realtimepublishers.com™

The Definitive Guide™ To

Information Theft Prevention

permeo™

Dan Sullivan

Introduction to Realtimepublishers

by Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical technology topics—at no cost to the reader. Although this feat may sound difficult to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading is the equivalent of any similar printed book you might find at your local bookstore—with the notable exception that it won't cost you $30 to $80. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions or the release of a new edition possible in a far shorter timeframe than is the case with conventional printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create "dream team" projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please send an email to feedback@realtimepublishers.com, leave feedback on our Web site at http://www.realtimepublishers.com, or call us at 800-509-0532 ext. 110.

Thanks for reading, and enjoy!

Sean Daily
Founder & Series Editor
Realtimepublishers.com, Inc.

Copyright Statement

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note**: This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit http://www.realtimepublishers.com/contentcentral/.]

Chapter 1: Evolving Threat of Information Theft

The famed American bank robber Willie Sutton once said he robbed banks because that is where the money was. Today's thieves do not have to leave their desk chair; they steal from computers because that is where the information is and some of that information is quite valuable. Consider the types of information available in compromised systems:

- Personally identifying information, such as Social Security numbers, credit card numbers, and bank account numbers
- Intellectual property, including product designs and copyrighted material
- Strategic business plans with details about product launches, marketing campaigns, and mergers
- Protected personal information such as healthcare histories

The inadvertent release of proprietary and confidential information can have costly and immediate consequences, ranging from regulatory fines and lost business opportunities to damage to brand and loss of customer confidence. A host of factors are resulting in an increasing threat of information theft, including:

- Increased amounts of sensitive data
- The changing economics of hacking and cybercrime
- Increased systems complexity and accompanying vulnerabilities
- Increased use of devices outside the control of a business' IT department, such as customer PCs and business partners' mobile devices

When an incident of information theft occurs, the impact is not limited to IT operations but can affect a company's brand and its financial and market position as well as bring on unwanted legal consequences. This chapter examines the changes in information technology (IT) use that have given rise to a new form of hacking and information theft and concludes with an introduction to the security industry's response to these new threats—on-demand security.

Increasing Amounts of Sensitive Information

It is not news to say the amount of information is growing. One study estimates that information in all forms grows at a rate of 800MB per person per year. On the Internet, Yahoo indexes more than 20 billion objects (as of August 2005), including 19.2 billion Web documents, 1.6 billion images, and more than 50 million audio and video files. And much useful information is still not in electronic form; in the United States, for example, federal government officials are promoting electronic medical records as a way to save as much as 20 percent of healthcare costs.

> 📖 For details about information growth, see the University of California, Berkeley study entitled "How Much Information? 2003" at http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#summary.

From a computer-security perspective, the prime concern that results from this information explosion is not just the volume of data but also the volume of sensitive information.

Rising Concern About Sensitive Information

Sensitive information is any information that requires restricted access. If the information is disclosed or changed, harm can result. This definition spans a wide range of topics, including:

- Personal financial information
- Corporate financial and performance information
- Classified and confidential government data
- Healthcare information
- Intellectual property

Banks, credit card companies, and merchants pay when personal financial information is compromised and credit card fraud is committed. The share price of public companies can be adversely impacted if information is disclosed prematurely or out of context. This disclosure might also give competitors an advantage in certain situations. The loss of classified and confidential government data can compromise public safety and national security. Disclosing protected healthcare information violates an individual's privacy as well as federal regulations. Losing control of trade secrets or other intellectual property can have devastating consequences, especially for small firms with limited product lines.

The impact of inadvertent disclosures can be difficult, or even impossible, to overcome. Consider CardSystems, a merchant credit card payment processing service whose compromised systems exposed data for more than 40 million credit card and debit card accounts in May 2005. American Express and Visa U.S.A dropped the company as a transaction provider and refused to engage in business with the firm even after the firm underwent a successful audit of its payment card industry (PCI) data security compliance. The firm's assets were sold to another company in the fall of 2005.

> 🕮 For more information about the rapid demise of CardSystems, see "Credit Cards Bar CardSystems" at http://www.redherring.com/Article.aspx?a=12823&hed=Credit+Cards+Bar+CardSystems and "CardSystems Bought (Again)" at http://www.redherring.com/Article.aspx?a=14028&hed=CardSystems+Bought+(Again).

The threat of security breaches and the loss of confidential information are not limited to financial services companies and startups. The rising concern about controlling sensitive information is well documented across industries:

- According to the 2004 Ernst & Young Global Information Security Survey, 66 percent of security executives surveyed cited loss of private customer data as a high or very high level of concern.
- The 2004 Deloitte Global Security Survey found 44 percent of respondents acknowledged managing third-party information sharing as a top concern for privacy compliance.
- Losses due to the theft of proprietary information rose sharply in 2005 with an average financial loss of $355,552 per respondent according to the 2005 CSI/FBI Computer Crime and Security Survey; in 2004, the average loss per respondent was $168, 529.

As the amount and value of online information increases, so too does the need to protect that information. Moreover, you must not assume that partial information or small amounts of confidential information are insignificant and not worth protecting.

Combing Pieces of Information

An attacker does not need to break into a network server the night before a board meeting to steal a copy of the company's strategic plan. In fact, that may not be the best method. Systems administrators and security professionals have formulated best practices for securing information on managed devices—that is, on devices they control. However, there are still vulnerabilities and best practice implementations are never perfect, but they have raised the cost of accessing well-managed information. Instead of attacking a server directly—the networking equivalent of walking in the front door—intruders can use less obvious methods.

One approach is to compile information from multiple sources. This method of attack is especially problematic when there is significant information leakage. Information leakage occurs when pieces of information are revealed or left unprotected. An attacker does not need a complete description of a plan, a design, a forecast, or other aggregate piece of information. Examples of information leaks include:

- A page of a spreadsheet used to derive quarterly revenue projections left in the browser cache on a hotel business center computer
- A printed email indicating a question about production volumes left in a printer at a public copying center
- Instant messages about an upcoming public announcement transmitted over an unencrypted wireless network in a coffee shop and picked up by a wireless eavesdropper
- Files left on a former file server that has been redeployed as a Web server, allowing the files to be found using Google hacking techniques

> 📖 Google hacking is a technique for using the popular search engine to find information leaks and vulnerable servers. For more information about how the technique works and how to protect your servers, see Johnny Long's "Google Hacking Mini-Guide" at http://www.informit.com/articles/article.asp?p=170880&rl=1 or read *Google Hacking for Penetration Testers* (Syngress, 2005) by the same author.

