduction of mobile malware brought into the corporate environment or government environment is exceedingly easy. It is not only the introduction of malware by these devices that is bringing problems into the Information systems, but it also is too easy to exfiltrate data since most smart devices have Bluetooth capabilities and near field communication (NFC) capabilities that automatically load data into their devices. In fact, Zitmo is the Trojan that can forward text messages with confidential information from a device to other phone numbers.

Zitmo is used by the cyber-criminal in the following manner: the cyber-criminal sends a text message that appears to look official requesting the targeted victim to update their security certificate or other software updates. The attached link that the targeted victim receives actually installs the Zitmo Trojan on to the victim's smartphone. If the victim executes this attached link, the Trojan returns the message to the cyber-criminal, who is now able to access the victim's bank records and possibly initiate transactions to transfer money from the targeted victims account to the cyber-criminal's account.

DroidKungFu is a malware that contains a rootkit permitting the cyber-criminal to have full control of the targeted victim's smart phone or mobile device. This Trojan is specifically targeted for devices using the Android operating system and is difficult to detect due to the rootkit malware that is capable of hiding the Trojan and attached malware. A cell phone virus does exactly what a computer virus can do to computers, and that is to send targeted victims executable files that infect the smart phone or mobile device.

The Symbian Operating System as well as Apple's Mobile Operating System (iOS) and Android have all been targeted by cyber-criminals to send viruses. CABIR was one of the first cell phone viruses, and Common Warrior followed as a more effective virus, but there are numerous viruses being prepared to take advantage of the large base of mobile users who now have interaction with corporate information and data systems.

Another difficulty is that software vendors have only recently begun preparing antivirus software for the smart phone market. The typical smart phone user is ignoring the need to install antivirus software. Shortly corporations, government agencies, and universities will have to address this problem of securing mobile devices that connect to their information and data systems. An approach that could be considered for establishing policies on mobile devices might contain some or all of the following restrictions:

- Devices must have current security patches.
- Devices must be password enabled.
- Two-factor authentication.
- Containerized capability.
- List of unauthorized Apps, such as "Jail Breaking" and "Rooting," and other Apps to be determined.
- Secure wireless access points and networks.
- Review BYOD policies annually and provide employees with copies of the policies.
- Initiate webinars informing employees of recent attacks and safe practices for the use of computer and Information systems.
- Have a recovery plan in place.

A very difficult challenge for CIOs, network managers, and Chief Information Security Officers (CISOs) regarding the number of BYOD brought into their information system environments is they simply do not know what devices are attaching to their network, and they clearly have no idea as to the types of applications that are running many of these BYOD devices. Further, so many of today's BYOD smart phones and tablets have embedded applications that will automatically seek out and transfer data to or from the device without the user even initiating the transfer action.

1.2.4 Botnets and Cyber Crime Applications

A botnet is not necessarily malicious as there are legitimate purposes and uses for automated programs that execute tasks without user intervention. However, botnets have recently gained notoriety for becoming a significant threat to the Internet due to the increasing malicious use of this technology by cyber-criminals. A botnet is a network of compromised computers that

can be coordinated remotely by a cyber-criminal or an attacker to achieve an intended and malicious purpose. The malicious goal may range from initiating a distributed denial-of-service attack, spam attack, click fraud attack or simply renting out an attack service to individuals who may want to have some other person or entity attacked. Thus, the botnet is a network of computers already under the control of the individual who will function as the central entity to control and communicate with each machine. The host components are the compromised machines that are under the control of the Bot Master. The malicious agent that enables a compromised computer to be remotely controlled by the Bot Master is called a Bot Agent. A Bot Agent can be a standalone malware component such as an executable or dynamic link library file or code added to the malware code. The Bot Agent's main function is to be the communication link with the botnet network. This permits the Bot Agent to receive and interpret commands from the Bot Master and to send data back to the Bot Master or to execute attacks as a result of the Bot Master's instructions. The C&C channel is the critical online resource of the Bot Master that permits the control of the bots. Without the C&C channel, the Bot Master cannot direct the malicious activity of the bot. Since the strength of the bot resides in the number of compromised computers under the control of the Bot Master, one can appreciate how important computer security is, so that those acting as Bot Masters cannot add more compromised machines to their collection.[20]

Examples of the malicious use of botnets are found in distributed denial-of-service attacks where the compromised machines are all directed to attack a predetermined victim, corporation, or government entity at a specific time and date. The result of such a massive attack in a simultaneous manner will create a buffer overflow problem for the targeted site's servers and take their site and service down. This type of an attack can also be used to send volumes of spam to a designated target hit.

