

realtimepublishers.comtm

The Definitive Guidetm To

Security Inside the Perimeter

Apani

Rebecca Herold

Chapter 2: Factors Working Against Securing Just the Perimeter	25
Tribal Thinking Must Change.....	25
Trust Where Trust Makes Sense	25
Preventing Crime by Insiders Is Difficult.....	26
New Technologies Make It Increasingly Difficult to Secure Networks.....	26
Consider What Insiders Can Do	26
Employees Have Wide Access Because they Are Employees	27
Employees Often Breach Security	27
Employees Need Security Understanding	27
Recent Studies Examine Insider Threats	28
Fraud Impacts Virtually Every Organization.....	29
The Perimeter is Porous	30
Business to Business Connections	30
EDI Was the Forerunner of Partner Connections	31
B2B Connections Are Typically Inconsistently Managed.....	31
B2B Connections Create Holes in the Perimeter.....	31
Business to Consumer Connections.....	35
Mobile Workers	41
Mobile Computing Devices	43
Business Use Is Increasing.....	44
Mobile Devices Store Increasingly Large Amounts of Data	44
Easier than Ever to Compromise	45
Easier than Ever to Lose Mobile Devices.....	45
Dealing with Theft and Loss.....	46
Wireless Connections.....	46
Connections Made Outside the Network Perimeter.....	47
Wireless LANs Have Significant Risks.....	47
War Driving	47
Legal and Regulatory Compliance.....	48
Inappropriate Technology for the Purposes Being Addressed	49
Increasing Data Value Increases Threats	50
Summary	51

Copyright Statement

© 2005 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

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.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

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 2: Factors Working Against Securing Just the Perimeter

Tribal thinking has existed for centuries within many different cultures in which members of a group, or tribe, were completely trusted to do what is right and good and those who were not members of the tribe were not trusted. There is a long history of organizations also trusting all their own members. Historically, organizations believed that trusting employees implicitly led to loyalty and better productivity. In fact, a study published by NFI in 2003 (<http://www.nfiresearch.com/subpage/release/EmpLoyalty.html>) stressed increasing trust, stating, “It isn’t the monetary rewards that build loyalty—it is the feeling of adding value, making a contribution and being trusted that matter most in building an organization of loyal employees.” This idea certainly reflects tribal thinking.

Tribal Thinking Must Change

According to the United States Department of Labor (<http://www.bls.gov/news.release/tenure.nr0.htm>), the median number of years that wage and salary workers had been with their current employer was 4.0 years in January 2004, and in January 1983 it was 3.5 years. Thus, the retention of employees in all industries has changed little in two decades. However, if you look at the statistics of employees who are actively searching for a new employer while with their current employer, you get a different view. A May 1976 Bureau of Labor Statistics survey (<http://www.bls.gov/opub/mlr/2000/09/art1full.pdf>) showed that 4.2 percent of all workers who had been at their jobs at least 4 weeks were interested in changing jobs. A 2005 survey conducted by the Society for Human Resource Management and CareerJournal.com reported that 81 percent of today’s employees are interested in changing jobs within the next 12 months. This statistic seems to indicate that your corporate tribal members are loyal only until something better comes along.

Trust Where Trust Makes Sense

Trying to retain good employees certainly is necessary, but organizations must realize that the trust they impart upon their employees needs to have certain limits. Not only are security measures necessary to help protect against the malicious activities of those employees who cannot be trusted, such security measures are also necessary to help protect against the mistakes and lack of knowledge of well-meaning employees that could lead to business-closing incidents. This instinct of trusting everyone that is a part of your team, organization, or tribe, must be tempered with good business practice and establishment of due care processes.

Some of the most trusted positions within an organization are within the IT areas. Security administrators hold rein over your network. Making sure these folks are appropriately monitored, have appropriate controls applied, and receive adequate training is a demonstration of due care that your organization must take the time to implement. Although the vast majority of IT staff will do the right thing, there are still those that could be tempted to abuse their powerful capabilities and do wrong.