A piece of information here and there may not sound too damaging, but it can be. Consider the practice of competitive intelligence (CI). Essentially, CI is the practice of gathering information about competitors by using public information and legal methods. CI professionals have used a wide variety of sources, including:

- Company Web sites and press releases
- News sources
- Local government records, such as building permits
- SEC filings
- Regulatory actions
- Lawsuits
- Patent office records

From these sources, competitors can create broad and deep profiles of companies. If one were to add confidential information that was inadvertently leaked to these detailed profiles, the threat could be magnified substantially.

The two broad types of information leakage are the loss of company confidential information and the disclosure of protected private information. The former can result in competitive disadvantages from the loss of trade secrets and proprietary processes. The latter can result in regulatory consequences as well as a loss of customer confidence and brand damage. The first step to protecting corporate and personal information is to understand its value to the organization and the appropriate level of confidentiality required to protect that information.

Varying Classifications of Information

Information is categorized in many ways. Companies have information about customers, inventory levels, production schedules, and sales quotas. The same data could be grouped according to financial groupings as it relates to income, expenses, and assets. For security purposes, the common designations are

- Public
- Sensitive
- Private
- Confidential

Each of these designations dictates a different level of protection. Public information can be disclosed without adversely affecting an organization or its customers, clients, or other stakeholders. Public information includes both information that is intended for public distribution, such as press releases, and operational information that is not necessarily intentionally disclosed to the public, such as the number of persons working in an office or a shipping schedule.

Sensitive data requires special protection to ensure confidentiality and integrity; its disclosure could cause moderate harm to the organization. Sensitive data includes marketing plans, sales forecasts, customer contact databases, and financial information.

Personal information is for use within a company, and its disclosure could harm persons working or otherwise involved with the organization. For example, a disciplinary finding against an employee would be considered private.

Confidential information is highly valuable to an organization and requires the greatest level of care to ensure that it is not disclosed or tampered with. Trade secrets, proprietary processes, strategic plans, and other competitively valuable information falls into this category. Categorizing various information types depends on several criteria.

Information Categorization Criteria

Information is categorized according to several measures, such as

- Usefulness of information to its owner and its competitors
- Timeliness of information
- Cost of damage done by disclosure of the information
- Cost of damage caused by altering the information
- Regulatory requirements

This list is not exhaustive but outlines the major elements of a categorization scheme.

Information Usefulness

Some information is useful to both owners and competitors, such as a list of sales prospects. In other cases, information that is valuable to its owner, such as a detailed project plan, may be of greater value to the owner than to others but is still of interest to competitors. Highly valuable information to both a company and its competitors is confidential, while information with asymmetric value to owners and competitors would fall into the sensitive category.

Other information is essentially useless outside of an organization. For example, a list of parking assignments or a notice about construction in the office is of little interest to outsiders. This information would be classified as public.

A common problem is that information that falls into different categories may be stored together. Public documents may be kept on the same network share as company confidential or private information. A Human Resources (HR) manager, for example, may have a document with employee names and telephone extensions (public information) in the same directory as a spreadsheet with salaries (private information) and a memo on the impact on staff of a proposed merger (confidential). As long as file permissions are set appropriately on confidential and private information, this setup is not a problem; vulnerabilities arise, however, when a file is added under the assumption that directory-level permissions are adequate to protect the information.

Training staff on information classification and best practices for dealing with private and confidential information can help to reduce the chance of an information leak. For example, private and confidential information should be located in tightly controlled directories. This setup reduces the opportunity for an unauthorized user to copy, modify, or delete protected information. Public information may be stored in those directories, but that information would then be protected at the stricter levels dictated by the most sensitive information in the directory.

Information Timeliness

Another consideration is timeliness. Having access to a United States Federal Reserve decision to change the discount rate (which is tied to interest rates charged by banks) is extremely valuable prior to the Federal Reserve's public announcement; after the announcement the information is public, and although still valuable, does not provide a competitive advantage. Similarly, an 18-month old sales and prospect list may still be of use to a competitor; however, it is worth significantly less than a current list. The level of protection maintained on information should change according to the current value, not its original value.

One must also consider how quickly the value of information can change. For example, a press release about a merger, unusual price earnings, or strategic chance must be treated as confidential prior to its release. After the release, it should be treated as public information.

Cost of Disclosure

The cost of damage as a result of disclosure can be difficult to measure. Would the entire value of a company plummet if a trade secret were revealed? If the trade secret is about a process used to produce a patent-protected product, competitors could not use the information to legally duplicate the protected product. Perhaps after the patent expires, the information could be of use to competitors. In other cases, the process itself may be adopted for use with other products produced by competitors. In these cases, there may be some detrimental, indirect affect on the owner of the trade secret value.

In other cases, the loss of a trade secret could be devastating. Consider an engineering firm that develops a signal-processing algorithm that enhances the reliability and speed of wireless networks. Rather than apply for a patent, which requires public disclosure, the company decides to maintain the algorithm as a trade secret. In this case, the company has no protection other than its ability to keep the algorithm secret. Clearly, the value of that information is a function of the marginal revenue the company will realize for as long it maintains a monopoly on that technique.

Regulatory Requirements

Government regulations controlling the confidentiality and integrity of data can carry stiff financial penalties for violations. Regulations sometimes require public disclosure of a security breach. For example, California law SB 1386 requires that California residents be notified if private financial information may have been disclosed during a security breach. Table 1.1 lists well-publicized cases of security breaches resulting in the disclosure of private information (the table is in descending order based on the number of incidents).

Name	Category	Number of Incidents	Date
Georgia Technology Authority (Driver's License Data)	Other	Hundreds of thousands	4/28/2005
MasterCard International	Financial	40,000,000	6/17/2005
CitiFinancial	Financial	3,900,000	6/6/2005
North Carolina Division of Motor Vehicles	Other	3,800,000	2/10/2005
DSW Shoes	Other	1,400,000	3/8/2005
Bank of America	Financial	1,200,000	2/25/2005
Medical Health Plans, Minnetonka, MN	Healthcare	1,200,000	6/14/2005
Wachovia, Bank of America, PNC Bank of Pittsburg, Commerce Bank	Financial	680,000	4/28/2005
Time Warner	Other	600,000	5/2/2005
Reed Elsevier, Seisint Unit (LexisNexis)	Other	310,000	3/9/2005
University of Southern California	Education	270,000	7/8/2005
Ameritrade	Financial	200,000	4/19/2005
GMAC Financial Services	Financial	200,000	1/26/2005
San Jose Medical Group	Healthcare	185,000	3/28/2005
Polo Ralph Lauren / HSBC North America	Other	180,000	4/13/2005
University of Hawaii	Education	150,000	6/17/2005

Table 1.1: Institutions with publicly disclosed security breaches in 2005 involving personally identifying information (Source: Permeo Technologies).