Click fraud is another example of how a Bot Master can direct their bots to specific sites for the purpose of collecting revenue from advertisers who pay to have potential customers click on their website. Since online advertisers pay for each click of the ads they have on websites, this provides an opportunity for the cyber-criminal to make money from this scheme. The following is an example of how the click fraud is executed.

First, the attacker puts up a website that contains only ads. The attacker then signs up with one or more ad affiliation program such as Google, Ad Sense, or Yahoo. Once arrangements between the ad affiliates and the attacker has been completed, the Bot Master then instructs the botnets under his control to click the ads on his website of ads. This action will trigger payments from online advertisers. Since they are ad affiliates, the payment will be coursed through Google or Yahoo.[21]

Another variation of this same theme is when an owner of a website that has legitimate software on their website contacts the Bot Master and requests the Bot Master to direct the bots to download the advertised software product. Since the software firm will pay the website owner for every downloaded installation of their product, this can result in a large profit to the website owner, especially if the Bot Master has thousands of computers under their control. In this situation, the website owner and the Bot Master both make money from the victimized software provider or firm. The Bot Master becomes a deployment agent or provider. As a deployment provider, the Bot Master can direct the bots to also use malicious software to attack an entity that may be requested by another individual who seeks to take revenge or secure some type of end result that can be accomplished by means of an underground agreement, which results in a "computer hit," an interesting variation of organized crime's "hit man."[22] The Bot Master who serves as a deployment provider can rent their services out to interested customers, and such sites do exist both on the Internet as well as "Deep Web" and "Silk Road."

The use of botnets is not limited to individual attackers since nation-states also envision applications and use for distributed denial-of-service attacks and cyber warfare applications. Other cyber offensive operations can include cyber espionage and cyber attacks against a critical infrastructure of a nation.

1.2.5 TOR and the Deep Web

We began this chapter discussing the historical development of the computer industry and the emergence of the Internet by 1997 after substantial research and investment of the federal government dating back to 1969. In 1996, the government was also funding research throughout the U.S. Naval Research Laboratory, which, by 2003, was released as the TOR ("the onion router") network referred to as the "onion router" due to the layers of encryption, which permitted the emergence of what is now referred to as the Deep Web. The Deep Web had a purpose of permitting law enforcement, military, and governmental organizations to use it for conducting their business in a private fashion or for intelligence and covert operations. Ironically, in 2006, the Deep Web was discovered by cyber-criminals and other actors who were using the Deep Web for illegal purposes such as the sale of drugs, the distribution of child pornography, and a variety of other illegal activities. Both illegal activities and the government covert operations were made possible by the levels of encryption that made it unlikely that the user of the Deep Web would be identified. In terms of the users of the Deep Web, it is instructive to note that there are 800,000 daily TOR users, downloading 30–50 million times a year in which TOR can access more than 6500 hidden websites.[23]

The extraordinary advancements in science and the power of technology and the Internet have enabled societies throughout the world to participate and share in this wealth of discoveries. There is, however, a dark side to the power of technology and the Internet, and this "dark side" appears when individuals choose to use it for criminal purposes such as child pornography, illegal drug sale and purchase, extortion, and other illegal acts. There is also a cost to society in terms of the growing loss of privacy and, perhaps worst of all, the distribution and sale of cyber weapons, which introduces a new scale of terrorism vulnerabilities.

1.3 Vulnerabilities, Risk Assessment, and Risk Management

In view of the increasing number of viruses and attack scenarios, it is incumbent on us to better understand the vulnerability and threat landscape. Risk management processes to protect financial assets, information databases, and intellectual property resources suggest that an active risk assessment process should be established to assist in the identification of how best to deploy security measures. Additionally, there exist a number of strategies for establishing risk mitigation processes as well. Both legal and insurance carriers need to be consulted in the creation of a sound and defensible strategy of both immediate and long-term protection of assets.

