An Engineer's Primer on Information Security

A White Paper by:

Brent Scott LaReau,
Consultant
www.designsbylareau.com

Revised: September 8, 2006

Copyright ©2006 by Brent Scott LaReau

This document and its content is protected by copyright, regardless of how this document or its content is printed, viewed, encoded, stored or transmitted. Permission to paraphrase, reproduce or copy any part, or all, of this document or its content is granted only if:

1. The reproduction or copy is not achieved for profit without this author's express consent, and...
2. Sufficient information is included to identify this document and its author. Specifically:
   - The full title of this document plus its copyright date(s), and...
   - This author's full name (Brent Scott LaReau) and his brief or complete contact information.

Brent Scott LaReau, *Consultant*
Voice/FAX (U.S.A.): 847-428-4923
E-mail: B.LaReau@DesignsByLaReau.com
Web: www.DesignsByLaReau.com
Mail (U.S.A.): 2413 W. Algonquin Road, PMB #258
Algonquin, IL 60102-9776

Disclaimer

Information in this document is subject to change without notice and is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, its author shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this document.

Trademark Information

Trademarked names may appear in this document. Rather than use a trademark symbol with every occurrence of a trademarked name, such names are used in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

About the Author

Brent Scott LaReau has been an independent consultant since 1987.

He provides design and development services in electronics, software, embedded systems and devices, web and intranet sites, knowledge base construction, technical writing and on-site training/mentoring. He is proficient in heterogeneous system design, where diverse components use different programming languages, interfaces, databases, networks and communications protocols.

Brent earned his BSEE at Marquette University, graduating first in his class. His academic awards include the International Engineering Consortium's (IEC's) *William L. Everitt Award*, Marquette University's *Top Scholars in Curriculum Award*, and the College of Lake County's *Outstanding Academic Excellence in Mathematics* and *Outstanding Scholar Award*.

He is a member of the Institute of Electrical and Electronics Engineers (IEEE), the Association of Computing Machinery (ACM), and American Mensa, Ltd.

Contents

Part 1

Introduction and Overview

Corporations, engineers and nontechnical people alike rely on globally available digital information having a definite dollar value. This has spurred **cybercriminals**[1] to use computers and software to steal personal identities, hold enterprise databases for ransom, and commit other information-related crimes.

In the U.S. alone, cybercrime costs companies roughly $67 billion per year, and costs individuals an extra $40 billion. On average, each U.S. wage earner 21 to 65 years old pays cybercriminals about $1500 each year, directly or indirectly.

Today, cybercriminals use **malware** such as **viruses**, **worms** and **spyware**, as well as **social engineering** (psychological) techniques, to achieve their goals worldwide. Their primary vector is the Internet. **Anti-virus** software is becoming irrelevant, as new types of attacks occur long before anti-virus companies can issue updates.

Even without falling prey to cybercriminals, companies and individuals can accidentally allow important information to fall into the wrong hands. Consequences of such **data leaks** include embarrassment, termination, blackmail, lawsuits or even financial ruin. Simply e-mailing a spreadsheet to a customer, or failing to erase a discarded hard drive, or using a wireless computer at a coffee shop, can provide someone with enough confidential data to bring down you or your company.

For example, in 2004 The SCO Group submitted a Microsoft Word document as part of a lawsuit against DaimlerChrysler and AutoZone. An analysis of that document's hidden "**meta-data**" revealed that SCO's lawyers had originally planned to target Bank of America instead. This data leak seriously weakened SCO's legal position.

[1] Most **boldfaced** words can be found in the Glossary located near the end of this White Paper.

Finally, engineers know that a company's *end products* can contain computers, custom software and site-specific data. In a classic case of "finger-pointing", customers will assume that vendors "lock down" their products and that data is backed up automatically, while vendors will assume that customers will somehow perform these tasks themselves. Legal trends indicate that vendors, and eventually engineers themselves, may soon be liable for security breaches or enterprise-crippling data loss at customer sites.

This White Paper introduces the field of **information security**—sometimes abbreviated **InfoSec**—which deals with the protection of critical data and the digital information systems that store such data. Also introduced are "best practices" in information security, which are tried-and-true security-related guidelines for designing, implementing and maintaining any kind of information system.

On a more detailed and practical level, this White Paper brings into focus security and privacy issues affecting individuals and corporations. It describes common attacks and their defenses; data leaks and their prevention; effective individual and corporate policies; and technological solutions and their shortcomings. A glossary and a list of references are included.

As you read this White Paper, remember—

Praemonitus, praemunitus
(Forewarned is forearmed)

Part 2

Introduction to Information Security

Billy Blanks, creator of the Tae Bo physical fitness method, said that once you have consumed calories you only have two choices: burn them off, or wear them. In the same vein, once you have stored information you only have two choices: protect it, or lose it.

2.1 Information? Security?

What types of information do you—or your company—rely on every day?

- Bids and contracts?
- Documents and specifications?
- Schematics, bills of materials and CAD drawings?
- Software and databases?
- Financial data?
- Addresses and phone numbers?
- Bank accounts?
- E-mail archives?
- Passwords?

What would happen if such information was lost, stolen, corrupted, sold, fell into your competitor's hands, held for ransom, or put on public display?

All right, then! Let's talk about preventing those things from happening.

2.2 Overview

In the past two decades we have increasingly used digital information systems to store all kinds of data: desktop computers, laptop computers, cell phones, PDAs, MP3 players, web servers, e-mail servers, file servers, USB memory sticks, CDROMs, DVDs, floppy disks, tape cartridges, hard drives, network storage devices and other devices.

Most people use these devices *without blinking*, as if all of these devices cannot corrupt or lose data, and will last forever, and cannot be lost or stolen, and can resist any stranger's attempts to copy stored data, and can be replaced at any time with another device that will somehow store the same data automatically.

Fortunately, a few people *did* blink, and consequently tried to minimize those problems by inventing a new methodology.

The field of **information security** (**InfoSec**) deals with the protection of information systems and the information stored in such systems. It applies equally well to personal electronic devices, file cabinets, computer centers, web sites, and the home or automobile.

2.3 Definition

The U.S. National Information Systems Security Glossary defines **information security** as: "*The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats*" [14][1]

[1] Numbers inside square brackets denote one or more cited references, which can be found at the end of this White Paper.

2.4 Objectives

Widely accepted objectives of information security [14] include:

- **Assurance** - Confidence that security measures work as intended to protect an information system. Vulnerability assessments and testing must be performed to establish a confidence level.
- **Availability** - Information systems should not break down when attacked. This requires knowledge of how attacks are performed.
- **Confidentiality** - Information should be accessible only to authorized parties. Generally, this requires access controls and **encryption** (see section 7.1.9).
- **Integrity** - Confidence that data was not altered by unauthorized parties, or was not lost due to equipment malfunction. Tools such as checksum generators can be used to verify data integrity.
- **Accountability** - Responsibility and liability issues regarding information systems. Impetus must come from effective management and legal council.

2.5 Security Considerations

Five main security considerations exist [14], corresponding to information security objectives mentioned in section 2.4:

- Vulnerability assessments and testing.
- Education on attack methodology.
- Encryption and access controls.
- Data integrity checks and alarms.
- Responsibility and liability policies.

2.6 Risk Management

It is important to realize that information security is not about establishing absolute protection for important information, which is impossible. Instead, information security is about **risk management**, which is the ongoing process of identifying risks and implementing mitigation plans to address them.

Risks can be managed only if they are known [15, 26]. A discovery process is necessary to identify information-related risks. Following established guidelines is better than going it alone, for two reasons. First, a lot of time can be saved by following in someone else's footsteps. Second, litigation often focuses on whether industry "best practices" were used, as mentioned in Part 3 .

2.7 Scope

Information security considerations are commonly, but incorrectly, thought to apply only to digital data stored on servers located behind corporate **firewalls**. In fact, information security considerations apply to *every* piece of information, regardless of encoding, storage media or physical form.

For example, hardcopy of your company's internal e-mail directory should not become publicly available through theft or carelessness. Confidential information stored in a PDA should not be readable by a thief who steals that PDA.

While it is obvious that enterprise information systems must be protected from unauthorized access, it is less obvious that a company's for-sale digital products are also information systems, which customers will rely on to securely store and process their personal or enterprise data. Legal trends show that vendors who do not employ information security "best practices" may one day be liable for security breaches suffered by their customers [11].

2.8 Security Technology

Information security certainly involves the use of hardware and software technology to establish safeguards for information:

- **Encryption** (see section 7.1.9).
- Integrity checkers.
- Locks and other access controls.
- Alarm systems.

- Vulnerability analyzers.
- Network **firewalls**.
- Intrusion detection systems.

2.9 Security Policies

Technology alone is insufficient to protect information systems. Policies for human behavior must also be established to protect critical information [28], as exemplified by the old military slogan, "Loose Lips Sink Ships".

Security policies, which guide human behavior, will become ever more important as cybercriminals increasingly use **social engineering** techniques to bypass technological protection methods (see section 5.7.10).

Policies also help us to prevent accidental **data leaks** that could bring harm to ourselves, our companies or employers, or our customers, as discussed in Part 7.

Finally, policies can define an "incident response" strategy, which is essential for any organization that depends on an information system for day-to-day business activities. Incident response strategies should encompass preparation, identification, containment, eradication, recovery and follow-up phases.

2.10 Laws and Regulations

An increasing number of Federal and state laws and regulations affect how enterprise information security must be managed on a day-to-day basis, as well as how security breaches must be dealt with. Initially, laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) were enacted to protect consumers, and others such as Sarbanes-Oxley Act were created to protect investors.

Currently there are no laws dictating how enterprise information security must be managed. However, information security-specific legislation is expected at any moment, with the Department of Homeland Security's National Strategy for Securing Cyberspace acting as a springboard.

2.11 Security Standards

In the absence of laws we can rely upon numerous industry standards to guide us. Popular standards and industry "best practices" published by various organizations are shown in Part 3.

2.12 Implementation

Establishing a formal information security methodology can require a great deal of time, labor and/or expense.

At the corporate level, this requires many departments to work together. Specialists may be hired on a full-time or consulting basis, to oversee the design, implementation, management and auditing of the corporation's top-to-bottom information security strategies. Such personnel will undoubtedly use industry "best practices" recommended by various organizations (such as those shown in Part 3). But be careful when hiring an outsider to perform security audits and vulnerability assessments, for who watches the watchmen?

In contrast to an elaborate and time-consuming formal methodology, this White Paper condenses "best practices" mentioned in Part 3 to create a simple, "hands-on" approach that both individuals and corporations can immediately employ on a day-to-day basis.

The remainder of this document will cover topics related to information security considerations mentioned in section 2.5. Topics include:

- Best practices.
- **Cybercriminals** and their **attack vehicles**.
- Internet and network threats.
- Non-technological threats.
- **Data leaks**, data loss and privacy.

Part 3

Best Practices

Industry standard "best practices" are commonly used during design, development and implementation activities of all kinds. Information security activities involve the same types of tasks, and therefore benefit from the use of best practices as well. There is no reason to "reinvent the wheel".

According to one study, organizations that employed best practices enjoyed greater success in their information security efforts than those that did not do so [35]. In specific, organizations that employed best practices saw a decrease in:

- Exploitation of operating system vulnerabilities.
- Network security incidents.
- Customer/employee records being compromised.
- Alteration of system and application files.
- E-mail system downtime.
- Downtime due to security breaches.
- Financial loss due to security incidents.

Also, litigation often focuses on "due diligence" and whether best practices were used during product (or infrastructure) design and development activities. This is true regardless of whether a lawsuit involves a vendor, a customer, a competitor, an employee or former employee, or a "**script kiddie**" who launched a "**denial of service**" attack on your web site.

The following organizations publish industry "best practices" guidelines for dealing with information security issues:

- **Information Security Forum (ISF)**: A leading independent and international authority on information security, with members in 50% of Fortune 100 companies. The ISF aims to deliver practical guidance and solutions to overcome today's wide-ranging security challenges. Best practices are defined in their massive 247-page document, *The Standard of Good Practice for Information Security*. URL: http://www.securityforum.org

  The Standard of Good Practice for Information Security covers:

  1. Enterprise-wide security management.
  2. Critical business applications.
  3. Computer installations.
  4. Networks.
  5. Systems development.

- **International Organization for Standardization** (ISO) and **International Electrotechnical Commission** (IEC): ISO is an international standard-setting body composed of representatives from national standards bodies. Similarly, IEC is an international standards organization dealing with electrical, electronic and related technologies. ISO and IEC often jointly publish standards documents. ISO/IEC 17799 contains guidelines for best practices in information security. URLs: http://www.iso.org *and* http://www.iec.ch

  ISO/IEC 17799 deals with:

  1. Security policy.
  2. Organization of information security.
  3. Asset Management.
  4. Human resources security.
  5. Physical and environmental security.
  6. Communications/operations management.
  7. Access control.
  8. Acquisition, development and maintenance.
  9. Information security incident management.