Public disclosures of security breaches have non-quantifiable effects on brand and company image in addition to any regulatory fines and related penalties that may be imposed.

Information is valuable. Companies protect stakeholders by protecting information. Governments protect citizens, businesses, and other organizations by regulating information integrity and confidentiality. Cybercriminals, industrial saboteurs, and others operating outside the law have much to gain by circumventing those protections.

The Changing Economics of Hacking and Cybercrime

The stereotypical image of a lone programmer hacking away to deface a Web site or deploy a virus that damages PCs is out of date. Hacking is no longer the province of vandals who are intent to prove their technical prowess. Economic incentives are now a driving force behind security breaches. Identity theft is one of the most common forms of cybercrime and is growing in severity.

Identity Theft

Identity theft is the crime of stealing another person's private information and using it to commit fraud. Three aspects of this type of crime include:

- The theft of personal information
- The use of stolen information for fraud
- The impact of identity theft

Stealing Personally Identifying Information

Stealing personal information is surprisingly easy. As Table 1.2 shows, there are many ways to collect personal information. One of the growing methods is, of course, the Internet. Although other methods, such as stealing or redirecting mail, can be performed relatively easily, Internet-based thefts can yield high volumes of identities. As Table 1.1 illustrated, the number of exposed identities in a computer security breach can easily reach into the hundreds of thousands and even millions of victims per breach.

Source	2003	2004	Percentage Change
Friend or family member	7.3	39.4	439.73%
Mail	0.6	10.6	1666.67%
Internet	3.7	5.3	43.24%
Wallet/Palm Pilot	6.1	4.5	-26.23%
Home/car by thief	10.4	3.8	-63.46%
College records	2.4	3	25.00%
Scam	0	2.3	
Work	3	1.5	-50.00%
Fraudulent address change	4.3	1.5	-65.12%
Trash	0.6	0	-100.00%
Other	61.6	28	-54.55%
Total	100	99.9	

Table 1.2: Stolen information comes from multiple avenues (Source: Identity Theft: The Aftermath 2004 by Identity Theft Resource Center).

Fraudulent Use of Identity Information

Victims of identity theft may find unexplained charges on their credit card bills, their mail has been forwarded to another address, phone or wireless services have been established in their names, car loans have been taken out in their names, or even that bankruptcy proceedings have been filed under their names. The most common types of fraud are credit card fraud, phone and utilities fraud, bank fraud, and employment fraud, Tables 1.3 through 1.5 show a further breakdown of the types of fraud in each of these categories (employment fraud is not further divided into sub-types).

> 📖 This data is from the Federal Trade Commission (FTC) "National and State Trends in Fraud & Identity Theft January - December 2004" available at http://www.consumer.gov/idtheft/pdf/clearinghouse_2004.pdf.

Credit Card Fraud	**Percentage of Complaints**		
	2002	2003	2004
New Accounts	24.4	19.3	16.5
Existing Accounts	12.2	12	11.9
Unspecified	5.4	1.4	0.1
Total	41	32	28

Table 1.3: Breakdown by sub-types of credit card fraud.

Phone and Utilities Fraud	**Percentage of Complaints**		
	2002	**2003**	**2004**
Wireless - New	10.6	10.4	10
Telephone - New	5.2	5.6	5.9
Utilities - New	3	3.8	4.2
Unauthorized Changes to Existing Accounts	0.7	0.6	0.7
Unspecified	2.2	0.8	0.3
Total	20	19	19

Table 1.4: Phone and utilities fraud subtypes.

Bank Fraud	Percentage of Complaints		
	2002	2003	2004
Existing Accounts	8.10	8.30	8.50
Electronic Fund Transfers	3.10	4.50	6.60
New Accounts	3.70	3.50	3.60
Unspecified	2.00	0.50	0.10
Total Bank Fraud	16.00	17.00	18.00

Table 1.5: Victim's information is used for several different forms of bank fraud.

Impact of Identity Theft

The impact of identity theft is measurable and severe. The consequences of identity theft strike both individuals and businesses:

- According to the United States FTC, identity theft cost business $47.6 billion, or $4800 per victim, in 2002.
- Another study, by the Identity Theft Resource Center, found the average fraudulent charges reached $90,000 per stolen identity in 2003.
- 67 percent of all identity theft victims said they have had existing credit cards misused, according to the FTC.
- Victims now spend, on average, 600 hours clearing their credit ratings after identity theft.

This volume of criminal activity attracts more than the lone attacker selling credit card number lists to the highest bidder. For example, the United States Department of Justice (DoJ) indicted 19 members of Shadowcrew, a group that founded and operated the Web site http://www.shadowcrew.com, which sold stolen identity information, credit card numbers, and debit card numbers. Prior to their arrest, the group had sold 1.5 million credit card numbers resulting in $4 million in fraudulent charges.

> 📖 For more information about Shadowcrew's crimes see "Shadowcrew: Web Mobs" at http://www.baselinemag.com/article2/0,1397,1774393,00.asp. And "Nineteen Individuals Indicted in Internet 'Carding' Conspiracy" at http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm.

The growing costs are indicative of the success of identity thieves, but they are not the only perpetrators of cybercrime.

Industrial Espionage

Industrial espionage—that is, spying on competitors or using other illegal means to gain market or financial advantage on a company—is not a new phenomenon. Two well-known examples are:

- The development of the Soviet supersonic jet, Tupolev TU-144, which relied on stolen plans for the French-British Concorde. In 1965, a Soviet agent was arrested in Paris in possession of designs for the landing gear, braking system, and airframe of the Concord. The Tupolev looked so much like the French-British supersonic, it was nicknamed the "Concordski."
- The United States government has admitted to using phone-call surveillance to discover evidence of a French competitor to an American company using bribery to win an air traffic control equipment bid with Brazilian officials.

The practice of industrial espionage is widespread and costly. A 1992 study by the American Society for Industrial Security found the most damaging types of information stolen were pricing information, manufacturing process information, and product development and specification information. By 2004, the top targets of foreign firms and governments were information systems, sensors, military systems, and electronics. The FBI estimates that United States firms loose $100 billion annually to industrial espionage. Clearly, the threat of information theft from competitors is a genuine and potentially costly threat.