1.3.1 Mobile Devices and Smart Phones

The incredible growth of mobile devices has created a landscape vulnerability of immense proportion. The sheer number of these devices, the absence of any meaningful security being operationalized on the devices, and the increasing number of viruses designed for mobile apparatus have been extremely disconcerting. As malware continues to be developed and used in conjunction with botnet attacks, mobile devices are an attractive target for cyber-criminals. The expanding number of corporations and governmental agencies that permit mobile devices to enter their networks as part of a BYOD policy further enhances the vulnerability equation.

The NFC capability of many mobile devices is a vulnerability for both credit card users and merchant's point of sale (POS) terminals because the NFC-embedded chip on a card is in an "always on" state, which means that if a user's card is in the field of an active NFC reader, such as those NFC readers in a POS terminal, the credit card automatically transmits the user's credit card number to the receiving NFC reader. In many smart phones, the software or applications are designed to activate the mobile device's NFC chip to emulate the behavior of a POS terminal's NFC reader. Cyber-criminals

can use a "Bump and Play" tactic where the attacker physically bumps into an unsuspecting user for the purpose of scanning their credit card to collect account numbers.[24]

1.3.2 Web Applications

Another continuing weakness, we must address centers on Web applications where we see the following vulnerabilities:

- Cross-site scripting
- Structured query language (SQL) injection
- Insufficient transport layer protection
- Security misconfiguration
- Broken authentication and session management
- Information leakage
- Improper error handling
- Insecure cryptograph storage

These and other insights are the result of Hewlett Packard's (HP's) review of thousands of assessments to ascertain the status of Web application security, and they concluded that many companies and individuals assume that their websites are of little interest to attackers, but in the experience of HP security teams, this is clearly not accurate, and they go on to state: "In fact, the lack of secure programming and IT security best practices only serve as an enabler for the proliferation of malware."[25] Notably, Internet security threats against websites have increased, and the volume and vector of website attacks in which multiple attack techniques are being employed to disrupt services on websites to compromise data or steal financial resources continue to grow with greater sophistication.

1.3.3 Social Media

Corporations and numerous other nongovernmental organizations have employees who are engaged in the use of social media tools. Governmental agencies, the military, and universities also have people who become actively engaged in the use of social media and can unknowingly create problems for their organization by mistakes that have very rapidly circulated to enormous numbers of people. Sometimes, problems emerge not only from a mistake but also because of calculated plans to either embarrass the organization or create a set of problems that can culminate in the loss of financial resources or respect and integrity to the impacted organization. The range of risk that social media can expose organizations to is now being carefully analyzed by use of risk assessment strategies. Typically, someone will be assigned responsibilities

to develop a risk management program to identify the range of social media risk exposure and to assess the level of the potential risk and its impact on the organization. After determining whether the risk is present and its potential for harming the organization, the risk will have to be mitigated or managed.

The types of social media channels that are being used today have enormous numbers of adherents and followers who utilize the easy-to-use services provided by these social media channels. The channels by themselves are not the problem; it is those who use and take advantage of this social media who create the problems. Currently, the social media channels in use with high subscription numbers are as follows:

- Facebook
- Twitter
- YouTube
- Vimeo
- Flickr
- Picasa
- Foursquare
- Chatter
- Epinions
- LinkedIn

The range of potential risk to organizations as a result of social media channel subscribers either making inadvertent mistakes or making calculated efforts to harm or embarrass others can result in the following:

- Reputational damage
- Release of confidential information
- Loss of intellectual property
- Disclosure of personal information
- Identity theft
- Hijacking another person's identity off a social media channel
- Malware attack
- Reduced employee productivity
- Defamation of character

In an excellent study by the Altimeter Group, they presented a very important risk management process for addressing the issues of social media risk. Their study discussed and outlined the process for identifying risk, assessing the risk, managing the risk, and monitoring risk vulnerabilities in the future. It also illustrated how to create a decision framework and analysis of risks with the pathway for creating a social media team. The need for an organization to establish social media policies and monitor situations that

may necessitate when they update or modify the policies is important and is clearly presented in Altimeter Group's study.[26]