10. Business continuity management.
11. Compliance.

- The **Computer Security Division** (CSD) is one of eight divisions within the **Information Technology Laboratory** of the **National Institute of Standards and Technology** (NIST). CSD acts to improve information systems security by raising awareness, devising techniques, and developing standards and validation programs. CSD publishes many general and specific documents relating to information security. For example, its "800 series" of Special Publications deals specifically with security guidelines. URL: http://csrc.nist.gov

  Noteworthy documents published by NIST and its divisions include:

  Special Publication 800-30: Risk Management Guide for Information Technology Systems. Topics include:

  1. Risk management overview.
  2. Risk assessment.
  3. Risk Mitigation.
  4. Evaluation and assessment.

  NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems. This covers:

  1. Management controls.
  2. Operational controls.
  3. Technical controls.

  Engineering Principles for Information Technology Security (A Baseline for Achieving Security). This deals with:

  1. Security foundation.
  2. Risk.
  3. Ease of use.
  4. Resilience.
  5. Vulnerabilities.
  6. Networking.

- The **SANS Institute** was established in 1989 as a cooperative research and education organization. SANS (an acronym for **S**ysadmin, **A**udit, **N**etwork, **S**ecurity) is now a widely-trusted worldwide source for information security training and certification. It maintains more than 1,200 freely available, original papers on various aspects of information security, and it operates the Internet's early warning system: the Internet Storm Center. SANS also publishes its own news digest (NewsBites), a vulnerability digest (@RISK), and flash security alerts. URL: http://sans.org

  Noteworthy documents published by SANS include:

  Information Technology System Security Plan - Development Assistance Guide (http://sans.org/projects/systemsecurity.php). This covers:

  1. System identification.
  2. Management controls.
  3. Operational controls.
  4. Technical controls.

  Information Security Management - SANS Audit Check List. This summarizes the same 11 subjects as the ISO/IEC 17799 specification (see previous).

- **Information Systems Audit and Control Association** (ISACA) and **IT Governance Institute** (ITGI): ISACA is a global organization for information governance, control, security and audit professionals. ITGI is a research think tank that exists to be the leading reference on IT-enabled business systems governance for the global business community. Jointly they publish *Control Objectives for Information and Related Technology* (COBIT), which is a set of best practices for information management. URLs: http://www.isaca.org *and* http://www.itgi.org

- The **CERT Coordination Center** of Carnegie Mellon University's Software Engineering Institute studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to help improve security. They created the OCTAVE (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) method for defining essential components of a security risk evaluation. Using the OCTAVE Method, executives and IT departments can work together to make information-protection decisions and address information security needs. URL: http://www.cert.org

Part 4

Cybercriminals and Their Attack Vehicles

For thousands of years, security threats consisted of physical attacks such as break-ins and hold-ups. The nearly sequential births of computer science and the Internet have forever changed the way criminals—such as thieves, con artists and corporate spies—commit their crimes.

4.1 Cybercrime

For thousands of years people have sought to obtain physical goods such as food, weapons, jewelry, or more recently, automobiles. But in recent decades there has been an explosion of globally available digital information that is increasingly seen to have a definite dollar value.

Hence today, people will pay good money for information, whether such was obtained legally or not. Worse, companies themselves are now starting to buy stolen enterprise information from **corporate spies** [39], and to hire **script kiddies** [13] to attack another company's web site [22], to gain a competitive edge.

This new demand for information has spawned **cybercriminals**, who are commonly but incorrectly known as **hackers**. True hackers have a passion for learning a technology so that they can innovate, regardless of whether they gain financially or not. Cybercriminals have a passion only for achieving illegal financial gain by learning a technology well enough to exploit it.

While hackers may be a nuisance, cybercrime is a severe and costly problem. The US Treasury Department's Office of Technical Assistance estimated that cybercriminals reaped $105 billion in 2004—more than illegal drug sales provided! [18]

After gaining access to a computer, cybercriminals will steal copies of saleable information, or will use a type of **malware** called **ransomware** to take enterprise information hostage [18], or will destroy or corrupt data as an act of sabotage or revenge, or will drain funds from bank accounts.

The Federal Bureau of Investigation (FBI) has reported that cybercriminals have attacked almost every Fortune 500 company at some time [12].

Recently, cybercriminals are finding it more profitable—and less risky—to sell their malware to other cybercriminals, instead of directly mounting an attack themselves.

Cybercriminals are not always shadowy outsiders who do their dirty work from afar. Indeed, roughly half of cybercriminals are (or were) employees of the very firms from which they steal [1]. Such "inside jobs" cost U.S. business $400 billion per year, according to the Association of Certified Fraud Examiners. Of that, $348 billion can be tied directly to employees who had been assigned higher-than-average computer access privileges [18].

On a more personal level, cybercriminals sell stolen information such as credit card numbers to unscrupulous individuals who intend to use this information for personal gain. According to a Federal Trade Survey, around 9.9 million Americans were victims of **identity theft** in 2003. In 2005 at least 55 million Americans were exposed to potential identity theft [7], and losses due to Internet fraud in the first four months of 2005 alone totalled $1.5 billion ($800 million more than for all of 2004).

A less-personal but more widespread form of criminal activity is the production of ordinary malware such as viruses, worms and spyware, which routinely cripple enterprise information systems, computer-based products, and personal computers alike, forcing victims to repeatedly perform costly mitigation activities.

4.2 Malware

Cybercriminals often use malicious software (**malware**) as attack vehicles to break into, or cripple, computers and other types of information systems [2, 3]. Today, malware is spread almost entirely through computer networks, both private and Internet. Therefore, **network security**—a subset of information security—is becoming ever more important.

How widespread is the malware problem? In June 2006, security firm Sophos identified more than 180,000 different types of malware traversing the Internet, which is 40,000 more than was found in June 2005 [10].

Microsoft's Malicious Software Removal Tool, which is distributed by Microsoft as part of its critical updates each month, removed more than 16 million pieces of malware from 5.7 million Windows computers during the 15 months prior to June, 2006 [8]. About 3.5 million of those Windows computers also had at least one "*backdoor Trojan*" installed—usually of the "*botnet*" variety—placing such computers under cybercriminals' direct control.

Common types of malware include **worms**, **viruses**, **spyware**, **adware**, **ransomware**, **rootkits** and **Trojans**.

Malware has two basic attributes: self-replication ability, and primary vector type. *Self-replication* is the ability of software to make copies of itself; software can either self-replicate or it can't. A *vector* is the delivery medium used to carry software to its destination; software can be carried by physical media such as disks, or it can be transmitted over a network such as the Internet [4].

Typical attributes of common malware are shown in table 4.1.

Table 4.1: **Malware Attributes**

Self-replicating	Primary Vector	Common Malware
No	Physical media	Spyware, adware, Trojans and rootkits
No	Network	Rootkits, spyware, adware and Trojans
Yes	Physical media	Viruses
Yes	Network	Worms

4.2.1 Worms

A **worm** is self-replicating software that can automatically find and penetrate remote computers or information systems on a network, by exploiting a vulnerability known to exist in application software running on those targets. Once penetration is accomplished, a worm will permanently install itself in its victim and then immediately seek other victim computers on the network.

Additionally, modern worms contain a payload designed to allow cybercriminals to profit from the worm's presence inside a computer. For example, a worm may turn infected computers into **zombies** as described in section 4.4.

Worms do not need human help to infect a vulnerable device. They simply need a network connection to that device. Hence, simply unplugging or disabling a device's network and Internet connections (creating an **air gap**) would absolutely prevent worms from ever infecting that device. Obviously, that would reduce a device's usefulness in today's networked environment.

Worms replicate and propagate extremely quickly. In 2003, the Slammer worm infected every vulnerable computer in the world within 15 minutes of being released [33].

You should be aware that in 2005-2006 cybercriminals began to create proof-of-concept worms designed to find and infect Bluetooth-enabled cell phones that use Symbian's embedded operating system. **Bluetooth** is a form of wireless network used by mobile devices such as cell phones and PDAs. Future Bluetooth worms could infect quite a few types of mobile devices, including automobiles.

4.2.2 Viruses

A **virus** is self-replicating software that, when activated, is able to attach copies of itself to other compatible files that are found within reach. A virus becomes

active and replicates itself only when its host file is executed (opened). Hence viruses most often replicate only with human help. A virus can replicate without human help only if someone has set up a means for a computer to automatically execute (open) an infected file, possibly by using a scheduler program.

Aside from self-replication, a virus can be manually replicated by simply making a copy of its host file. This can even happen during routine backups, where infected files are copied from one computer to another. However, copies are in fact dormant and benign unless executed (opened).

While the primary purpose of a virus is to replicate itself, some viruses carry a payload designed to cause damage by deleting or corrupting files. A large number of viruses carry a payload that is simply annoying. For example, some viruses display an egotistical or political message of some kind.

Viruses were once the most important and extensive type of malware, but worms now have that title because worms are much faster and more effective.

4.2.3 Spyware

Spyware is surveillance software that gains entry to a computer only with human help. Once entry is gained, spyware will permanently install itself in its new host, often not only hiding itself but also rigging the computer to automatically re-install itself should someone remove it. Once installed, spyware will automatically start running every day as soon as your computer is powered up.

Spyware has only one purpose: to collect specific information about you, and then transmit that information to someone who can profit from that information. For example, in 2005 researchers found evidence of a massive spyware-base **identity theft** ring that used **keystroke loggers** to obtain personal information [37].

Collected information can include anything stored on your hard drive, anything you type on your keyboard, and anything you view on web pages:

- Your contact information (name, address, phone number, etc.).
- Your demographic information (age, sex, race, sexual preference, city, state, income, etc.).
- Information about your buying habits.
- Your passwords and account numbers.
- Your bank accounts and balances.
- Your credit card numbers and expiration dates.
- Addresses of web sites you visit.
- Your search engine queries.

Common sources of spyware are spam e-mail attachments, disreputable or hacked-into web sites, disreputable application software, free games, and third-party screensavers.

Spyware can enter a computer only when someone opens infected e-mail attachments, visits infected web sites, installs infected application software, or installs infected screensavers. Otherwise spyware would never enter your computer.

The National Cyber Security Alliance reported that 91% of computers in a studied group had been infected by spyware. Webroot Software (in association with Internet service provider EarthLink) scanned more than one million Internet-connected computers and found an average of 28 spyware programs on each computer [18]. Some people actually have *many hundreds* of spyware programs on their computer.

4.2.4 Adware

Adware is closely related to **spyware** in terms of its source, technical characteristics, and operation. But whereas spyware informs someone else about you, adware is designed to inform you about products or services offered by someone else.

A computer infected by adware may:

- Display "pop-up" advertisements for products, services or pornography.
- Hijack your web browser so that you will be exposed to specific online shopping sites.
- Notify disreputable companies of your e-mail address so that they can send you unsolicited mail (spam) containing all types of offers.
- Attempt to influence your political position.

4.2.5 Ransomware

First seen in 2006, **ransomware** is designed to take a victim's data hostage by **encrypting** one or more specific types of data files stored on a victim's computer. After this is accomplished a ransom demand will be made known to the victim.

Money is usually demanded in exchange for a decryption key with which to restore the victim's data. Small-time ransomware demands as little as $10.99 or as much as a few hundred dollars per computer—payable through PayPal or Western Union—which increases the likelihood that someone will pay the ransom [18]. Big-time ransomware can immobilize enterprise databases until tens (or hundreds) of thousands of dollars are paid.

An interesting aspect of ransomware is that it can't propagate by itself. It must be carried as a payload by an attack vehicle such as a virus or worm.

4.2.6 Trojans

A **Trojan** is an appealing or seemingly useful software program, usually free, that actually contains some type of malware.

A Trojan cannot infect a computer unless someone deliberately obtains and installs such software. Hence, a Trojan is a clever way to entice victims to voluntarily install malware on their computer.

Trojan programs usually fall into the following categories:

- Games and related programs.
- Screensavers.
- Anti-virus or anti-spyware programs (ironically).
- Pirated software ("warez").
- Trendy software for children and teens.

4.2.7 Rootkits

A **rootkit** is software that hides itself in a computer, obtains administrative privileges and then replaces some normal operating system functions with its own [32]. Rootkits are undetectable by many experts and usually cannot be removed without destroying the operating system's capability to function normally.

Traditionally, rootkits have been used by cybercriminals to gain unrestricted "super-user" access to remote computers. But recently, some companies like Sony have begun to use rootkit technology for Digital Rights Management purposes to control access to digital data such as software, music and movies.