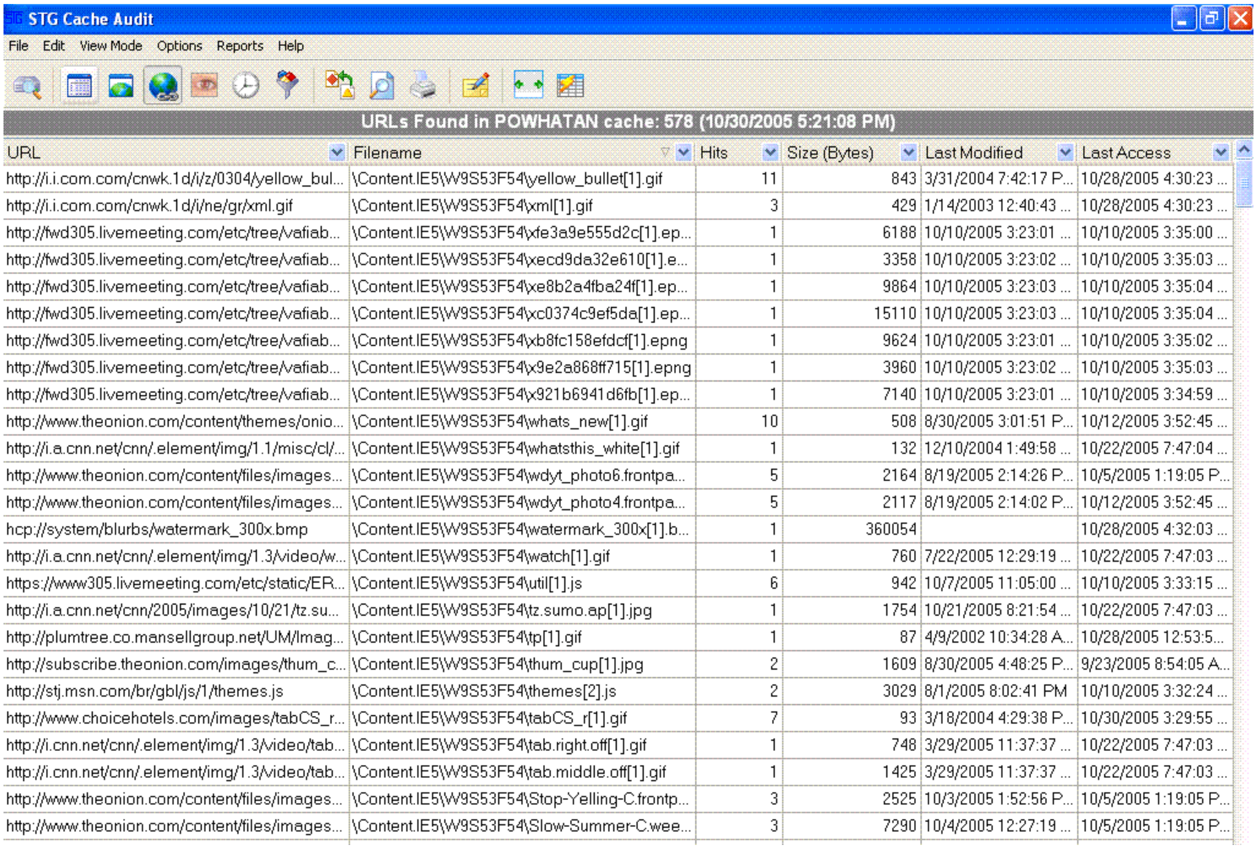
There are many methods for conducting industrial espionage:

- Direct request
- Solicitation of marketing services
- Exploitation of relationships
- Internet-based activities, such as information theft

By some estimates, as much as 70 percent of information theft is conducted by people with legitimate access to at least some information in a company—for example, employees, consultants, and contractors. In the past, a competitor might try to recruit a mole within the company or, in the case of the Tupolev-Concorde case, get their own agent access within the company. The perpetrator would then use access to facilities to collect and steal information. The pattern is still the same, but with wide-scale Internet access, the methods have advanced.

Internal resources with legitimate access do not have to be in close physical proximity to the information they want to steal. Files can be copied from anywhere in the world using file transfer protocol (FTP). Trojan horse programs can be left to activate after the perpetrator has left the company to transmit the stolen information.

Other methods for industrial espionage are emerging with the increasing use of unmanaged devices. For example, users can easily discover contents left in memory buffer caches of shared computers found in hotel business centers. With easily obtained programs, another user can find the URLs of recently visited sites (see Figure 1.1).



URLs Found in POWHATAN cache: 578 (10/30/2005 5:21:08 PM)