1.3.4 Cloud Computing

The term *Back to the Future* can be applied to the development of cloud computing. Some observers believe that cloud computing evokes a perception of accessing and storing both software and data in the cloud as a representation of the Internet or a network and using associated services. Krutz and Vines suggest that it only represents a modernization of the "time-sharing" model of computing that was the model of computing in the 1960s before the advent of lower-cost computing platforms. The time-sharing model was replaced by a "client-server" model and evolved into the PC, which placed large amounts of computing power at the desktop of the computer user and, in effect, eliminated the time-sharing model of computing. Cloud computing has many of the metered elements of the former time-sharing computing model; however, it also has some challenging new features that many regard as a new future computing model.

Peter Mell and Tim Grance of the National Institute of Standards and Technology define cloud computing as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction."[27]

Krutz and Vines observe that the cloud model is composed of six essential characteristics, three service models, and four deployment models. They identify the essential characteristics of cloud computing as follows:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Measured service
- Rapid elasticity

The service models are described as follows:

SaaS—Cloud software as a service, in which the provider's applications are provided over a network
PaaS—Cloud platform as a service, in which one deploys customer created applications to a cloud
IaaS—Cloud infrastructure as a service, in which one rents processing, storage, network capacity, and other fundamental computing resources

These four deployment models can be either internally or externally implemented as follows:

Private Cloud—enterprise owned or leased
Public Cloud—sold to the public, megascale infrastructure
Hybrid Cloud—composed of two or more clouds
Community Cloud—shared infrastructure for a specific community[28]

The public cloud offers computing services to the general public, accessible via an Internet connection and shared among thousands of customers. Examples of a public cloud would be Amazon Web services, Microsoft Windows, and Rackspace Cloud. On the other hand, private clouds are typically created and hosted by a single organization, usually behind the corporate firewall, and they provide services to employees. Private clouds can also be hosted by third parties, but they remain dedicated to a single customer. Private clouds will cost more than a public cloud, but they offer greater control over the data. The private cloud configuration provides the owner or user full knowledge of the geographic location and, in most cases, the totality of computing resources. The public cloud may well have its geographical location and computing resources anywhere in the world, and the user may not have knowledge of either the location or computing resources unless specified by contractual language.[29]

Security of one's data and intellectual property is a principal concern when entrusting one's data and information to geographically dispersed cloud platforms not under the direct control of your organization. Depending on which cloud model is selected for use, the burden of security may remain with the customer or it could fall on the cloud provider. In any event, carefully prepared contractual language will be necessary to reflect who is responsible for computer security, what level of protection is being provided, and what performance record the cloud provider has against computer security threats. Also, does the cloud provider meet the security standards of confidentiality, integrity and availability, governance, risk management, and compliance?

Despite all the benefits cloud computing provides to its customers and users, it also brings an array of issues that must be addressed around computer security and privacy of information as a result of the size, structure, and geographical dispersion. The potential vulnerabilities are as follows:

- Leakage and unauthorized access of data among virtual machines running on the same server
- Failure of a cloud provider to properly handle and protect sensitive information
- Release of critical and sensitive data to law enforcement and government agencies without the approval or knowledge of the client

- Ability to meet compliance and regulatory requirements
- System crashes and failure that make the cloud service unavailable for extended periods of time
- Hackers breaking into client applications hosted on the cloud and acquiring and distributing sensitive information
- The robustness of the security protections instituted by the cloud provider
- The degree of interoperability available so that a client can easily move applications among different cloud providers and avoid "lock-in provisions"[30]

Cloud computing offers many new opportunities, but it also brings many new disruptive changes to the entire computer industry.

1.3.5 Big Data

The term *big data* actually entails much more than simply the size of data or a database as it encompasses the technologies, hardware, software, and the analytical capabilities to offer judgments and predictions regarding the collection and use of data. Big data and the processes involved address issues such as how one stores data in both its structured and unstructured format and how to process this massive amount of data that is now being created. So the issue becomes one of understanding how and where data are being created and how to store these data since relational database technology cannot absorb and process the unstructured data being generated because these require new database formats. The retrieval of massive amounts of both structured and unstructured data requires computer processing capabilities that are more than a mainframe-based approach, as the requirements for massive data processing require Hadoop cluster computer processing, which is a unified storage and processing environment that is scalable to large and very complex data volumes.