4.3 Zero-day Exploits

In 1995, new malware spread so slowly that software companies and anti-virus vendors had sufficient time to roll out patches and anti-virus updates before that new malware got out of control.

Ten years later it took mere *hours* for cybercriminals to roll out malware that took advantage of the newly discovered Windows Metafile vulnerability, but it took Microsoft *nine days* to release a patch to fix that vulnerability [18]. As mentioned in section 4.2.1, malware can infect every vulnerable computer in the world within minutes of being released. As a result, those cybercriminals were able to wreak havoc around the globe for the entire nine day time period.

The immediate exploitation of the Windows Metafile vulnerability was a prime example of a **zero-day exploit**. Unfortunately, zero-day exploits are becoming more common as time goes by.

4.4 Zombies and Botnets

A **zombie** is an Internet-connected computer that was successfully attacked in a manner designed to place it under the remote control of a cybercriminal. Such attacks are usually performed automatically by worms carrying a specific type of payload, although a cybercriminal may choose to accomplish that deed manually. Owners of zombies are usually unaware that their computers were compromised.

A single worm can quickly turn a large number of computers into zombies. This will form a **botnet**, which is a special-purpose distributed computing farm with a very high-bandwidth connection to the Internet.

Today, most cybercriminals do not personally use the botnets they create. Instead, they find it much more profitable to sell or rent their botnets to other cybercriminals who don't possess technical skills required to create botnets themselves. Sadly, some botnet creators are even advertising "first hour free" sales to potential customers.

Botnets are usually put to two primary (and profitable) uses, although their possibilities are many:

- **Spam e-mail generation**. According to estimates, in 2006 between 50% and 75% of all spam worldwide originated from zombies. Disreputable businesses use zombies or botnets to produce spam that cannot usually be traced back to its source.
- **Distributed Denial Of Service (DDOS) attacks**. Disreputable businesses use botnets to disable a competitor's web site or e-mail server in a manner that cannot usually be traced back to its source [18].

Everyone faces the risk of having their computer become a member of a botnet. During one investigation, the U.S. Justice Department found that hundreds of Department of Defense and U.S. Senate computers were botnet members, generating spam under outside control [18].

4.5 Anti-virus Software

Anti-virus software is hyped by its vendors as a "cost-effective" solution to the very large problem of malware. Contrary to what its name implies, most anti-virus software is designed to fight several types of malware, not just viruses.

Anti-virus software uses a malware "signature" database combined with a heuristics engine to detect other, similar types of viruses. In practice, heuristics engines are not as effective as one might think, merely because vendors would receive too many complaints about "false positives" if heuristics engines erred on the side of caution.

Advantages of anti-virus software include:

- Detection of thousands of known kinds of malware.
- Automatic deactivation of detected malware.
- Periodic updates to signature databases and heuristics engines.
- Widespread availability of free or inexpensive versions.

Disadvantages of anti-virus software include:

- Each vendor's anti-virus software produces slightly different results. None has "100% coverage" of all known viruses.
- Generally, you cannot install more than one anti-virus software package at a time (which would have increased coverage).
- Today, detected malware can no longer be removed from infected files. Instead, infected files can only be deleted or quarantined, possibly resulting in data loss, data corruption, or the inability of application software to run.
- It doesn't protect a computer against all known types of malware. This is usually deliberate, as vendors would rather sell you two or more types of protection software instead of just one. Also, certain types of malware such as rootkits have never been (and may never be) detected by anti-virus or other protection software.
- Updates to signature databases and heuristics engines *always* lag hours or days behind the arrival of new types of malware [18]. The increasing use of zero-day exploits is making anti-virus and other protection software irrelevant.
- Updates are usually not free; they often require a paid yearly subscription.
- Using anti-virus software gives people a false sense of security because of marketing hype, blind trust in technology, and ignorance of anti-virus software limitations.
- Anti-virus itself is vulnerable to attack [18]. New types of malware have been known to silently deactivate or cripple anti-virus and other protection software, so that the malware can permanently escape detection.

4.6 The Writing on the Wall

Ponder This: What good is protection software such as anti-virus or anti-spyware software, when their detection signatures and heuristics engines can only be updated hours or days *after* new malware has attacked your computer? Isn't that like slamming the barn door after the horse has bolted?

Now, consider these facts (as of July, 2006):

- Microsoft Windows has a 90% market share worldwide.
- Obviously, the remaining 10% do not run Windows.
- Almost 100% of the roughly 180,000 known types of malware can *only* target computers running Windows. They have *no* effect on non-Windows computers.
- The number of known types of malware that target non-Windows operating systems can be counted on one hand. Security firms estimate that for each of these, the number of infections found "in the wild" are in the 0-49 range.

Possible Conclusions:

- Microsoft and/or anti-virus companies will save us somehow. Or...
- We're doomed. Or...
- It's OK to suffer, since everyone else in the world is suffering too. Or...
- Keep using Windows computers, just don't store anything important on them. Or...
- Don't use the Internet at all. Or...
- Use two Windows computers instead of one, where one is used only for Internet access and the other is protected by an "air gap". Or...
- *Stop using Microsoft Windows. Duh!*

News Flash: Sophos, a security software vendor that caters primarily to corporate users of Microsoft Windows, now recommends that home users replace their Windows PCs with Apple Mac computers [29]. This is the proverbial "writing on the wall".

Side Note: For four years this author has run his business exclusively on *Linux*. Results: No licenses, no patches, no updates, no anti-virus, no fears, no blue screens, no "pop-up" advertisements, no spyware, no adware, no worms, no crashes, no downtime, no expenses.

Part 5

Internet & Network Threats

The rise of ubiquitous data communications networks—such as corporate networks, wireless networks, and the Internet—coincides with the rise of network-borne attack vehicles and the decline of simple viruses.

5.1 Targeting

As mentioned in Part 4, cybercriminals and worms use a network such as the Internet to find vulnerable computers. But exactly how is this accomplished, and what can be done to stop it?

A review of four basic networking concepts, plus an introduction to three common diagnostic programs, is required before we can address that question.

5.2 Networking Concepts

- Every computer on a network is assigned a unique network address, commonly called an *IP address*. A computer's IP address is analogous to a building's street address. IP addresses are commonly expressed as four decimal numbers, each between zero and 255 inclusive, separated by a period. "216.109.112.135" is an example of an IP address.
- The Domain Name System (DNS) was developed to allow human-readable computer names (such as "google.com" or "yahoo.com") to be specified instead of IP addresses. DNS "servers" are provided as part of Internet and network infrastructures to translate such names into corresponding IP addresses. For example, "google.com" might be translated into "72.14.207.99", from which we can deduce that the computer serving Google's web page has an IP address of "72.14.207.99".
- A computer can obviously execute software that communicates over the network with another computer running compatible software. That's how you "surf the web". But you can run an e-mail program at the same time as a web browser. A computer prevents communications conflicts between programs by assigning a unique *port number* to each program. A port number is expressed as a single decimal number between 1 and 65,535 inclusive, and is analogous to an apartment number within a building. *Well-known* port numbers are those traditionally used for a specific function. For example, web server programs normally use port 80.
- A program running on one computer, can communicate with a program running on another computer, only by first establishing a "connection". It does so by transmitting a *connection request* to a specific port number at the other computer's IP address or name. A connection request is received by a program only if it is actually "listening" on its assigned port number. For example, web servers listen on port 80 for connection requests from remote web browsers. When a program is listening on a port, that port is said to be "open".

At this point we are on the verge of understanding how cybercriminals or worms locate computers on a network. However, a quick look at some common networking tools would add some clarity to our discussion.

5.3 Diagnostic Software

Networking specialists use several types of diagnostic programs to accomplish common network-related tasks, such as:

- Verifying network connectivity between two computers.
- Determining whether any computer has been assigned a particular IP address or name.
- Discovering which, if any, ports are open at a specific IP address.

Ping

One such diagnostic program is built into every computer operating system. That program is called *ping* and it's quite easy to use. You can try it *right now*:

1. In Windows, click Start - Run and then type `cmd` into the "Open" textbox. Click OK. A black command-line window will appear. If this fails, use another means to bring up an MS-DOS command window.
2. Type `ping google.com` and then press Enter. If your computer is set up in the normal manner, you will see something like this:

```
Pinging google.com [72.14.207.99] with
32 bytes of data:
Reply from 72.14.207.99:  bytes=32
time=71ms TTL=245
```

From this response we can infer that:

- A DNS server was able to translate "google.com" into a specific IP address, and...
- The ping program was able to send a request over the Internet to a remote computer at that IP address, and...
- A program at that IP address was listening on the appropriate port number, and...
- That program sent a response back to our ping program.

Ping programs accept either a computer name such as "`google.com`" or an IP address such as "72.14.207.99". So you could have typed "`ping 72.14.207.99`" instead of "`ping google.com`".

Netstat

Another diagnostic program called *netstat* is built into every computer operating system. It lets you see which ports are open on your computer, and which network connections to other computers are established [4].

Netstat is not a beginner's tool, but once you learn how to use it you can:

- Discover certain types of malware running on your computer. For example, the so-called Nachi worm will open port 707 for malicious purposes once the worm has infected a computer.
- Identify potential security risks by identifying which standard ports are open. For example, port 21 indicates the presence of an FTP server running on that computer, and FTP servers are a known security risk.

Nmap

Another diagnostic program is called **Nmap**, which is a free third-party program (not provided with Windows). Nmap falls into the *port scanner* category even though it performs many other functions [2].

A port scanner is an automated means to determine which ports at an IP address are open. A port scanner does its job by sending thousands of connection request messages to thousands of port numbers at a target IP address, hoping to receive some replies. When finished, port scanners will display a list of open ports if any were found.

Nmap can also perform a *ping sweep*. A ping sweep is an automated means to find computers on a network, by blindly running the equivalent of a ping command against every IP address within a given range. When finished, a ping sweeper will display a list of IP addresses for which ping succeeded.

A ping sweep and a port scan may be combined to produce a list of open ports for every computer within a range of IP addresses. This can bring to light some rather interesting facts. For example, this author once discovered that 16 computers at a customer's facility were infected by the Nachi worm, because port 707 was open on those computers.

If you are interested in Nmap you can visit its web site (http://www.insecure.org/nmap/).

5.4 Vulnerabilities, Exploits & Patches

Now, we can *finally* address how cybercriminals or worms find vulnerable computers on a network.

Cybercriminals (or worms) can simply perform a ping sweep to locate active computers. Then, for each corresponding IP address, they can run a port scan to locate open ports. Interestingly, cybercriminals can also use search engines such as Google to discover vulnerable servers [2].

If a well-known port number is open, it's clear that a specific type of program is running on that computer. For example, if port 465 is open then one can assume that a mail server program is running.

Cybercriminals and security experts alike know that some programs are known to have certain vulnerabilities, which can be exploited in specific ways.

A cybercriminal or worm need simply transmit a specially crafted message to a vulnerable program, to cause that program to malfunction in a predictable way, resulting in a highly desired result: external control of that computer [13].

That's why it is *critically* important for vendors to discover and immediately fix vulnerabilities in their software.

And, that's why it is *critically* important for you to apply security updates to all of your software the very instant these become available.

5.5 Port Management

Imagine this dialog:

> **Patient:** "*It hurts for hours every time someone kicks me in the shins. What can I do about it?*"
>
> **Doctor:** "*Stop letting people kick you in the shins!*"

If open ports will expose vulnerabilities, why keep them open?

Windows used to be famous in network security circles for its wide-open port configuration "out of the box" [4]. For example, previously to Service Pack 2's (SP2's) arrival, Windows XP Home Edition's default configuration opened the "messenger service" port. That service is traditionally used by corporate system administrators to send official announcements to employees. But why enable that service in XP's *home* edition? Did Microsoft think that each home contains multiple PCs supervised by a system administrator?

Furthermore, most home computers have Internet access, which means that "average Joe" has *all kinds of ports open on the Internet*. So it was easy for disreputable companies to set up automated ping sweeps and ports scans to find every open messenger service port on the Internet, so that advertisements could be sent continuously to every available home computer in America. Thanks, Microsoft!

At least Microsoft's SP2 closed that security hole. But what about other open ports? You have several choices:

1. Learn about network security so that you can manage port-related security risks yourself. *Advantages*: Your port configuration will match your specific requirements. You won't be blindly following someone else's advice for better or worse. *Disadvantages*: The learning process is time-consuming. Your initial security fixes will be delayed until you know what you're doing.
2. Have a computer geek close them for you. *Advantages*: You will get expert help in short order. *Disadvantages*: You must blindly trust that geek, for better or worse.
3. Install a **firewall**. *Advantages*: You will be protected in short order. Later, you can "tweak" your firewall to match your specific requirements. *Disadvantages*: At least initially, you must blindly trust your firewall vendor's default configuration, for better or worse. Some firewalls are *themselves* vulnerable to attacks by cybercriminals or their worms.