URL	Filename	Hits	Size (Bytes)	Last Modified	Last Access
http://i.i.com.com/cnwk.1d/i/z/0304/yellow_bul...	\Content.IE5\W9S53F54\yellow_bullet[1].gif	11	843	3/31/2004 7:42:17 P...	10/28/2005 4:30:23 ...
http://i.i.com.com/cnwk.1d/i/ne/gr/xml.gif	\Content.IE5\W9S53F54\xml[1].gif	3	429	1/14/2003 12:40:43 ...	10/28/2005 4:30:23 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\xfe3a9e555d2c[1].ep...	1	6188	10/10/2005 3:23:01 ...	10/10/2005 3:35:00 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\xecd9da32e610[1].e...	1	3358	10/10/2005 3:23:02 ...	10/10/2005 3:35:03 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\xe8b2a4fba24f[1].ep...	1	9864	10/10/2005 3:23:03 ...	10/10/2005 3:35:04 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\xc0374c9ef5da[1].ep...	1	15110	10/10/2005 3:23:03 ...	10/10/2005 3:35:04 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\xb8fc158efdcf[1].epng	1	9624	10/10/2005 3:23:01 ...	10/10/2005 3:35:02 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\x9e2a868ff715[1].epng	1	3960	10/10/2005 3:23:02 ...	10/10/2005 3:35:03 ...
http://fwd305.livemeeting.com/etc/tree/vafiab...	\Content.IE5\W9S53F54\x921b6941d6fb[1].ep...	1	7140	10/10/2005 3:23:01 ...	10/10/2005 3:34:59 ...
http://www.theonion.com/content/themes/onio...	\Content.IE5\W9S53F54\whats_new[1].gif	10	508	8/30/2005 3:01:51 P...	10/12/2005 3:52:45 ...
http://i.a.cnn.net/cnn/.element/img/1.1/misc/cl/...	\Content.IE5\W9S53F54\whatsthis_white[1].gif	1	132	12/10/2004 1:49:58 ...	10/22/2005 7:47:04 ...
http://www.theonion.com/content/files/images...	\Content.IE5\W9S53F54\wdyt_photo6.frontpa...	5	2164	8/19/2005 2:14:26 P...	10/5/2005 1:19:05 P...
http://www.theonion.com/content/files/images...	\Content.IE5\W9S53F54\wdyt_photo4.frontpa...	5	2117	8/19/2005 2:14:02 P...	10/12/2005 3:52:45 ...
hcp://system/blurbs/watermark_300x.bmp	\Content.IE5\W9S53F54\watermark_300x[1].b...	1	360054		10/28/2005 4:32:03 ...
http://i.a.cnn.net/cnn/.element/img/1.3/video/w...	\Content.IE5\W9S53F54\watch[1].gif	1	760	7/22/2005 12:29:19 ...	10/22/2005 7:47:03 ...
https://www305.livemeeting.com/etc/static/ER...	\Content.IE5\W9S53F54\util[1].js	6	942	10/7/2005 11:05:00 ...	10/10/2005 3:33:15 ...
http://i.a.cnn.net/cnn/2005/images/10/21/tz.su...	\Content.IE5\W9S53F54\tz.sumo.ap[1].jpg	1	1754	10/21/2005 8:21:54 ...	10/22/2005 7:47:03 ...
http://plumtree.co.mansellgroup.net/UM/Imag...	\Content.IE5\W9S53F54\tp[1].gif	1	87	4/9/2002 10:34:28 A...	10/28/2005 12:53:5...
http://subscribe.theonion.com/images/thum_c...	\Content.IE5\W9S53F54\thum_cup[1].jpg	2	1609	8/30/2005 4:48:25 P...	9/23/2005 8:54:05 A...
http://stj.msn.com/br/gbl/js/1/themes.js	\Content.IE5\W9S53F54\themes[2].js	2	3029	8/1/2005 8:02:41 PM	10/10/2005 3:32:24 ...
http://www.choicehotels.com/images/tabCS_r...	\Content.IE5\W9S53F54\tabCS_r[1].gif	7	93	3/18/2004 4:29:38 P...	10/30/2005 3:29:55 ...
http://i.cnn.net/cnn/.element/img/1.3/video/tab...	\Content.IE5\W9S53F54\tab.right.off[1].gif	1	748	3/29/2005 11:37:37 ...	10/22/2005 7:47:03 ...
http://i.cnn.net/cnn/.element/img/1.3/video/tab...	\Content.IE5\W9S53F54\tab.middle.off[1].gif	1	1425	3/29/2005 11:37:37 ...	10/22/2005 7:47:03 ...
http://www.theonion.com/content/files/images...	\Content.IE5\W9S53F54\Stop-Yelling-C.frontp...	3	2525	10/3/2005 1:52:56 P...	10/5/2005 1:19:05 P...
http://www.theonion.com/content/files/images...	\Content.IE5\W9S53F54\Slow-Summer-C.wee...	3	7290	10/4/2005 12:27:19 ...	10/5/2005 1:19:05 P...

***Figure 1.1: Widely available tools, such as STG Cache Audit, allow users with even limited technical skills to quickly gather substantial amounts of information about what other users have referenced*.**

This ability to access information does not appear too threatening at first glance. After all, the fact that a salesperson looks up a company on Hoovers, Factiva, or other business intelligence sites is not all that revealing. However, that piece of information along with

- A copy of a spreadsheet with calculations used in a proposal
- A list of URLs to a company's document management system, which have path names that include prospect's names
- An email message with a prospect's contact information found by clicking the back button on the browser

This combination of information begins to paint a more revealing picture of the previous user's business.

> 📖 For more information about industrial espionage, see "Case Study of Industrial Espionage through Social Engineering" by Ira S. Winkler at http://www.simovits.com/archive/socialeng.pdf. See also, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004" at http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnualreport_2004_NoCoverPages.pdf.

Someone does not need to break into a company's vault and steal the plans for the next great invention to commit industrial espionage. The potential for leaking information is high. The ability of competitors to amass many pieces of public information is great. Together, these techniques can combine to create a mosaic of diverse pieces of data that present information that can be greater than simply acquiring the individual pieces.

The increasing value of information will continue to make it a target of industrial espionage. The ability to commit industrial espionage through the use of IT, either as a primary tool or as an adjunct to traditional methods, will continue and probably increase as cybercriminals become more proficient with the use of malicious programs to conduct industrial espionage.

Targeting Information

The Economist estimates that as much as 75 percent of the value of publicly traded companies in the United States is comprised of intangible assets—a substantial increase over the 40 percent estimated value of the 1980s. These are not just academic reflections on the evolving categorization schemes of corporate assets. Intellectual property directly generates substantial revenues. Consider the following examples:

- IBM earns $1 billion per year from intellectual property
- Hewlett-Packard licenses more than $200 million worth of intellectual property annually
- 54 percent of companies in a McKinsey survey found licensing revenues increasing 10 percent to 50 percent between 2000 and 2002
- 75 percent of executives surveyed expect to buy and sell more licenses over the next 2 to 5 years.

📖 For more information about the market value of intellectual property, see "A Market for Ideas: A Survey of Patents and Technology" (*The Economist*, October 22, 2005).

With the clear value of intellectual property, it is not surprising to find malware targeted at stealing information. Myftp, a worm discovered in August 2004, spreads through poorly secured network shares by authenticating as an administrator using a list of weak passwords. Once in place, the worm copies Microsoft Word, Adobe Acrobat, Microsoft Access databases, and a few types of computer aided design (CAD) files to an FTP site where the attacker presumably retrieves the pilfered files.

Although this malware type is clearly dangerous, many misjudge its reach. After all, the files have to be copied somewhere; one simply needs to find that place. Clearly, copying files to one FTP server presents a potential single point of failure if that server were shutdown. Attackers may try to hide the ultimate destination by redirecting traffic, but with enough effort, the final destination can be determined.

Not to be left vulnerable to such an obvious weakness, cybercriminals are developing more sophisticated techniques, such as malicious peer-to-peer networks, like Stint, a Trojan horse program that gives attackers control of a compromised machine and allows for later download of specialized payloads for attacks, such as searching for particular file types. Encrypted communications are used to further thwart detection.