To appreciate the difference between structured and unstructured data, one only has to recall that structured data are data that are contained in spreadsheets or relational databases and adhere to the SQL, which is an international standard for defining and accessing relational databases. This standard provides an accepted process for storing, processing, and accessing data by defining how data will be stored consistently with commonly accepted international standards. On the other hand, unstructured data are data that most will recognize as digital photographs, video, graphical images, sound bites, and any other number of presentations from social media that do not enjoy a common reference point of storage and accessibility based on a common set of standards such as structured data technology. Therefore, unstructured data will require a new format for database processing, as they will not

be accommodated by current relational database technology. This is precisely why the emergence of Hadoop technology is so critical to the processing of what is now being categorized as big data.

Big data is generally viewed by three main categories: its volume, velocity, and variety. In fact, Douglas Laney first articulated these categories for big data, and examples of applications within each category provide insight as to the emerging massive shift that is occurring within the computer industry.

1. Volume: many factors contribute to the increase in data volume. The emergence of a digital environment from the previous analog environment created incredible amounts of unstructured data, basically originating from social media and machine to machine data generated by sensors. To place this into perspective Chris Forsyth, notes the following:

> …A typical passenger jet that generates ten terabytes of information per engine every thirty minutes of a flight, in a single six hour flight from New York to Los Angeles on a twin-engine Boeing 737 the total amount of data generated is a massive 240 terabytes of data. With the total number of commercial flights approaching 30,000 in the U.S. on any given day, a day's worth of sensor data quickly climbs into the petabyte scale. Multiply that by weeks, months, and years and the number is colossal.[31]

> Digital data exist everywhere, especially generated by social media, mobile phones, and networked sensor nodes present in transportation, automobiles, industrial plants, and utility companies using the smart grid. With over 50 million networked sensors in operation and more than 60% of the world's population using mobile phones and interacting with various social media channels, the amount of unstructured data being generated is phenomenal. A recent report by the McKinsey Global Institute states that big data is a growing torrent with over 30 billion pieces of content shared on Facebook every month. Social media sites, smart phones, and other consumer devices including PCs and laptops have allowed billions of individuals around the world to contribute to the amount of big data being produced each day of the year.[32]
>
> Another perspective on understanding unstructured data and their volume being produced can be appreciated by the number of blogs on social networking sites, geo-location devices in use, the bar codes being read by merchants, x-rays, phone conversations, video, text messages, ads, and numerous other methods in which data are being produced, acquired, and stored.[33]

2. Data velocity refers to the unprecedented speed in which machine-to-machine data are created and move between millions of sensors that are contained in a variety of consumer electronics, home appliances, automobiles, public utility equipment such as the smart grid, and other applications. These data are in constant movement and are, in reality, a digital stream of data that have to be both managed and secured. Another example of how a large volume of data moves with a velocity of speed occurs daily within our stock markets and financial institutions, where high-frequency stock trading algorithms reflect market changes and must be captured within microseconds. A recent report by Symantec noted the following:

> …a large credit card company gained a competitive edge with the advanced analytics from Hadoop by reporting they reduced the process time for seventy-three billion transactions amounting to thirty-six terabytes of data, from one month with traditional methods to a mere thirteen minutes.[34]

3. Variety of big data is generated in both formats of structured and unstructured data feeds, so the data are not only just numbers, dates, or strings but also geo-spatial and video must be stored, processed, integrated in both formats, and then analyzed for its best use. Massive databases that may have taken days or hours in the past to complete may now be completed in minutes or seconds.

Big data is really a term that describes a new generation of technologies and architectures that are designed to extract value from very large volumes of a variety of data sources by enabling high-velocity capture, processing, and, ultimately, analysis. The emergence of big data is about more than deploying a new application or software technology such as Hadoop. It really represents a very significant new information technology domain that, over time, will continue to make incredible advancements, which will, in turn, require new system designs and new skill sets of the personnel working within this domain.[35]

In short, big data is ushering in a most transformative range of changes to the computer industry. These changes will be experienced throughout the world in virtually all organizations and will literally impact billions of people.