5.6 Firewalls

A **firewall** is a software or hardware means to block certain types of network traffic while allowing other types to pass. Therefore, a firewall can place a large

obstacle in the path of cybercriminals and worms [2, 3, 4]. Interestingly, the recent increase in firewall usage has caused many cybercriminals to shift their focus to **social engineering** techniques (see section 5.7.10).

Two types of firewalls exist: Hardware, and software. You can use both at the same time to get the best of both worlds, which is precisely what this author recommends.

Hardware Firewalls

A *hardware firewall* is a piece of electronic equipment designed to block common types of network threats. Hence you must connect it in-line between a "dirty" network (such the Internet) and your computer, so that all network (or Internet) communications must pass through the firewall.

The best hardware firewalls employ Network Address Translation (NAT) and Stateful Packet Inspection (SPI), which prevent unsolicited external network or Internet traffic—such as attack probes generated by cybercriminals or worms—from ever reaching your computer.

Firewall using both NAT and SPI are not that expensive ($100 & up). Do yourself a favor and insist on both NAT and SPI when purchasing a hardware firewall.

Advantages of a hardware firewall include:

- One device can protect an entire private network.
- It provides a central "control panel". All computers behind the firewall will receive the same type of protection.
- It is less vulnerable to attack than software firewalls.
- It usually has a built-in Internet sharing feature, automatically providing Internet access to all computers behind the firewall.
- It can usually be configured to block certain communications protocols, IP addresses, web site URLs, web page keywords, etc.

Disadvantages of a hardware firewall include:

- It costs $50-200.
- An extra piece of equipment must be maintained.
- It introduces an extra point of failure.
- It cannot be configured to disallow specific software programs from obtaining network (or Internet) access.
- It will **not** notify you when a new type of software program running on your computer attempts to obtain an outbound connection to a remote computer. Many types of malware will try to "phone home", *and you don't want them to do that*.

Software Firewalls

A *software firewall* is a program designed to block common types of network threats. You must install this program on every computer connected to a network (or the Internet).

The best software firewalls employ Stateful Packet Inspection (SPI), which provides additional protection against attacks mounted by cybercriminals or worms.

Advantages of a software firewall include:

- No extra equipment is required.
- No hardware failure can occur.
- Some are available free of charge (within the terms of their license).
- It can be configured to disallow specific software programs from obtaining network (or Internet) access.
- It will notify you when a new type of software program running on your computer attempts to obtain an outbound connection to a remote computer.

Disadvantages of a software firewall include:

- It is vulnerable to attack, just like any other software. As of April 2005, almost 80 vulnerabilities had been discovered in defensive (firewall and anti-virus) software products sold by Symantec, F-Secure, CheckPoint Software Technologies, and others.

- If you have more than one computer you may have to pay additional license fees.
- You must manually ensure that every firewall is set up the same (there is no central "control panel").
- If you use an Apple Mac *and* a Windows PC, you must buy and learn two entirely different types of software firewalls.

5.7 Safe Computing

So far we have been focusing on how cybercriminals or malware invisibly attempt to get into your computer, and what defenses you can mount to keep them out.

But what if you unwittingly invite them into your computer?

This is more common than you may think. First, consider this fictional story:

> *To keep out criminals you have fortified your property by erecting a barbed-wire fence with a locked gate. Every day you unlock that gate and cross the road to fetch your newspaper and your mail. One day, you pause to read a startling front-page story before returning home, where you discover that your wallet is no longer on the kitchen table!*

Now, consider this analogous but true story:

> *To keep out cybercriminals you have fortified your computer by installing anti-virus software and a firewall. Every day you check your e-mail and surf the web to read top news stories. One day, you receive a startling e-mail message from your bank, stating that your account will be suspended unless you verify your account information. You click the e-mail's web page link and fill out their form. Later, you discover that your bank account is empty!*

Remember, a weak link in a chain will cause that chain to break.

Anti-virus software, firewalls and other technological protection methods are strong and important links in your chain of protection. However, your computing habits are chain links, too, and if they are weak then your chain will break.

You can tremendously strengthen your chain of protection by establishing *safe computing* habits [3, 31].

5.7.1 Good Habits

Safe computing habits include:

1. Use *strong* user ID / password combinations (see section 5.7.9).
2. Shred every printed page before throwing it out (see section 7.1.8).
3. Guard mobile electronic devices (such as PDAs and laptops) as if they were your wallet or purse. Don't store PINs and passwords in these devices. See section 6.3.
4. Use a safe web browser such as Firefox to surf the web (see section 5.7.3).
5. Use a safe e-mail client such as Thunderbird to send and receive e-mail (see section 5.7.5).
6. Put a firewall on your Internet connection (see section 5.6).
7. Turn off your computer when you're not using it, especially if your computer has a continuous connection to the Internet. Configure your computer to blank its screen and lock itself after a few minutes of inactivity (requiring a password to restore normal operation).
8. **Encrypt** confidential data stored in your computer or on external media such as disks or USB memory sticks, as described in section 7.1.9 [3, 4]. Use a strong password (see section 5.7.9).
9. Destroy old disks and tapes so that no one can read their contents (see section 7.1.6).
10. Use a Mac or a Linux PC when using the Internet (see section 4.6). Update every software program you own the instant an update is available (see section 5.4).
11. Never click on any web page link you find in any e-mail. Instead, type the web page address (URL) into your browser yourself. See section 5.7.10.

12. Avoid online accounts if you can. Otherwise, try to minimize the amount of personal information you provide to web sites. Lie if you must provide extra information that seems to have no bearing on your account. Absolutely avoid "secret questions" (a.k.a. "security questions"). See section 5.7.9.

13. Obtain a credit card with an extremely low credit limit, which you will use **only** for online shopping. Fraudulent charges will be much easier to spot that way. Make sure you **never** use a debit card for online purchases.

14. Disable all "macros" in office document-related programs (such as Microsoft Office). Configure those programs to also warn you if a macro is present in a document. Macros can be put to bad uses as well as good uses.

15. Never open e-mail attachments unless you absolutely have to. Never open any attachment directly by clicking on it (see section 5.7.4).

16. Occasionally check your computer and web browser security levels by running free online tests offered by computer security firms [3]. For example, PC Flank Ltd. (http://www.pcflank.com) offers six on-line tests: Quick Test, Advanced Port Scanner, Stealth Test, Browser Test, Trojans Test and Exploits Test.

5.7.2 Web Page Landmines

People use search engines such as Google and Yahoo! every day. Unfortunately, people mistakenly assume that search engines will find only quality web sites run by reputable individuals or companies.

In reality, search engines **don't** filter search results to weed out web sites created by cybercriminals.

Even so, you may wonder what harm there could possibly be in simply *viewing* a web page. After all, it's not as if viewing a web page could force malicious software down your computer's throat, right?

ActiveX: A Nuclear Bomb

According to Microsoft, ActiveX is one of many "exciting and powerful features of Internet Explorer", with which one can easily create "a rich browsing experience" when surfing the web.

Simply put, Microsoft's ActiveX technology is a programming interface between Internet Explorer and your computer's resources (disk drives, memory, files, sound cards, etc.). So, through the miracle of ActiveX, when you use Internet Explorer to view a web page containing a suitable program, that program can reach deep into your computer and do all sorts of things [2, 18]. It can even reboot your computer!

One software engineer was so aghast at the power of ActiveX that he created an informative web page titled "*ActiveX: Or how to put nuclear bombs in web pages*" [27]. Obviously Microsoft was unhappy about that, and threatened legal action against the engineer—for simply telling the truth.

Among other things, ActiveX can allow a disreputable web site to engage in a "drive-by download attack", in which malware is quietly installed whenever a user visits that site.

The good news is that (as of July 2006), ActiveX only works with Internet Explorer. All other browsers—Firefox, Netscape, Opera and others—are, perhaps deliberately, incompatible with ActiveX. Therefore, no other browser permits web page programs to reach so deeply into your computer.

This author recommends against using Internet Explorer for that reason (see section 5.7.3).

Java

Java, not to be confused with JavaScript, is a general-purpose, standalone programming language invented by Sun Microsystems.

Java normally has nothing to do with web browsing. However, all modern web browsers contain a built-in interface to whatever Java run-time environment is installed on the computer. That interface allows Java programs to be embedded into web pages, introducing two additional security risks.

First, it's possible that a flaw in Java's run-time environment may be discovered and exploited. Fortunately, its run-time environment has suffered few known vulnerabilities, but new exploits are being seen on all fronts every year.

Second, Java can permit a disreputable web site to launch a "drive-by download attack" in an effort to install malware whenever a user visits that site.

Non-malicious Java programs are found in very few web pages, so this author recommends that you change your web browser's configuration settings to disable Java. If you have occasional need to visit a reputable, Java-enhanced web site, simply re-enable Java long enough to view that web content. Then disable it again.

Jscript

Before discussing Jscript it is necessary to briefly mention its cousin, JavaScript. In 1995, Netscape Communications invented JavaScript to enable simple programs to be embedded in web pages. Later, JavaScript was adopted as an international standard. JavaScript was designed with the user's security in mind from the very beginning.

Jscript is Microsoft's version of JavaScript. That means it does not follow the actual international standard. Due to Microsoft's "embrace and extend" philosophy, Jscript offers many more powerful capabilities than does JavaScript.

While this extra power may allow one to have "a rich browsing experience" it also allows one to have a greater risk when surfing the web, because more power generally equates to more security risks and vulnerabilities. Therefore this author believes the use of Jscript is another reason to avoid using Internet Explorer (see section 5.7.3).

5.7.3 Internet Explorer

Internet Explorer (IE) is one of of two missing sections of chain-link security fence surrounding your computer, big enough for a Mack truck [4]. That's why some people call it "Internet Exploder".

IE is Microsoft Windows' native web browser, and, like many Microsoft software products, it is tightly integrated with Windows itself.

So tightly integrated, in fact, that IE allows web sites to have full access to—and control of—Windows itself. That is why you can update Windows (and other Microsoft products) by using IE to visit Microsoft's Windows Update web site. And that is why you can't perform updates using any other browser.

Think about it: Why would you want to stumble across www.cybercrime-central.com using the *same* web browser that Microsoft uses to update Windows?

You can close that huge gap in your security fence quite simply:

1. Obtain and install the **Firefox** web browser by visiting www.mozilla.com, downloading Firefox, and installing it according to Mozilla's instructions.
2. Set up Windows' **Internet Options** as follows:
   (a) Put **only** microsoft.com into Windows' "Trusted Sites" zone.
   (b) Disable **every** feature in **all** other zones ("Internet", "Local Intranet", "Restricted", etc.). You may have to ask a computer geek for help with this [3].
3. **Never** use IE again, except to obtain software updates directly from Microsoft's web site (which is why step "2a" is included in the procedure shown above).
4. Use **only** Firefox when you surf the web [4].

5.7.4 E-mail Landmines

E-mail messages and attachments carry a huge amount of malware right through defensive systems such as firewalls and anti-virus software (as if spam weren't enough to deal with) [2].

Never click on any attachment to open it—save it to disk instead. Why? Because various techniques allow cybercriminals to mask part of an attachment's name, so recipients cannot easily determine an attached file's true name or type. For example, you might think an attached file's name is "CoworkersNaked.bmp" when its name is actually "CoworkersNaked.bmp.exe". You wouldn't want to click on the latter!

After the attached file is saved, do **not** find that file on your hard drive and then click on it! That would be the same as clicking on the attachment, and you don't want to do that.

Instead, simply open the application program designed to handle that type of file, and use the application's

"File - Open" dialog to find and open that file. Image programs that will open "BMP" files will refuse to open "EXE" files, thereby saving you from inadvertently executing malware.

5.7.5 Outlook

Outlook and Outlook Express are Microsoft's e-mail clients for enterprises and home (or small businesses) users, respectively. Here we will simply call them both "Outlook" since they share the same roots.

Outlook also happens to be the other missing section of chain-link fence [4]. It is is tightly integrated with Windows and IE, and so it suffers from many of the same vulnerabilities as they do.

You can close that huge gap in your security fence quite simply:

1. Obtain and install the **Thunderbird** e-mail client by visiting www.mozilla.com, downloading Thunderbird, and installing it according to Mozilla's instructions.
2. **Never** use Outlook again. Yes, really!
3. Use **only** Thunderbird for e-mail [4].

5.7.6 PDF Landmines

Adobe's Portable Document Format (PDF) file format is ubiquitous on the World Wide Web. However, most people don't realize that, for years now, JavaScript programs can be embedded into PDF files.

Adobe has occasionally reported vulnerabilities in its version of JavaScript, which cybercriminals were able to exploit to give PDF files a virus-like behavior when they are opened with Adobe's Acrobat Reader.