The same type of co-evolution that occurs with viruses and antivirus software is taking place with cybercrime in general. Attackers exploit a vulnerability; security professionals identify and correct the problem while developing general solutions to a broad category of threats. The cybercriminals then devise another way to exploit systems, hide their tracks, or outmaneuver current countermeasures, and the cycle continues.

Preventing cybercrime is one benefit of sound security policies and procedures. Those policies and procedures often include detailed plans for controlling access to devices; limiting access to files, databases, and other resources; and ensuring that significant events, such as log in failures or database record changes, are recorded for audit purposes. Implementing these controls is feasible when the devices are managed within an organization—a situation that is no longer always the case for many organizations.

Increasing Use of Unmanaged Devices

When considering network security and Web-based applications, it is useful to distinguish managed and unmanaged devices. First, consider managed devices. Servers, routers, disk arrays, and tape drives are staples of IT computing centers. These devices are physically isolated, often in controlled environments, to limit physical access to system managers and other IT personnel with a need to work directly on the hardware. In addition, these devices use logical controls, such as authentication mechanisms and access control lists (ACLs) to restrict operational access to the systems. Desktops, laptops, and sometimes mobile devices can be similarly controlled. These are all examples of managed devices.

One of the benefits of the Internet is that it provides the ability to access remote devices. Systems administrators and developers have long enjoyed the flexibility of working on remote servers with applications such as UNIX’s remote shell program (rsh) and remote execute program (rexec). Now, IT organizations can allow access to any Web-enabled application, including back-office systems such as order processing and inventory management. Unfortunately, opening networks and applications to devices outside of the control of one’s IT group brings with it a host of new potential problems. The challenges faced when having to contend with managed devices are amplified with unmanaged devices.

The Extended Perimeter

The traditional network perimeter was defined by the outermost firewall. Demilitarized zones (DMZs) are created with a firewall with multiple network interface cards (NICs). One NIC controls traffic between the Internet and the DMZ and the other controls traffic between the DMZ and the internal network. Devices and servers needing the most security, such as databases and file servers, were maintained within the internal network. Devices that could be exposed to Internet traffic, such as Web servers, were placed inside the DMZ, as Figure 1.2 shows.

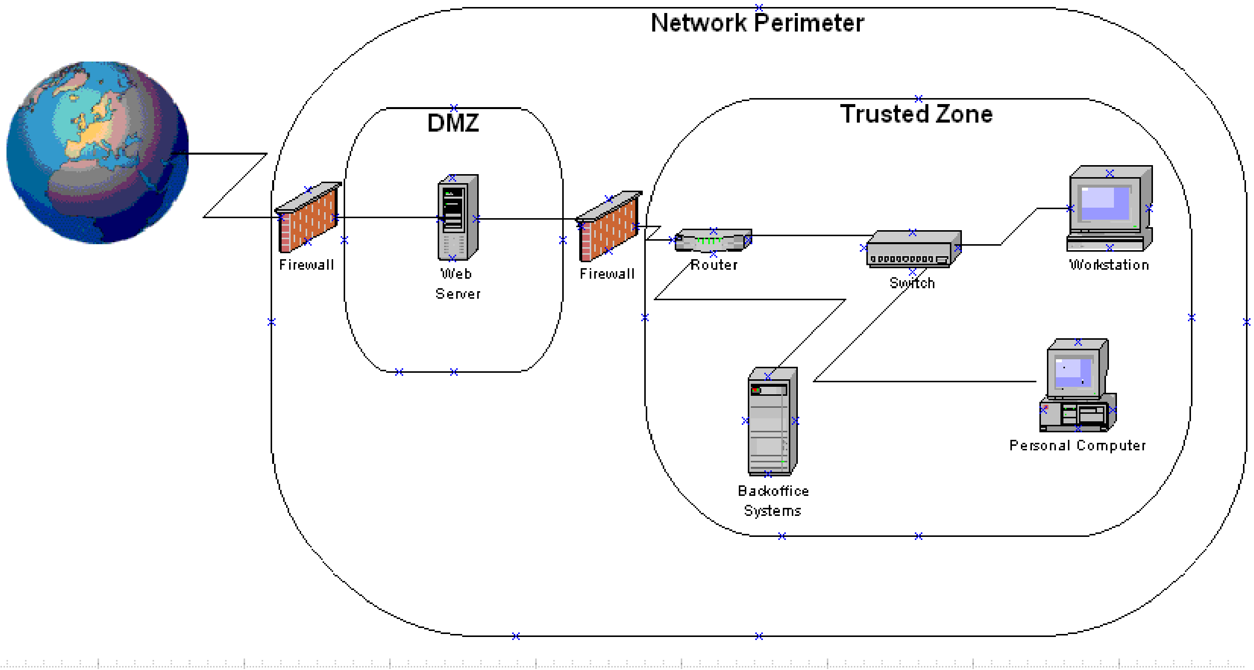


Figure 1.2: Well-defined network perimeters separated devices according to the level of security needed to protect the asset.

This type of network architecture is still popular and continues to meet the needs of many organizations. However, there is also growing demand for more flexible, broader access to information. Business drivers to open access to internal computing services and resources are coming from a range of potential users:

- Business partners
- Remote users
- Telecommuters
- Customers
- Branch offices
- Mobile workers

The perimeter can be extended to reach these users, as Figure 1.3 shows, but it is worth noting some differences between the types of control systems administrators will have to employ to secure the extended perimeter.