The Simons Institute for the Theory of Computing at the University of California-Berkeley noted the following with reference to the theoretical foundation of big data analysis:

> The Big Data phenomenon presents opportunities and perils. On the optimistic side of the coin, massive data may amplify the inferential power of algorithms that have been shown to be successful on modest-sized data sets. The

> challenge is to develop the theoretical principles needed to scale inference and learning algorithms to massive, even arbitrary, scale. On the pessimistic side of the coin, massive data may amplify the error rates that are part and parcel of any inferential algorithm. The challenge is to control such errors even in the face of the heterogeneity and uncontrolled sampling processes underlying many massive data sets. Another major issue is that Big Data problems often come with time constraints, where a high-quality answer that is obtained slowly can be less useful than a medium-quality answer that is obtained quickly. Overall we have a problem in which the classical resources of the theory of computation—e.g., time, space and energy—trade off in complex ways with the data resource.[36]

There is another question that demands further research into the big data era and that will focus on research into the security vulnerabilities that massive big data is introducing into our environments. Will it be easier for cyber attackers to design malware and place it into computing systems, since computer security measures will have to respond to big data as a new threat landscape? Also of concern will be the question of privacy. How will big data impact privacy and what research measures will be designed to weigh the benefits and costs of this incredible new system of technologies?

1.4 Emerging Field of Cybersecurity

From the computer's inception, no thought was given to the necessity of creating computer security programs for it. After all, the development of this field was by scientists, engineers, physicists, and mathematicians. Their work was designed to create and usher in new ways to improve the research and scientific communities' trust, and a set of social values and mores were within the very fabric of their cumulative work. It never occurred to them that one day, people would be inclined to abuse their discoveries or to even use them for immoral, illegal, or criminal purposes. The challenges were never anticipated; consequently, computer security was not built into these technologies. However, after the late 1980s, it was apparent to some that computers would need to have security capabilities. Interestingly, the security on most devices was placed in a default mode, and when it became more apparent that security was necessary for this field, changes in hardware have slowly evolved. Hardware was not the sole security vulnerability, as the software also had security problems. Eventually, encryption emerged as a technique that could protect information data stored within our databases.

Because there emerged viruses, worms, and malware, an industry was created to provide software solutions to protect computer users from these viruses and malware. As the virus and malware designers became more

sophisticated in products they were making, the industry has always been in a position of reaction and trying to catch up with the malware designs. The irony is centered on how little it costs to design a virus and how incredibly expensive it is to develop antivirus tools to protect against these viruses.

In addition to an industry committed to creating antivirus tools, we have also witnessed the emergence of major corporations developing both computer security functions as well as computer forensic investigation teams. Since computer fraud, abuse, and theft of intellectual property have now reached a level capable of destroying entire companies, there is a national interest in protecting our information assets.

Since 1984, the federal government has been encouraging industries and our corporations to address the issue of securing their assets, data, and intellectual property. The corporate sector has historically pushed back from these government recommendations and urging because they viewed information systems as cost centers, and since American corporation's executives focused more on quarterly profit and loss statements, they were more interested in profit centers not, cost centers. Another area of corporate push back emerged over the concern of the Freedom of Information Act and also the costs involved in litigation.

After 9/11, many American corporations began to take the security of their data more seriously, and slowly, some movement has been made to offer additional security of their information assets and intellectual property. The wholesale loss of incredible amounts of intellectual property attributed to both Chinese and Russian entities has finally alerted our corporate community. Presidents Clinton, George W. Bush, and Obama have consecutively and consistently called on our corporate community to increase their computer and information security, and we are now seeing action to effect some improvements in these areas.