Few PDF files contain any JavaScript code. Therefore, this author recommends that you change your Acrobat Reader's configuration settings to disable JavaScript. If you have a legitimate need to view a trusted, JavaScript-enhanced PDF file, simply re-enable JavaScript long enough to view that one document. Then disable it again.

5.7.7 Flash Landmines

Macromedia's Flash (SWF) file format allows movies to be embedded into web pages. This requires Macromedia's Flash Player "plug-in" software to be downloaded and installed, which almost everyone has already done.

Unfortunately, Macromedia has occasionally reported some rather serious security risks due to software bugs within their Flash Player software. Cybercriminals can literally take over a computer by exploiting those vulnerabilities.

Worse, the Flash Player plug-in cannot be disabled and is difficult to remove once installed. But this author strongly recommends that you search Adobe's web site (adobe.com) to learn how to remove the Flash Player (or just its browser plug-in component).

5.7.8 Multimedia Landmines

In 2004, RealNetworks reported a serious vulnerability in its RealPlayer software, which is used to play music and video files. If a specially crafted music or movie file is played it can cause that player software to malfunction in a predictable way, resulting in a highly desired result: external control of that computer.

Unfortunately, flaws have been found in almost every media player software available, at one time or another. You should think twice about using your computer to listen to music or watch a movie.

More importantly, you should **never** play any media file you receive in an e-mail (even if it's from someone you know), because a cybercriminal could have created it! Burying a rootkit in a funny video would be an excellent example of social engineering (see section 5.7.10).

5.7.9 Passwords and User IDs

People obviously know that their user ID and password are supposed to guard their account from unauthorized access, but most people fail to understand five critical concepts:

1. *Someone may actually try to get into their account.*
2. *Their user ID is just as important as their password.*
3. *Most user IDs and passwords are weak (easy to guess or compute).*
4. *"Security questions" are a curse.*
5. *Cybercriminals have all the time in the world.*

Let's discuss these concepts one by one.

Online Break-ins

The Gartner Group has reported that $2.4 billion had been robbed from Internet-accessible bank accounts between June 2003 and May 2004 [18]. Newer statistics are probably higher because of the trend towards ubiquitous online banking.

Therefore, we can conclude that cybercriminals do, in fact, break into password-protected accounts.

User IDs

Most people think every account is protected by its password. *This is false!* In fact, it is the *combination* of user ID and password that protects an account.

To increase your account's security you must learn to regard a user ID and a password as being the same kind of thing. They are both the same sort of combination lock.

Common sense tells us to secure a door with two locks instead of just one. We know that our security suffers when one of those locks is missing or is extremely cheap. Similarly, we should realize that every account should be secured with both user ID and password, instead of just the user ID. We should know that our security suffers when the password is missing, or when the user ID or password is *weak*.

Weak User IDs and Passwords

A user ID or password is *weak* when it can be easily guessed by someone, or easily computed by password-cracking software.

Before we learn about what makes a user ID or password *strong*, let's stop to consider why most people have weak user IDs and passwords, so that we can learn what *not* to do.

People have weak user IDs for two main reasons:

- A user ID was assigned to them when its account was established. Very interesting, because people don't realize that in many cases an "assigned" user ID is simply a *recommended* or *default* user ID. If so, they could have overridden that default when the account was established.
- They chose their own user ID when its account was established, but they followed the common but foolish practice of basing their user ID on their name.

In either case, people usually end up with a weak user ID such as "jsmith", which even a six-year old child can guess.

When a user ID is weak, the password is all that protects that account, and so the password absolutely must be strong. A better solution would be to strengthen your user ID if possible. Some accounts let you change both user ID and password at any time.

Similarly, there are seven main reasons that people choose weak passwords:

- They don't understand how some passwords are stronger than others.
- They think their password is so clever that no one could possibly guess it, such as "GR8-ONE", "SteveRocks", "kennwort" (which is German for "password"), or simply "z".
- They want a password that's easy to remember, like "grapefruit".
- They desire a password that represents something (or someone) meaningful to them, like "69mustang" or "angeleyes".

- They think they don't need a password, so they just leave it blank.
- A default password was provided to them, and they think it's good enough.
- They don't realize that cybercriminals use social engineering techniques and automated password-cracking software to discover user IDs and passwords.

That last reason is key, for it directly addresses all of the other reasons.

Cybercriminals commonly use three different methods to obtain illegal access to someone's account. First, a cybercriminal will check to see if the account's password is either blank (missing) or is set to a well-known default value (which can be discovered via some Googling).

Second, a cybercriminal may use a targeted attack based on social engineering. Here, a cybercriminal will assemble dossiers by collecting odd tidbits of personal information. When a sufficient amount is collected, the cybercriminal will have found his next "mark" (victim) [30].

For example, if someone whose online nickname is "Jeb69" posts a message on a web site complaining about the First National Bank of Briar Patch, it's likely that "Jeb" has an account there. Some extra Googling may bring to light that this same person's e-mail address is jebsmith@hotmail.com, that he has a German Shepherd named "Lilly", and that he owns a '69 Harley Sportster motorcycle. As a result, a cybercriminal would target Jeb Smith's bank account, using passwords based on his dog or bike. Perhaps the cybercriminal would try to find and answer the account's "secret question", as discussed later.

In some cases, the "cybercriminal" is actually someone relatively close to the victim, such as a neighborhood teen, an estranged brother, or a coworker. In that case the cybercriminal is able to more easily collect personal information about the victim. Regardless of how they are done, targeted attacks are surprisingly effective.

Third, a cybercriminal may use easily available but sophisticated password-cracking software to generate lists of likely passwords. Some password-cracking software permits "hints" to be specified, which could be "Jeb", "Smith", "Lilly", "German", "Shepard", "1969", "69", "Harley" and "Sportster" for the previous example. Other password-cracking software simply uses a **dictionary attack** strategy, where passwords are generated based on common words found in the dictionary [4]. Or, a "brute-force" method can be used, in which every possible combination of characters is tried, one by one.

Password-cracking software is surprisingly effective, but only because most people use weak passwords!

The Curse of the Secret Question

In recent years, online accounts have sported a new "feature" designed to help you log on should you forget your password. This is usually based on a "secret question" (a.k.a. "security question"), which you are asked to define when setting up your account.

For example, you might be asked to select one of four "secret questions" (such as "What was your first pet's name?"). Then, you will be asked to provide an answer to that question (such as "Wolfie").

This is a really stupid idea! Here's why:

1. It creates a "back door" that deliberately circumvents your password.
2. It offers only a very limited set of simple questions, each of which can only have a very limited set of simple answers.
3. Cybercriminals can use a targeted attack to obtain (or guess) answers to those simple questions.
4. The answer to a secret question never changes, which means the "back door" will continue to work even if you change your password.

The solution is to deactivate the "back door" [36]. To do this, select any "secret question" at random, and then answer that question by simply hitting a bunch of keys at random to generate something like "awropuqwpegjhvkl". If you should ever forget your password, simply contact tech support personnel and provide sufficient credentials to allow them to reset your password.

Time is on Their Side, Not Yours

When setting up an account we usually have only a few seconds in which to choose a new user ID or password. But cybercriminals face no time limit at all when trying to break into an account. They can keep trying for hours if they wish.

That is why we must be prepared to select strong user IDs and passwords *ahead of time*. We cannot wait to ponder such things until a new account setup screen is staring us in the face. If we do, we will likely pick weak user IDs or passwords.

When we pick a strong user ID and password, cybercriminals will likely give up after a while and move on to the next person's account. There's far more profit to be made by plucking many "low-hanging fruit" than by focusing on one difficult target.

Strong User IDs and Passwords

Now that we have examined weak user IDs and passwords, let's see how to create strong ones [3, 17]. A user ID or password is strong if it:

1. Contains no common word(s) in any major language in the world, **and**
2. Uses both uppercase and lowercase letters, **and**
3. Includes numeric digits, **and**
4. Has punctuation characters such as "!", **and**
5. Contains at least eight (preferably 10) characters in length, **and**
6. Is seemingly too difficult to remember, **and**
7. Is not used for any other account, **and**
8. Is changed frequently.

Here are some examples of strong user IDs or passwords (no kidding!):

- `@^H~6Bx@9i`
- `f~4fj*wCrK`

Since strong passwords can't be easily remembered, you will want to write these down and store that list so that it cannot be found by untrusted persons. For example, you could store the list in an unmarked manila folder within a locked file cabinet in your locked office. A cybercriminal is unlikely to travel to your state (or even your country), break into your home and find your password list before draining your bank account.

5.7.10 Social Engineering

Social engineering is a relatively new attack method. It is designed to bypass technological security measures (such as firewalls and anti-virus software) by using human psychology to trick people into letting a cybercriminal gain access to computers or information systems [2, 4].

Social engineering techniques are most often used in connection with the Internet, but such techniques can also be used in many other ways (see section 6.1). Internet-related social engineering techniques such as **phishing** appeal to basic human instincts such as curiosity and fear.

Phishing

Phishing is a social engineering technique involving the use of fake but seemingly authentic e-mail or instant messages to obtain someone's confidential information, such as credit card numbers or passwords [3].

In June 2004 The Gartner Group estimated that 1.98 million adults in America had suffered losses from phishing scams [18]. As of July, 2006, more than 40 million phishing scams were being attempted *every week*.

Phishing usually relies on e-mail address *spoofing*, which is the creation of a false "From:" address for an e-mail. As a joke, this author once sent his wife a "threatening" e-mail message that was apparently from Bill Gates at Microsoft. Unfortunately, she was quite shaken because she had believed the message was genuine!

Phishing also makes extensive use of e-mail messages that are coded in HTML (HyperText Markup Language), which allows logos, web page links and other features to be incorporated into a message.

The tricky thing about HTML-based web page links is that *the link's URL doesn't have to match the link's human-readable text*. Therefore, it's easy to create a link saying "http://news.google.com" or "Bank of America" that actually points to "www.nasty-spyware.com" instead. *That is why you should never click on any link in any e-mail message!*

A classic example of a phishing attempt is an e-mail message that is carefully constructed to mimic what a bank would normally send to its customers. This message might inform the recipient that his account would be suspended if he didn't confirm certain critical facts (such as his Social Security Number, his bank account number, online banking password, etc.). A link to a fake "bank" website is usually provided so that gullible recipients can fill out a form to provide cybercriminals with all the information needed to drain the recipient's bank account.

A less-obvious example of a phishing attempt would be an e-mail supposedly from CNN or another news agency, containing a copy of an actual or fictitious news story with a web site link so that you can "Read More". People will click on that link without even questioning why they would ever receive an e-mail from CNN, and a few seconds later "www.fooled-you.com" will begin to load malware into their computer.

Other Trickery

To demonstrate the effectiveness of social engineering techniques, some bank security auditors placed 20 USB memory sticks at random locations in a bank's parking lot, as if someone had lost them. Within hours, bank personnel had used bank computers to execute completely unfamiliar software stored in 15 of those devices.

Fortunately, the software was not dangerous, but had cybercriminals planted those devices instead, all sorts of malware would have been installed *behind the bank's firewall*. This would have been a really bad thing because firewalls generally allow outbound traffic, so it is possible that the malware would have been able to "phone home" (to the bank's severe disadvantage).

5.8 Threats to Wireless Networks

Wireless access points (WAPs) create a cable-free "bridge" between conventional wired networks and mobile devices such as laptop computers. WAPs have been deployed worldwide by corporations, libraries, stores, schools and homeowners alike.

According to a Federal Bureau of Investigation (FBI) security presentation in 2005, about 70% of the millions of WAPs in the U.S. are completely unprotected against random access by strangers [18].

If protected at all, most WAPs use an **encryption** method known as Wired Equivalent Privacy (WEP). Unfortunately, WEP can be cracked in minutes using software that is freely available on the Internet [2, 18]. This was demonstrated by the FBI when they penetrated a wireless network in three minutes during their presentation. It should also be mentioned that many people enable WEP but don't change the default password provided by their WAP's manufacturer!

In 2003, WEP was superseded by Wi-fi Protected Access (WPA or WPA2), which is thought to offer superior security. Everyone should use WPA instead of WEP [3]. However, new attacks are being invented daily, so one cannot simply set up WPA and then forget about it [13].

You may think it unnecessary to bother with WEP or WPA, because after all, how would a cybercriminal even know where to find your WAP? Surely that would be like finding the proverbial needle in a haystack!

You can directly answer that question by clicking on the "Web Maps" link on wigle.net's home page (http://wigle.net).

There, you easily "zoom in" to see your city or your neighborhood. Each colored dot on the map represents a WAP; green indicates an unprotected WAP, while red represents one that uses WEP or WPA encryption. It's possible that you may even see your own WAP.