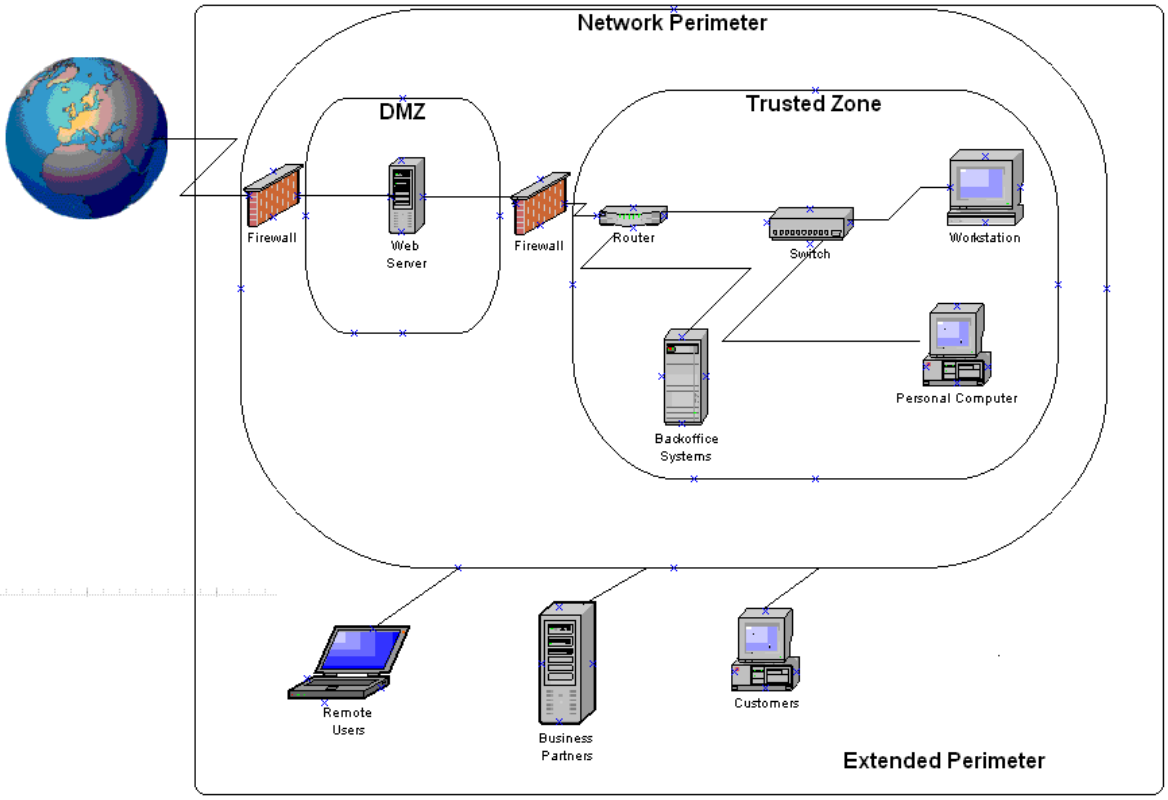


Figure 1.3: The extended perimeter includes both long-term and short-term users with varying needs to different information and resources.

Security Objectives

The security objectives in an extended perimeter environment are the same as in any network:

- Confidentiality
- Integrity
- Availability

If you are to realize the operational benefits of extending trusted network access, you must ensure these objectives are met.

Confidentiality

Confidentiality ensures that information is not shared with unauthorized users. Systems and network administrators use access controls, such as file permission and user accounts with passwords, to provide confidentiality of information stored on managed devices. Information transmitted outside of trusted zones may be encrypted so that even if someone were to intercept communications, it would not be intelligible.

> Encryption cannot guarantee that someone will never discover the original message given the encrypted version. Encryption algorithms and keys are generally chosen to balance the need for efficient processing (strong encryption takes longer than weak encryption) with the need for confidentiality. What was once considered reasonably "unbreakable"—such as the 56-bit DES encryption algorithm—can now be easily cracked. New algorithms, such as AES, and longer keys, into the thousands of bits, are now used to ensure confidentiality. Eventually, with increases in computing resources and improved cryptanalysis, current techniques will be easily broken.

Integrity

Integrity is maintained when both the sender and receiver are confident that a message has not been changed once it was sent. A message digest, also known as a message hash, is a calculation that uses the content of a message to compute a string of characters. If any part of the message is tampered with, even changing a comma to a period, for example, the message digest will change. When a sender transmits confidential information, a message digest is calculated and encrypted along with the message itself. The receiver calculates the message digest again and compares it with the one sent with the message. If they do not match, the message has been compromised.

Availability

As the name implies, availability ensures resources are functioning as needed when they are needed. In the broader area of information management, availability includes disaster recovery planning, backup and restoration operations, and security concerns. Devices that are compromised by malware or subject to Denial of Service (DoS) attacks are partially to fully unavailable. When the network is extended to allow unmanaged devices access to trusted resources, it must protect itself against threats such as Distributed DoS attacks or malware infections.

Meeting Security Objectives in the Extended Network

The options for implementing effective security measures in the extended network depend on the extent to which unmanaged devices are used. Devices used by telecommuters, branch offices, and mobile workers can be controlled almost as much as desktops used by in-office workers. For example, mobile workers can be given company-issued laptops, fully configured with antivirus software, a personal firewall, automatic operating system (OS) updates, and standard access controls. Similarly, branch offices can be established with local area networks (LANs) that adhere to company policies. In these cases, the one remaining issue is how to connect to the network.

Prior to the widespread adoption of the Internet, organizations could lease dedicated telecommunications lines between branch offices and headquarters. A T1 (1.544 Mbps) or fractional T1 was commonly used for this type of connectivity. One advantage of dedicated lines was that they were not shared. These were point-to-point solutions that did not introduce the same types of threats found through Internet-based connectivity.

Although easier to secure, dedicated networks have their drawbacks. First all, they are not very flexible. Telecommunications companies must configure dedicated circuits for their customers, and they serve only local networks on either end of the line. The cost of a dedicated line is substantially more than the cost of the same bandwidth to access the Internet. A combination of features of the dedicated lines and general Internet access is needed.

Virtual private networks (VPNs) provide the benefits of both dedicated lines and the Internet (see Figure 1.4). VPNs transmit data over the Internet but encrypt the data before it is sent. In some cases, proprietary software is used on clients and VPN servers to encrypt network traffic. Other VPNs use standard Internet protocols, particularly the Secure Sockets Layer (SSL), to authenticate devices and encrypt messages.

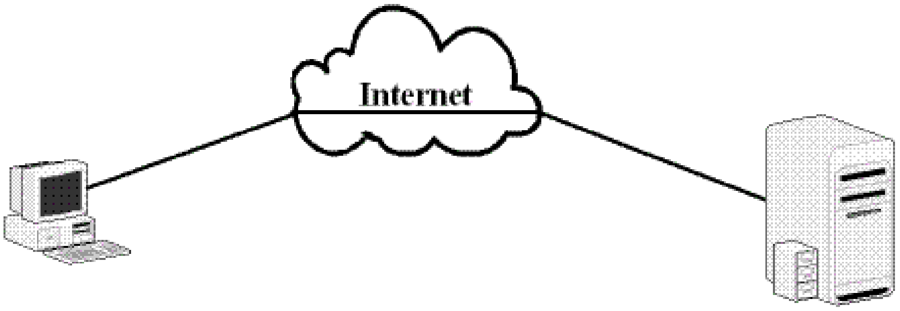


Figure 1.4: VPN software creates a virtual, dedicated, secure communication path over the Internet.