1.4.1 Framework for Improving Critical Infrastructure Cybersecurity

On February 12, 2014, the National Institute of Standards and Technology issued a report to guide our nation in improving our critical infrastructures. This report was issued as a result of President Obama's Executive Order 13636 regarding efforts to improve our nation's critical infrastructure cybersecurity. Because the national and economic security of the United States depends on the reliable functioning of our critical infrastructure, and since cybersecurity threats exploit the increased complexity and connectivity of our critical infrastructure systems, placing our nation's security, economy, public safety, and health at risk, the Executive Order created a new cybersecurity framework. This framework enables organizations, regardless of size

or degree of cybersecurity risk, to apply the following framework core elements, which consist of functions that are envisioned as outcomes:

- Identify
- Protect
- Detect
- Respond
- Recover

These five functions are designed to organize basic cybersecurity activities at their most critical levels. A structure is provided that both advises and guides the management of risk while providing an assessment strategy to address and manage cybersecurity threats and incidents.[37] In short, it is hoped that the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity will become a standard across all major industries and corporations to improve their cybersecurity.

1.4.2 Risk and Threat Assessment

The U.S. Department of Homeland Security has adopted the Threat Agent Risk Assessment methodology as designed by the Intel Corporation. Intel's predictive methodology establishes priorities on areas of concern and then targets the most critical exposure to identify and manage the information security risk. As part of the prediction capability, Intel developed a standardized Threat Agent Library that is used to identify the most likely attack vectors. Thus, their Threat Agent Risk Assessment is used to measure current threat risks. Their methodology then quantifies those threat agents that exceed baseline acceptable risks. An analysis is made of the attacker's objectives and then what attack methods might be anticipated. By preestablishing the known areas of exposure, this process then allows the alignment of a strategy to target the most significant exposures and to apply controls in a direct fashion, not simply across the range of all weak points.[38]

1.5 Summary

The challenge confronting professionals in their effort to improve the state of our cybersecurity is an enormous responsibility, and significant research must be performed to move these efforts forward. Clearly, the early industry solutions to computer security problems were not solved by firewalls, virus scans, authentication credentials, intrusion detection programs, encryption, and cryptography. As impressive as these programs and efforts have been, much more remains to be done to offer greater security

to the vast number of people who rely on the tools and technologies of our computer industry. From an historical reference point, one can see how the technology of the computer industry has increased in such exponential terms. This has resulted in major improvements to our society and to the health and welfare of so many citizens. At the same time, we can also observe the very sophisticated viruses, malware, and attacks that have occurred on our cyber systems. We must continue to focus our efforts to improve our research and development role in addressing these new and emerging challenges.

Notes and References

1. Hicks Jr., *Information Systems in Business: An Introduction*, Second Edition, @ 1990 South-Western, a part of Cengage Learning Inc. Reproduced by permission. http://www.cengage.com/permissions, 433.
2. Ibid., 434–435.
3. Ibid., 435–436.
4. Ibid., 437.
5. Ibid., 438–439.
6. Ibid., 439–440.
7. Ibid., 447–448.
8. Denning and Denning, *Internet Besieged: Countering Cyberspace Scofflaws*, 15–16.
9. Ibid., 16–17.
10. Ibid., 18–19.
11. Loc. Cit.
12. Cole, Krutz and Conley, *Network Security Bible*, 146.
13. Spafford, "Computer Viruses," in D. Denning and P Denning, *Internet Besieged: Countering Cyberspace Scofflaws*, 74.
14. Ibid., 76.
15. Cole, Krutz and Conley, Ibid., 147.
16. Fadia, *Unofficial Guide to Ethical Hacking*, 434.
17. Loc. Cit.
18. Piper, "Definitive Guide to Next Generation Threat Protection: Winning the War Against the New Breed of Cyber-Attacks," 20.
19. "Symantec's Cyber-Attack Tool Kits Dominate Threat Landscape," 1–3.
20. Elisan, *Malware, Rootkits and Botnets: A Beginner's Guide*, 56–59.
21. Ibid., 66.
22. Ibid., 68.
23. Grossman and Newton-Small, "The Deep Web," in *Time: The Secret Web, Where Drugs, Porn and Murder Hide Online*, 28–31.
24. Hewlett Packard, "White Paper: HP 2012 Cyber Risk Report," 19–20.
25. Ibid., 2–6, 22.
26. Webber, Li and Szymanski, "Guarding the Social Gates: The Imperative for Social Media Risk Management," 4–7, 12–14.
27. Krutz and Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, 2.
28. Loc. Cit.