So much for your "needle in the haystack" theory!

In case you're curious (or even enraged) at this point, all of the WAPs in wigle.net's database were discovered by people who engage in a hobby called **wardriving** [2].

Part 6

Non-technological Threats

Ask any elder about what financial or business troubles he or she faced earlier in life, and you will hear nothing about losses due to online account break-ins, or contract penalties due to hard drive crashes. Instead, you will hear about property theft and con-men, which are still problems today. The more things change, the more they stay the same!

6.1 Social Engineering

As mentioned in section 5.7.10, social engineering is the use of human psychology to trick people into exposing vulnerabilities. While the term "social engineering" is new, the techniques themselves are quite ancient. Every con man throughout history has used social engineering techniques.

The problem with social engineering is that criminals such as con artists know all about this technique, but honest people do not! Fortunately, some books and web sites on social engineering are available, which may shock you but at least will educate you [5, 30, 39].

Social engineering techniques used by corporate spies and other criminals include:

- Pretending to be a woman by using a voice changer during telephone calls. Male targets will more often provide critical information to a woman than to a man, especially if she appears to be flirting with him.
- Sending a letter to obtain information. For some reason, people trust the written word and let down their guard. Some con artists mail out fake sweepstakes forms (etc.) to obtain personal information such as mothers' maiden names and Social Security Numbers!
- Pretending to be a janitor, maintenance man, coffee machine repairman, landscaper, city code inspector, flower deliverer, or exterminator, to gain entry to a facility. Once inside, a cybercriminal can attempt to gain access to important company information.
- Wearing a fake ID badge, possibly fashioned after an actual sample that was photographed through a telephoto lens. Many employees will open a door for a "fellow employee" whose ID badge fails to scan correctly.

6.2 Facility Security

Many business facilities are wide open to intruders. For some reason, no one seems to know or care about things like:

- Rear doors propped open for ventilation, or for smokers' convenience.
- Front doors unguarded by receptionists who are often away from their desk.
- Exterior door mechanisms that are prone to being "jimmied" because they are in such poor condition.
- Out-opening doors with no latch guards. A screwdriver or ice pick is all it takes to open such doors.
- Shipping bays that are wide open most of the time (day or night).
- Automatic door closers that take 10 seconds to cycle. It is easy to walk in after someone else has unlocked the door.
- Keys left in unlocked company vehicles, possibly with facility keys on the same keyring.

Since information is stored everywhere—on disks, in notebooks, and on paper—it is not hard for a corporate spy or common thief to grab some important information and run out the door [39].

6.3 Property Theft

Thieves and corporate spies rely on poor facility security and employees' unfamiliarity with social engineering techniques, to steal loads of equipment, prototypes or files from businesses [38]. Examples:

- Many laptop computers, video projectors and even purses or wallets are stolen from offices and conference rooms near unsecured doors, because thieves can simply walk in and grab these during lunchtime.
- Thieves almost always dress to blend in with their victims, and sometimes even take lunch with them before stealing something.
- Some thieves enter a building and then hide inside until after employees leave.

Security experts recommend:

- Hiding purses, wallets, USB memory sticks, PDAs and other valuables every time you step away from your office.
- Using a security cable on each computer (whether desktop or laptop), and on other equipment such as video projectors.
- Informing a manager when a "stranger" is found inside or outside the building.
- Not holding the door open for someone unfamiliar to you, even if they sport a badge.
- Watching automatic doors close so that no one can sneak in.

Part 7

Data Leaks, Data Loss & Privacy

You should stop distributing Microsoft Office documents via e-mail and web sites—immediately—unless you "scrub" those documents using a reputable third-party tool.

7.1 Data Leaks

Enterprises and individuals can inadvertently allow important information to fall into the wrong hands. For example, an employee can e-mail a spreadsheet file to a customer, not knowing that the spreadsheet contains hidden information such as profit margins or even derogatory statements about that customer.

Or, company personnel can store proprietary documents and photographs in a "hidden" corner of a company's web server, not knowing that Google and other search engines might easily find such items and make them publicly visible in search results [2].

Finally, it is a sad fact that competing companies sometimes hire cybercriminals to steal or discover information so that a competitive advantage can be gained [5, 39].

Such "**data leaks**" have consequences such as embarrassment, termination, blackmail, lawsuits or even financial ruin.

7.1.1 Meta-data

Microsoft Word documents (.DOC files) contain a wealth of hidden **meta-data** including deleted text, employee names and computer user IDs, text from other (unrelated) documents, company information, computer filename and pathname, local printer names, computer hardware information, e-mail headers and/or web server information [6, 20, 21].

In 2003 the British government published a Microsoft Word document which was supposedly their dossier on Iraq's security and intelligence services. Dr. Glen Rangwala of Cambridge University dissected that file and discovered much of its text was plagiarized directly from a U.S researcher on Iraq. Worse, the document's revision history identified its last ten authors plus their edits and commentary [19].

While it is true that later versions of Microsoft Office programs can be configured to not save personal data in document files, only a fool would trust that feature to scrub documents completely clean.

Many third-party tools are available to remove meta-data [21]. These include:

- **iScrub** by Esquire Innovations (http://www.esqinc.com).
- **ezClean** by Kraft Kennedy & Lesser (http://www.kklsoftware.com).
- **Metadata Assistant** by Payne Group (http://www.payneconsulting.com).
- **Doc Scrubber** by Javacool Software LLC (http://www.docscrubber.com).
- **Out-of-Sight** by SoftWise (http://www.softwise.net).
- **Workshare Protect** by Workshare (http://www.workshare.com).
- **Metadata Scrubber** by BEC Legal Systems (http://www.beclegal.com).

Note: This author has evaluated *none* of these tools and can offer no recommendations for or against any of these.

7.1.2 E-mail

In 2002, Internet security journalist Brian McWilliams decided to try "hacking into" Saddam Hussein's e-mail account on the official Iraqi government web site. McWilliams succeeded, simply by using the word "*press*" for both user ID and password! [25] Once "in", McWilliams saw many e-mail messages from businessmen and corporate executives who wanted to do business in Iraq.

From this lesson we should learn to secure every e-mail account with strong user IDs and passwords (see section 5.7.9). But e-mail-related data leaks can occur in other, more insidious ways.

For example, e-mail messages and their attachments are often forwarded and re-forwarded to third parties without much thought, which can create quite a sizable data leak. This can be mitigated two ways:

- Mandatory **encryption** for attached files, as described in section 7.1.9 [3, 4].
- E-mail forwarding policies set and enforced by management.

Many companies have a web-based e-mail portal set up so that employees can check their mail from home or while on the road. Such e-mail servers should be configured to require strong passwords, and to lock an account if three or more incorrect login attempts are seen.

7.1.3 Corporate Networks

Company personnel are not so stupid as to install network jacks in their parking lots. But many do install jacks in publicly-accessible conference rooms, lobbies, cafeterias and libraries. Or, they install wireless access points in or near those areas (see section 5.8). Outsiders can simply plug right into the corporate network.

Even if no network jacks or wireless access points are accessible, cybercriminals may still find a "back door" or alternate way in. For example, sometimes an old-fashioned analog modem will be installed on a server so that Information Technology (IT) staff members can establish a remote administrative connection via telephone line. Such modem connections are often left active for years, long after IT staff has upgraded to a modern Virtual Private Network (VPN) connection.

The good news is that a simple security audit can be performed to determine if any network access is available in public areas of the company.

7.1.4 Voice-mail

During Hewlett Packard's merger with Compaq in 2002, an intruder obtained access to the HP CEO's voice-mail account and leaked voice-mail messages to the press [24].

Voice-mail accounts are usually protected by simple user-defined numeric access codes. New accounts are usually set up with well-known default codes that any cybercriminal can find via Google. When phone system administrators reset someone's access code, it is usually set to the same default.

Unfortunately, people generally fall into the same sort of traps when choosing a voice-mail access code, as they do when choosing a computer account user ID or password (see section 5.7.9).

In short, you should not leave the default access code in place; you should not choose your birth year or another personal datum as your code; you should not choose stupid codes like "123"; and you should not choose a code based on any physical pattern of button presses on a keypad (like "159" or "258"). Believe it or not, some books and web sites list every possible pattern of telephone button presses, so a cybercriminal doesn't even have to invent these himself!

Your phone system administrator should configure your phone system to lock an account if three or more incorrect access codes are entered.

7.1.5 Web Servers

Most businesses and many individuals have a web site, which of course is stored as individual files on a web server computer. Since a file is just a file, it is possible to store a large number of files—and many different kinds of files—on a web server. In fact, some companies use their web server as a sort of file server for their employees' convenience.

This begs the following questions:

1. *What files are currently stored on your web server?*
2. *Which files are currently required?*
3. *Which files are obsolete (dead wood)?*
4. *Which files are not related to any web page?*
5. *Which files are confidential?*
6. *Which files are publicly visible?*

Most employees (including company web design staff) don't really know the correct answer to most, or even all, of these questions. Worse, they don't even have the ability to find out. And even worse, they think that none of these questions is important because, after all, their web site "works the way it's supposed to".

As a result, from many web servers spring a great number of data leaks.

If you or your company have a web site, here's an experiment that you can try *right now*:

1. Open your web browser and bring up Google's main page (google.com).
2. Suppose your web site's URL is "www.abc.com". Into Google's search text box, simply type "`site:abc.com`" (with no double-quotes and no spaces).

You will see every page *and file* that Google has found on your web server. It's possible that you will find some stuff that shouldn't really be there, such as:

- Confidential spreadsheet files.
- Obsolete web pages.
- Customer databases.
- Half-finished web pages still being worked on by your web designer.
- Internal PowerPoint presentations for last month's sales meetings.
- Proprietary documentation intended for Field Service personnel.
- "Private" web pages meant for some specific use.

The moral of this story is: *Never put sensitive data on a web server!*

7.1.6 Equipment Disposal & Repair

Tons of electronic equipment and data storage media are sold, donated or put into the trash every day. Therefore, "tons" of stored data are also being sold, donated or put into the trash every day, causing a massive data leak.

For example, an Ohio couple had taken their computer to Best Buy to have its hard drive replaced. The company assured them that the old hard drive would be physically destroyed. Almost a year later, the couple received a phone call from a Chicago man who had bought that same "destroyed" hard drive at a flea market. The Chicago man had found the couple's phone number (as well as Social Security numbers, bank statements and investment records) stored on the hard drive, but was conscientious enough to notify its original owners [9].

It is important to find and destroy all stored data before taking a device in for repair, or before disposing of anything. However, that is easier said than done:

- We often delegate to, or rely on, other people who may not know or care about information security. The Ohio couple fell into this category.
- It's hard to locate where data is stored in modern devices. Do you know where your cell phone's address book is physically stored? Have you ever removed the cover from your computer, let alone replaced a hard drive?
- Simple erasure (deleting or even reformatting) doesn't actually destroy data [34]. Simple software tools are often all that's needed to recover data.
- Dead hard drives do tell tales. Drives that will no longer "boot up" a computer are usually totally readable by plugging them into another computer as a "slave" drive. Even drives that are unreadable as slaves can be sent to a data recovery service.
- Destroying a data storage device—such as a CDROM disk or hard drive—is physically messy and potentially dangerous.

The bottom line is that data destruction must be a part of everyone's information security plan.

7.1.7 Bluetooth Devices

Did you know that malicious passers-by can plant a virus on, or obtain confidential data from, your **Bluetooth**-enabled phone or PDA? It takes only 15 seconds for someone to locate and copy your phone's address book via Bluetooth.

One security auditor visited Britain's House of Parliament, where he had the opportunity (which he didn't take) to use Bluetooth to obtain the address books and calendars of several prominent politicians. His report resulted in a mandate that all Bluetooth devices be turned off in the House of Parliament.

As cell phones become smarter and begin to converge with PDAs, malware such as worms and spyware will begin to spread via Bluetooth and other mobile communications media. As of July 2006 there were only a few known cell phone viruses, and these were still rare. They were transmitted via Bluetooth and only infected smart phones running Symbian's operating system.

You may want to examine your own phone. Is it a smart phone? Do you even need a smart phone? Does it have Bluetooth capability? Do you even need that feature? Can you permanently disable Bluetooth? Can you turn on Bluetooth only when you need to use an accessory such as a wireless headset? Do you need to store confidential information in your phone at all?

7.1.8 Shredding

When Iranians stormed the U.S. Embassy in 1979, embassy officers shredded everything they could, but Iranians managed to *reassemble* and publish 70 volumes of those documents [23].

Many people don't bother shredding at all, causing a great data leak. Three basic types of shredders exist:

Strip-cut: These inexpensive and fast shredders offer a lot more security than not shredding at all. However, the U.S. Embassy had used strip-cut shredders, which did not stop the Iranians for long.