Limits of Network Security

Even with strict controls on managed devices that are used outside of the corporate network (such as laptops used by sales staff) and perimeter defenses (such as firewalls, antivirus appliances, and intrusion prevention systems—IPSs), security breaches can still occur. If someone has enough desire and resources to breach a system, they will succeed. In an ideal world, businesses and organizations would respond by deploying countermeasures up to the value of the information and system that could be compromised.

Too often when we think of information security, we think of someone breaking *in* to a system to collect, tamper with, or otherwise compromise the device or its data. Just as important is protecting information that is sent *out* of the trusted zones and into the realm of unmanaged devices and uncontrolled use of the information.

Business Impact of Information Leaks

Information leaks can have both measurable and non-quantifiable impacts on business. Three key types of impacts on a business are:

- Brand damage
- Financial costs
- Legal consequences

Often a single incident can result in more than one of these consequences.

Brand Damage

Companies spend money, time, and resources creating and developing brands. Brands carry with them a psychological dimension that implies a product or service is higher in quality, more effective, or otherwise superior to the competition's offerings. Well-developed brands are broadly recognized and carry with them their own value, known as brand equity. Information theft and other security breaches can damage brand equity.

Brand equity is determined, in part, by the additional demand that is created for a product or service that results from branding as well as the relative strength or weakness of a brand in comparison with competitor's brands.

> 📖 Brand equity is a relatively soft metric but, as with other intangible assets, techniques have been developed to measure the value of brands. For more detail about brand equity, see Jan Lindemann's "Brand Valuation" at http://www.poolonline.com/archive/issue24/iss24fea2.html.

Publicly disclosed security breaches, especially the loss of personally identifying information, can damage brands in at least two ways:

- Demand for the product or service is reduced. In many cases, consumers can easily substitute other products and services for one from a company perceived to be irresponsible with customers' personal information.
- The competitive value of a brand is diminished when a security breach occurs. Even if competitors are just as insecure, the public disclosure of a breach at one company may lead some to assume their competitors are more secure.

In the past, security breaches could be kept confidential. Companies were not required to publicly disclose such failures. Now, laws such as California SB 1386 and the Sarbanes-Oxley Act are bringing greater scrutiny to the internal operations of companies and, in the process, exposing their brands to greater risk. The impact on brand equity is just one form of the more general problem of financial impact of information disclosure.

Financial Impact of Information Leaks

The financial consequences of information leaks manifest themselves directly and indirectly. Direct losses occur when revenue is lost as the result of an information leak. For example, if a competitor acquires a copy of a sales proposal prior to its submission, the competitor can adjust its own proposal to win the business. In other cases, the thief sells stolen information itself, such as an analyst report, a design strategy, or a computer program. In the case of identity theft, banks and credit card issuers lost $1.2 billion in one year according to a Gartner Research study published in 2004.

Indirect losses occur when a competitive advantage is compromised due to an information leak. As noted earlier, those conducting industrial espionage can target IT vulnerabilities to steal information.

Legal Consequences

The legal consequences of information leaks are most clearly seen with regulatory penalties. For example:

- Violations of the Health Insurance Portability and Accountability Act (HIPAA) can carry a $50,000 fine and 1-year imprisonment sentence. If there is an attempt to sell or otherwise personally gain from a disclosure, the penalties increase to $250,000 fine and 10 years of imprisonment.
- Under California law SB 1386, a victim of personal information disclosure may sue for damages.
- Violations of one regulation, such as SB 1386, may trigger violations of other regulations, such as the Gramm-Leach-Bliley Act, which addresses privacy, among other issues, in the banking industry

These examples address commercial and private information. National security laws impose additional severe penalties for the disclosure of sensitive or classified information.

The threat of information theft is substantial and the increasing economic value of intellectual property and personal information is motivating an increase in cybercrime directed at acquiring those kinds of information. As a result, more comprehensive and effective security measures must be deployed. One method used to meet these needs is on-demand security.

Rising Need for On-Demand Security

As businesses and users demand more flexibility in information services, more unmanaged devices are accessing valuable and protected information and systems. At the same time, the economic value of this information is well understood and thus attracts criminal enterprises. Businesses and organizations are held responsible for how they manage information, and both government regulators and consumers impose consequences on firms that mismanage customer information. Markets impose their own ruthless competitive logic on firms that cannot protect proprietary information.

On-demand security is a set of integrated security measures designed to protect information independent of a particular device or network. The key characteristics of on-demand security are:

- These measures are transient and are delivered as needed
- They leave no footprint, or installed software, on devices
- They enable systems administrators to enforce security measures and policies on unmanaged devices
- They minimize the dependency on the security settings and configurations of unmanaged devices
- They provide a low total cost of ownership (TCO) and rapid deployments

On-demand security is an emerging segment of information security. The challenges to effectively deploying transient security to unmanaged devices are formidable, but the need is critical. Current security practices, based on creating trusted zones and enforcing access controls on managed devices, have worked well when properly implemented and maintained. These same measures cannot, however, meet requirements for access from unmanaged devices. Throughout, this guide will examine the technologies and methods of on-demand security as well as the best practices for preventing information theft both within and outside of managed networks.

Summary

A significant portion of corporate assets are now in the form of information. Assets, such as proprietary processes and customer information, are rising in importance as we shift to an economy more dependent on information. At the same time, more private information—such as healthcare information—is being stored and transmitted online. Both confidential company information and private personal information must be protected.

The need for information protection has both business and regulatory drivers. The market has demonstrated that it will not tolerate egregious information breaches, such as occurred with CardSystems. Government regulations, such as HIPAA, require the protection of personal information and call for severe fines for violations.

Protecting against information theft begins with understanding what type of information is created, stored, and transmitted within an organization and classifying that information accordingly. Controls—such as password-protected accounts, file permissions, and application access controls—are then used to secure the information. Although these traditional controls work well, they are not all encompassing. Vulnerabilities and other threats can compromise the integrity and confidentiality of protected information. On-demand security techniques have arisen to address these vulnerabilities; these techniques will be addressed in detail later in this guide. The next chapter examines the need for information protection from a regulator perspective by examining business integrity regulations, such as the Sarbanes-Oxley Act and Basel II, as well as personal privacy legislation, such as HIPAA and SB 1386.

Content Central

Content Central is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, Content Central offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: http://www.realtimepublishers.com/contentcentral/.