29. Grimes, "Staying Secure in the Cloud," in *Cloud Security: A New Model for the Cloud Era*, 2.
30. Krutz and Vines, op. cit., xxiii–xxiv.
31. Forsyth and Chitor, "For Big Data Analytics There's No Such Thing as Too Big: The Compelling Economics and Technology of Big Data Computing," 19.
32. Manyika, Chui and Brown et al., "Big Data: The Next Frontier for Innovation, Competition and Productivity," 1–2.
33. Forsyth and Chitor, op. cit., 5.
34. Symantec, "Better Backup for Big Data," 1.
35. Borovick and Villars, "The Critical Role of the Network in Big Data Applications," 1–2.
36. Simons Institute for the Theory of Computing, "Theoretical Foundations of Big Data Analysis," 1.
37. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 7–9.
38. Rosenquist, "Prioritizing Information Security Risks with Threat Agent Risk Assessment," 1–5.

Bibliography

Borovick, L., and Villars, R. "The Critical Role of the Network in Big Data Applications." White Paper IDC Analyze the Future. Massachusetts: International Data Corporation, February 2012.

Cole, E., Krutz, R., and Conley, J. W. *Network Security Bible*. Indiana: Wiley Publishing, Inc., 2005.

Denning, D. E., and Denning, P. J. *Internet Besieged: Countering Cyberspace Scofflaws*. New York: Addison-Wesley, ACM Press, 1998.

Elisan, C. C. *Malware, Rootkits and Botnets: A Beginners Guide*. New York: McGraw Hill, 2013.

Fadia, A. *Unofficial Guide to Ethical Hacking*. MacMillan India, Ltd.: Premier Press, 2001.

Forsyth, C., and Chitor, R. "For Big Data Analytics There's No Such Thing as Too Big: The Competing Economics and Technology of Big Data Computing." White Paper. San Jose, CA: Forsyth Communications, March 2012.

Grimes, R. "Staying Secure in the Cloud." In *Cloud Security: A New Model for the Cloud Era*. San Francisco: InfoWorld Deep Dive Series, 2013.

Grossman, L., and Newton-Small, J. "The Deep Web." In *Time: The Secret Web, Where Drugs, Porn and Murder Hide Online*, November 11, 2013.

Hewlett Packard, "White Paper: HP 2012 Cyber Risk Report." Contributors: Haddix, J., Hein, B., Hill, P., Hils, A., Jaydale, P., Lancaster, J., Muthurajan, S. S., Painter, M., Pril, J., Sechman, J., Strecker, R., and Timpe, J., Informationweek.com; UBM Tech: San Francisco, 2013.

Hicks, J. O., Jr. *Information Systems in Business: An Introduction*, Second Edition. South-Western, a part of Cengage Learning Inc., Farmington Hills, MI, 1990. Reproduced by permission. Available at http://www.cengage.com/permissions.

Krutz, R. L., and Vines, R. D. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Indiana: Wiley Publishing Company, 2010.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A. H. "Big Data: The New Frontier for Innovation, Competition and Productivity." New York: McKinsey Global Institute, May 2011.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." Washington, DC: US Government Printing Office, February 12, 2014.

Piper, S. "Definitive Guide to Next Generation Threat Protection: Winning the War Against the New Breed of Cyber-Attacks." Maryland: Cyberedge Group, LLC, 2013.

Rosenquist, M. "Prioritizing Information Security Risks with Threat Agent Risk Assessment." IT@Intel, White Paper. Santa Clara, CA: Intel Corporation, December 2009.

Security Technology and Response Organization. "Symantec's Cyber-Attack Tool Kits Dominate Threat Landscape." California: Symantec Corporation, 2011.

Simons Institute for the Theory of Computing. "Theoretical Foundations of Big Data Analysis." Berkeley, CA: University of California–Berkeley, December 2013.

Spafford, E. H. "Computer Viruses," in Denning, D. E., and Denning, P. J. eds., *Internet Besieged: Countering Cyberspace Scofflaws*. New York: Addison-Wesley, ACM Press, 1998.

Symantec. "Better Backup for Big Data." California: Symantec World Headquarters, 2012.

Webber, A., Li, C., and Szymanski, J. "Guarding the Social Gates: The Imperative for Social Media Risk Management." California: Altimeter Group, 2012.