Cross-cut, diamond-cut or oval-cut: These offer superior security compared to the strip-cut type, but are significantly slower and more expensive.

Shredding services: This is a way to "farm out" your shredding chores to a third party. For security reasons this author does not recommend outsourcing basic security tasks such as shredding.

Note that most (if not all) shredders are able to destroy credit cards as well as paper. Some will also destroy CDROMs and DVDs.

Once you have got a shredder or a shredding service, it's important to define a shredding policy. What gets shredded and what doesn't? This author simply recommends shredding everything that isn't public knowledge.

7.1.9 Encryption

Encryption is the reversible process of using a password as the basis for translating information into an undecipherable form to ensure secrecy. The reverse process is known as **decryption**.

Some encryption methods are inherently weak, meaning that cryptographers can eventually perform decryption without knowing the password. Other encryption methods are strong, which is desirable.

The easiest, cheapest universally available way to encrypt a data file is to simply put that file into a password-protected "zip" file. Well-known programs such as PKZIP, WinZip and others are readily available and fully compatible with the "zip" file standard.

It's true that many "zip" file password cracking programs are widely available, but they all use techniques such as the **dictionary attack** and others described in section 5.7.9. Therefore, *you absolutely need to use a strong password* when encrypting a file.

7.2 Data Loss

We can be our own best enemy when it comes to information security, for we constantly trust that our critical paper files and data storage devices will always be there for us.

But what would happen if some (or all) of your paper files or data storage devices were lost, stolen, damaged, corrupted, burned, or flooded? Would your projects

fail? Would your job be in jeopardy? Would customers tolerate the consequences? Would your business survive?

Let's take a look at some important considerations for preserving your data.

7.2.1 Paper Files

Before the digital era, people used to "back up" all paper hardcopy on film (usually using microfilm or microfiche formats). An enormous number of pages could be stored in each roll or fiche. Duplicate copies could be stored off-site to protect intellectual property and legal evidence in case of a fire or flood.

Today, people use a lot of paper but act like it's no longer important. They seem to forget that a legal "paper trail" may still be required to demonstrate "due diligence" in a court of law. They forget that specifications, reports and contracts are still signed, stamped and annotated.

They may back up their data but fail to "back up" their paper!

There are three fairly inexpensive and quick ways to "back up" your paper copies:

- Invest in an old-fashioned photographic copy stand, plus a suitable low- to mid-priced digital camera. Mount the camera on the copy stand and take a "snapshot" of each printed page. Back up the digital photo files as you would normally back up any other files. Snapping a photo of a document is quick and easy, plus it captures a full-color image of any document regardless of its size. This is the author's preferred way to back up paper copies.
- Buy a scanner for your computer, and use it to scan each document to a file. Back up these files as you would normally back up any other files. Unfortunately, scanning a document can be a painfully slow process even if you use a sheet-fed scanner (which can jam), and you will be unable to scan anything much larger than a letter-sized original.
- Use a copier to create paper copies. This can be painfully slow, and it creates many pounds of paper. You may have trouble with oversized documents, although many copiers seem to work well with legal and 11x17 originals. You may have to use a color copier for some items.

Once you have "backed up" your paper copies, you will need to carefully consider how and where to store those backups. This is covered in section 7.2.5.

7.2.2 Computers, Cell Phones, PDAs

Unfortunately, it can be difficult to "back up" data stored in some cell phones or PDAs. You will need to figure out the best way to do this, based on your specific phone or PDA.

Cell phones and PDAs are often misplaced because they are so small. You should always stand ready to lose any data they contain, unless you find a way to perform backups.

In contrast, it's fairly unlikely that you will misplace your laptop computer, but the rise in popularity of laptop computers have made them a likely target for thieves. Also, let's face it: laptop computers aren't built to withstand much abuse despite their mobile nature. Basically, you need to be always ready to "lose" your laptop computer, by constantly back up its data (see section 7.2.4).

But, more importantly, you need to ensure that if a thief takes your laptop or PDA, he will not have access to your data. You absolutely need to **encrypt** your personal, proprietary or confidential data as discussed in section 7.1.9 [3, 4].

Thieves need to work fast to avoid getting caught, so they won't waste much time trying to crack your encrypted files. They will more likely take a quick look around to see if any valuable unencrypted information can be copied off for future use (and possibly sold for identity theft purposes).

It is a mistake to believe that you need not encrypt files if your computer requires a log-in password to "boot up". To the contrary, it's quite easy to boot a computer using a separate operating system—usually DOS or Linux—stored on a floppy disk, CDROM or USB key. This completely bypasses your normal log-in and gives one complete access to your computer's hard drive.

Once you have backed up your phone, PDA or laptop, you will need to decide how and where to store your backup media (see section 7.2.5).

7.2.3 Media and Memory Sticks

We tend to consider floppies, CDROMs, DVDs, portable hard drives and USB "memory sticks" as various sorts of backup devices, but in fact they often contain original copies of files that are not backed up anywhere else. It's important to manage all those files on all those media and memory devices. Fortunately, files on these devices can be copied quite easily using one of the backup methods described in section 7.2.4.

Small devices and disks can be misplaced, lost or stolen, so you need to ensure that if someone finds or steals these, he will not have access to your data. You absolutely need to encrypt your personal, proprietary or confidential data as described in section 7.1.9 [3, 4].

Once you have backed up your media and memory sticks, you will need to think about how and where to store your backups. This is covered in section 7.2.5.

7.2.4 Backup & Restoration

Everyone might agree that religiously backing up data is important, but in reality this task is often overlooked in today's fast-moving world. Establishing a solid computer backup method and a backup schedule is actually harder than it sounds [3, 16]. Difficulties include:

- Most hard disks hold more data than will fit on common backup media.
- Backing up a large amount of data can take many hours.
- Many backup methods don't verify that data was written correctly.
- Backups require supervision so that problems can be corrected.
- Validating a backup is difficult and time-consuming.
- Reusable backup media can eventually become unreliable.
- Management of backup media is not trivial.

Three main backup methods exist:

- **Bare-metal** backups create a so-called "image" file, which is perfect bit-for-bit copy of an entire hard drive. Later, the image can be written onto a new or existing hard drive, which can then be installed in a computer to restore normal operation. An image contains everything your original hard drive contained: boot sector(s), partition table(s), operating system(s), application software and user-created data files. A bare-metal backup can consume hours. Some bare-metal backup software allow individual files to be recovered from the backup, while others require a complete restoration of the entire hard drive just to gain access to a single file.
- **User-file** backups record only user-produced data files such as documents and pictures. Operating system and application software files won't be backed up. If you have only a few user files then a backup could take just a few minutes. But most people accumulate tons of user files, so backups can take hours. Individual files can usually be restored from a user-file backup. However, if your hard drive fails or becomes corrupted, you will have to completely re-install the operating system and all application software from scratch, and then apply all patches and updates, before you can restore your user-file backup. This can take hours, and after it is done your computer will likely operate differently than you were accustomed to.
- **Incremental** backups record only those files that have changed since the last full backup, which means that this type of backup must be used in combination with a full (bare-metal or user-file) backup. Incremental backups are generally very quick.

Once you have backed up your digital data, you will need a plan for how and where you will store your backups. This is covered in section 7.2.5.

A critical but often-overlooked part of the backup and restoration process is the backup *validation* process. Some people back up data all the time, but have never had to actually restore it. It is quite a shock to discover that all of your backups are useless, because something was wrong with your methodology or implementation. Validating a backup process can be quite time-consuming but it absolutely must be done before it's too late.

Finally, we should mention that the backup and restoration process plays a vital role when you buy new equipment such as computers or memory sticks, for it provides an easy and familiar way to transplant data from old devices to new ones.

Backups also play a vital role when you need to send in your computer for repair. Most people don't know that computer warranties usually cover only hardware, not software. If software is covered, it will clearly be only software included with the original purchase. Many vendors would rather replace than repair, which means that you have only a slim chance of getting your original computer or hard drive back. At that point you would have lost a lot of data *and* created a massive data leak at the same time (see section 7.1.6).

7.2.5 Storage of Backup Media

An amazing number of people store their backups right next to their computer. What if upon arriving at their office one day they find a burnt-out shell instead of a cubicle?

It's extremely important to store backup copies at a secure off-site location that is unlikely to be affected by the same disaster as might affect your home, office or business.

If no off-site storage facility is available, you should strongly consider buying fire-resistant storage units, such as those made by companies like Sentry Group (http://www.sentrysafe.com). Some are fairly inexpensive (under $100). You should place these storage units far from your office in a location that is unlikely to be flooded, so that it is less likely that your backup would be destroyed along with your computer and other devices.

You may want to purchase some of these storage units for off-site storage purposes as well.

While fire-resistant storage units are primarily designed to protect paper documents during a typical fire, disk media and small electronic devices can survive too if these are inserted into flattened, zipper-sealed, airtight heavy-duty plastic bags. This prevents damage from high humidity levels found inside fire-resistant storage units during a fire. Flattening the bags allows for considerable air expansion due to higher than normal temperatures, while still maintaining an airtight seal.

7.2.6 Uninterruptible Power Supplies

An Uninterruptible Power Supply (UPS) is a piece of electrical equipment designed to continuously supply 120VAC to a load, even during a power failure. Most, if not all, UPS units also contain transient suppressors and power filters to reduce power line noise. Some UPS units will also auto-correct for voltage sags or surges.

All UPS units contain one or more lead-acid gel cell batteries and a power inverter circuit that produces a crude approximation of a sine wave during power outages. Otherwise, normal "wall" power flows through the UPS to the load, charging the UPS's batteries at the same time. UPS units will normally run for 20-60 minutes at full load.

UPS units are commonly connected to computers and related equipment so that computers can stay running during a power failure. Most UPS units can, via a separate cable, send battery status data to a computer connected to the UPS. This allows for an orderly but automatic shutdown of that computer should the UPS batteries become exhausted during a power failure.

To preserve your data, you should strongly consider buying one or more UPS units for your computers and related equipment.

Here are some important points to consider when buying and using UPS units:

- Each unit is designed to carry a maximum load, usually expressed in Volt-Amperes (VA). You should not buy a UPS that would operate close to its limit. It is best to have some headroom.
- Two or more UPS units may be more practical and cost-effective than one big unit.
- You should connect most, if not all, of your computer peripherals to a UPS too. This includes networking equipment, analog phone line modems, DSL and cable modems, scanners, small ink-jet printers, speakers, PDA cradles, etc.
- *Never* connect a laser printer to a UPS unit. A laser printer's fuser draws way more current than any UPS can provide.
- A separate UPS unit can be used to provide power to various office equipment other than computers, such as cordless phone base stations, cell phone chargers, clocks, radios, telephone answering machines, and small FAX machines.

- Batteries in brand-new UPS units typically last two or three years, but even brand-name replacement batteries seldom last more than 18 months. Worse, UPS battery-condition indicators simply cannot be trusted. It is a good practice to run a full-load power-failure test on each UPS every six months to determine its run time. You can use one or more light bulbs as a load if you wish.
- If you are really crazy about continuous power, you can consider buying a gasoline- or natural gas-powered generator to power your UPS during an extended power failure.

7.3 Privacy

Privacy is a small but important part of information security. There is no reason to accidentally share personal, confidential or business data with those who really don't need to know [3, 4, 5]. Doing so can increase your risk of identity theft, jealous acts, intellectual property theft, fraud, and so on.

Some simple tactics and a few accessories can help prevent accidental sharing of information:

- Password-protect all electronic devices (PDAs, computers, memory sticks, etc.).
- Don't leave opened mail or paychecks lying around.
- Don't face your PC's display screen towards windows or doorways.
- Use a password-protected screensaver that kicks in within a few minutes of inactivity.
- Shred all unwanted junk mail or statements relating to financial matters, to reduce risk of identity theft.
- Install a privacy filter on your computer display to prevent passers-by from seeing your screen.
- Hide all computer backup media.
- Don't mount whiteboards, drafting tables or prototypes so that they face doorways or windows.
- Encrypt files and e-mail attachments.
- Close office blinds, shades, curtains or drapes at night.
- Put extraneous paperwork into drawers before you leave your office to take lunch, attend a meeting or leave for home. This is called a "clean desk" policy.
- Turn off computers and other electronic devices at night.
- Lock your office, drawers and/or file cabinets when you leave the office.
- Make sure your online (web) accounts do not automatically log you in when you visit. Configure them to require you to enter a user ID and password every time.
- Don't leave your password list under your keyboard or in an unlocked drawer.
- And no exceptions for executive management!

Side note: Privacy addicts can learn a lot by looking into the field of *digital forensics* (a.k.a. *computer forensics*), which deals with ways to learn all about someone's computer or online activities. Practitioners in this field are often employed by prosecutors to obtain vital evidence by "digging into" someone's hard drive. Forensics investigators know that everyone produces a continuous, invisible, detailed and accurate electronic "paper trail" while using a computer to create documents, play games, surf the web. . .

7.4 Policies

One can best address data leaks, data loss and privacy issues by taking the time to write—and then enforce—specific information security policies.

Before writing these you will want to review Parts 2 and 3 of this White Paper. Several organizations mentioned in Part 3 offer useful security checklists that can supplement your policies.

Part 8

Glossary

Air Gap: A term used in the **network security** field, referring to the absolute isolation of one or more computers from any kind of external network (whether private or Internet, wireless or wired). **Worms** and other network-borne malware require some sort of network connection to propagate; they cannot cross an air gap.

Anti-virus: Originally, a type of software designed to locate and deactivate computer **viruses**. Today, "anti-virus" software typically recognizes several types of **malware**, not just viruses.

Attack: An attempt to gain unauthorized access to an information system. Sometimes an **attack vehicle** is employed during the attempt.

Attack Vehicle: A technological or other means to gain access to an information system. Commonly, **malware** such as **worms** and **spyware** are used as attack vehicles.

Bluetooth: A form of wireless network used by mobile devices such as cell phones, PDAs, laptop computers and even automobiles.

Botnet: An organized collection of **zombie** computers, possibly including thousands or tens of thousands of zombies.

Corporate Spy: A person hired by one company to provide inside information and/or to steal intellectual property from another company.

Cybercriminal: A person who commits a crime using computers and (usually) a network such as the Internet.

Decryption: The process of using a password as the basis for translating secret information from an undecipherable form to its original, normal form. Decryption is the reverse of **encryption**.

Denial of Service: A type of attack on a remote computer, usually characterized by a massive flood of network traffic aimed at that computer, which causes that computer to virtually cease network operations. This can be disastrous for businesses that rely on online shopping for much of their revenue.

Dictionary Attack: One of several automated or semi-automated password-cracking methods based on the use of word dictionaries for popular languages such as English or Spanish. For example, the password "maverick1975" would fall prey to a dictionary attack.

Distributed Denial Of Service: A **Denial of Service** attack simultaneously mounted by many computers on the Internet (usually members of a **botnet**).

Data Leak: An unauthorized or accidental disclosure of important information to a third party. A data leak can occur when a confidential document is stored on a public web server (which Google might find), or when incriminating **meta-data** is allowed to remain hidden inside a document (which special tools can extract).

Encryption: The reversible process of using a password as the basis for translating information into an undecipherable form to ensure secrecy. The reverse process is known as **decryption**. Some encryption methods are inherently weak, meaning that cryptographers can eventually perform decryption without knowing the password. Other encryption methods are strong, which is desirable.

Firewall: A software or hardware means to block certain types of network traffic while allowing other types to pass.

Hacker: A person with a passionate interest in learning and modifying the technical aspects of various things, typically electronic, mechanical, computer or software devices. "White Hat" hackers are those who find, report and possibly solve flaws and security vulnerabilities in products such as software. "Black Hats" find and exploit flaws and security vulnerabilities to boost their ego, and/or to engage in criminal activities for profit or for revenge.

Identity Theft: The criminal act of obtaining a victim's personal information so that purchases, transactions or other fraudulent actions can be accomplished in the victim's name (and at his risk).

Information System: Any type of system designed to store and process digital information. Includes desktop and notebook computers, smart phones, network storage devices, servers, etc. It also includes various digital products sold to end users (customers).

Information Security (InfoSec): The U.S. National Information Systems Security Glossary's definition is: "*The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats*". **Risk management** is the foundation on which information security rests.

InfoSec: An abbreviation for **Information Security**.

Keystroke Logger: **Malware**, usually of the **spyware** type, that logs every pressed key and then forwards that log to a **cybercriminal**. Keystroke loggers help cybercriminals discover vast amounts of personal information, such as user IDs, passwords, account numbers, etc.

Malware: **Mal**icious soft**ware** such as **worms**, **viruses**, **spyware**, **ransomware**, **Trojans** or **rootkits**.

Meta-data: Data that describes other data. Examples of meta-data include a disk file's time stamp, a JPEG file's image resolution, and a document's author. Verbose meta-data is often hidden inside disk files, allowing anyone with meta-data extraction tools to easily discover facts that the file's creator might consider highly confidential. See **data leak**.

Network Security: A subset of **Information Security** that deals specifically with securing private networks and/or Internet access.

Packet Sniffer: A **network security** software tool that reveals many low-level details of communications transmissions in wired or wireless networks. A packet sniffer allows one to see the exact contents of messages sent over a network.

Phishing: A **social engineering** technique that uses spam e-mail messages to dupe unsuspecting victims into providing **cybercriminals** with passwords, account information, etc.

Ransomware: A form of **malware** designed to take a victim's data hostage by encrypting every common type of data file stored on a victim's computer. After this is accomplished a ransom demand will be made known to the victim. Money is usually demanded in exchange for a decryption key with which to restore the victim's data.

Risk Management: The ongoing process of identifying risks and implementing mitigation plans to address them.

Rootkit: **Malware** that hides itself in a computer, obtains administrative privileges and then replaces some normal operating system functions with its own. Rootkits are undetectable by many experts and usually cannot be removed without destroying the operating system's ability to function normally. Rootkits have been traditionally used by **cybercriminals** to gain remote "super-user" access to a computer, but recently some companies like Sony have begun to use rootkits for Digital Rights Management purposes to control people's access to digital data such as software, music and movies.

Social Engineering: A new attack method designed to bypass technological security measures by using human psychology to trick people into letting a **cybercriminal** gain access to information systems. **Phishing** is an example of a social engineering technique.

Script Kiddie: A disparaging term for inexperienced **hackers** or budding **cybercriminals** who use other people's software to break into computers or to launch "**denial of service**" attacks on web servers. Most script kiddies haven't a clue about how such software works, and have no ability to write their own. Script kiddies usually launch their attacks on remote computers via the Internet.

Spyware: A form of **malware** that, with human assistance, gains entry to a computer through e-mail, web sites or application software. Therefore, spyware cannot infect a computer unless someone surfs the web, opens an e-mail attachment or installs application software.

Trojan: A free and appealing (or potentially useful) software program that actually contains **malware**. Trojan software was named after the legendary Trojan Horse of Greek mythology. A Trojan cannot infect a computer unless someone deliberately obtains and installs such software.

Virus: A form of self-replicating **malware** that, when activated, is able to attach copies of itself to nearby executable computer files. A virus becomes active only when its host file is executed (most often by humans). Hence viruses usually spread only with human help.

Wardriving: A hobby that involves driving around in a car with a Global Positioning System (GPS) unit and a wireless laptop, looking for **wireless access points**. Wardrivers usually feed their findings into massive online public databases of wireless access points (such as *wigle.net*). Your personal and/or corporate wireless access point locations can most likely be found in such databases. Yes, really.

Wireless Access Point: A piece of network equipment that forms a bridge between a normal, wired network (such as a private network or the Internet) and laptop computers, PDAs or other mobile devices.

Worm: A form of self-replicating **malware** that is able to automatically penetrate a remote computer on a network, by exploiting a vulnerability found within that computer's network-aware software. Once penetration is accomplished a worm will permanently install itself in its victim, and then immediately attempt to find other victims on the network. Worms do not need human help to propagate. Worms move fast; in 2003 the Slammer worm infected every vulnerable Internet-connected computer in the world within 15 minutes.

Zero-day Exploit: The exploit of a newly discovered security vulnerability within hours after the discovery of that vulnerability. The term "zero-day" refers to the practical inability of software vendors to provide security updates (patches) quickly enough to prevent a vulnerability from being exploited.

Zombie: An Internet-connected computer that was successfully attacked in a manner designed to place it under the remote control of a **cybercriminal**. Owners of zombies are usually unaware that their computers were compromised. Zombies commonly become members of a **botnet**.

References

[1] *2005 CSI/FBI Computer Crime and Security Survey* (Computer Security Institute and Federal Bureau of Investigation); Gordon, Loeb, Lucyshyn and Richardson.

[2] *Hacking Exposed Fifth Edition: Network Security Secrets & Solutions*; McClure, Scambray and Kurtz.

[3] *Geeks On Call Security and Privacy: 5-Minute Fixes*; Geeks On Call.

[4] *Computer Security for the Home and Small Office*; Thomas Greene.

[5] *The Art of Intrusion*; Mitnick and Simon.

[6] *Information Leakage Caused by Hidden Data in Published Documents* (IEEE Security & Privacy magazine); Simon Byers.

[7] *The Year of Breaches* ("News Track" item); Communications of the ACM.

[8] *The Windows Malicious Software Removal Tool: Progress Made, Trends Observed (June 2006)*; Rapid Response Team, Waggener Edstrom Worldwide.

[9] *Ohio Couple's "Destroyed" Hard Drive Purchased in Chicago* (plus similar news titles); WLWT-TV reporter Tom Sussi et al.

[10] *Security Company Recommends Macs* (http://www.toptechnews.com/story.xhtml?story_id=01100000AFT3)

[11] *Data losses may spark lawsuits* (eWEEK Magazine June 12, 2006); Matt Hines.

[12] *The Simple Economics of Cybercrimes* (IEEE Security & Privacy magazine); Nir Kshetri.

[13] *Learning from Information Security History* (IEEE Security & Privacy magazine); Dragos Ruiu.

[14] *Information Security* (http://en.wikipedia.org/wiki/Information_security); Wikipedia, The Free Encyclopedia.

[15] *An Introduction to Information Risk Assessment* (SANS Institute); Vishal Visintine.

[16] *GIAC Enterprises - Data Backup Security Policies and Procedures* (SANS Institute); Martin A. Reymer.

[17] *Password Management: Awareness and Training* (SANS Institute); Neil Witek.

[18] *Security Absurdity* (http://www.securityabsurdity.com/failure.php); Noam Eppel.

[19] *Microsoft Word Bytes Tony Blair in the Butt* (http://www.computerbyesman.com/privacy/blair.htm); Richard M. Smith.

[20] *Hidden Text Shows SCO Prepped Lawsuit Against BofA* (http://news.com.com/2100-7344_3-5170073.html); Stephen Shankland and Scott Ard.

[21] *Hidden Data in Electronic Documents* (SANS Institute); Deborah Kernan.

[22] *FBI busts alleged DDoS Mafia* (http://www.securityfocus.com/news/9411); Kevin Poulsen.

[23] *20 Years after the Hostages: Declassified Documents on Iran and the United States* (http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB21/); The National Security Archive of The George Washington University (edited by Malcolm Byrne).

[24] *H-P CEO's merger comments surface* (http://www.washtimes.com/upi-breaking/10042002-070323-8042r.htm); The Washington Times.

[25] *Internet security journalist hacks Saddam's e-mail* (http://www.showmenews.com/2002/Nov/20021124News014.asp); The Associated Press.

[26] *Risk Management Guide for Information Systems* (Special Publication 800-30); National Institute of Standards and Technology.

[27] *ActiveX: Or how to put nuclear bombs in web pages* (http://www.halcyon.com/mclain/ActiveX/); Fred McLain.

[28] *The Many Facets of an Information Security Program* (SANS Institute); Robert L Behm, Jr.

[29] *Sophos Security Report reveals Trojan domination in first half of 2006; Malware statistics suggest it is time for home users to switch to Macs* (http://www.sophos.com/pressoffice/news/articles/2006/07/securityreportmid2006.html); Sophos Plc.

[30] *The Complete Social Engineering FAQ!* (http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt); Unknown.

[31] *Safe Personal Computing* (http://www.schneier.com/blog/archives/2004/12/safe_personal_c.html); Bruce Schnier.

[32] *Rootkits, Part 1 of 3: The Growing Threat*; McAfee, Inc.

[33] *Inside the Slammer Worm* (IEEE Security & Privacy magazine); Moore, Paxson, Savage, Shannon, Staniford and Weaver.

[34] *Remembrance of Data Passed: A Study of Disk Sanitization Practices* (IEEE Security & Privacy magazine); Garfinkel and Shelat.

[35] *The State of Information Security 2004: Best Practices* (CIO Magazine); Ware.

[36] *The Curse of the Secret Question* (http://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html); Bruce Schneier.

[37] *Spyware Researchers Discover ID Theft Ring* (http://www.eweek.com/article2/0,1895,1845248,00.asp); Ryan Naraine.

[38] *Computer theft in businesses becoming a growth industry* (The Associated Press) (http://www.crime-research.org/news/2003/11/Mess2901.html); Mark Niesse.

[39] *Confessions of a corporate spy* (Computerworld magazine) (http://www.computerworld.com/securitytopics/security/story/0,10801,100252,00.html); Gary Anthers.