In August 2005 the Helsinki, Finland branch of global financing company GE Money had police investigate the theft in June of about €200,000 (\$245,400). The police reported they believe the company's head of data security stole the money using banking software from the company along with passwords for its bank account. Accomplices then accessed the account from a laptop computer using an unprotected WiFi network at a nearby apartment building. Investigation revealed the laptop's MAC address (the unique identifier on the network card) belonged to GE Money, and the bank's security officer was soon implicated.

Preventing Crime by Insiders Is Difficult

It is difficult for companies to guard against crimes in which internal staff is involved, making it even more important to implement security measures internally. There are few reported incidents of computer crimes committed by insiders, but that definitely does not mean that there are few crimes that are actually committed.



In July 2004, Scotland Yard's Computer Crime Unit reported UK businesses typically only report 5 to 7 percent of all computer-based crimes to the police. "Around 93 to 95 percent of all cybercrimes go unreported because companies rate unwanted publicity as potentially more damaging to their business than the incident itself."

It is likely many of these unreported crimes are committed inside the network. It is also likely that many crimes go undetected.

New Technologies Make It Increasingly Difficult to Secure Networks

There has been an explosion in the creation of new technologies in the past decade that make it very easy to link networks. Staff members who do not realize the threats they present use new technologies widely inside the network, often without the knowledge of management. The availability of inexpensive technologies can be easily accessed by large numbers of people, employees, and outsiders alike. More and more employees are moving their business work to their home computers. Of course, this move can provide tremendous benefits to businesses. However, by increasingly putting powerful computing devices into the hands, and control of, employees, the businesses inevitably become more vulnerable to unauthorized network intrusion and abuse.

Consider What Insiders Can Do

So how vulnerable are businesses to the activities of their own tribe members? Considering virtually any computer system is susceptible to unauthorized intrusion, very vulnerable. Just consider a few of the types of authorized activities an insider can typically perform:

- Open the door of a computer room
- Dial into a computer network
- Obtain access to a direct-wired terminal
- Send email messages
- Supply or write a software program for a computer system
- Perform a computer maintenance or repair service

Your internal tribal members can do any number activities by exploiting their authority to wreak havoc on your network:

- Tamper with any service residing within the system
- Interfere with the work of systems administrators and operators
- Deny access to legitimate users
- Add false information
- Read, copy, or erase programs and data
- Enter other computer systems
- Change system instructions and protocols
- Introduce disruptive programs and applications



It only takes one person to corrupt a corporation's information network. Are you comfortable believing that 100 percent of your tribe members will always do the right thing?

Employees Have Wide Access Because they Are Employees

Employees, simply by virtue of their status as employees, enjoy wider access to a company's information assets and information equipment than outsiders do. Many, if not most, employees are now savvy computer users and, if they wanted, are better positioned to insert malicious code into a network than are hackers. They are also more able to steal passwords than any industrial spy. In fact, when it comes to leaking, copying, reading, stealing, altering or deleting information, employees participate in these activities far more than any external intruder.

Employees Often Breach Security

Why do employees want to deliberately fiddle with their organization's information? For many reasons, including greed, anger, frustration, and revenge, just to name a few. There are also hundreds of unintentional security lapses committed by employees daily as a result of carelessness, gullibility, and ignorance. Employee access to information is the greatest threat and greatest challenge to securing an organization's information infrastructure.

Employees Need Security Understanding


Organizations must instill a security mentality into their tribe members. This goal can only be successfully accomplished through careful planning and implementation. Such an awareness and training program must encourage employees to identify the need for information security and to willingly accept and follow the security controls and procedures in place. Such a program must implement constant communication, consistent reinforcement, audits for compliance, and investigations into non-compliance.

Trust is vital for successful business; it is also vital as part of the security equation. Security technology, controls and procedures are definitely essential in protecting information. Ultimately, however, the employees are critical to ensuring security.

If you explain clearly, consistently, and often to employees why security measures are established most will still feel trusted and understand the reasons why such measures are necessary. In fact, you *must* communicate that you trust your employees—this idea is a vital human factor in employee job satisfaction. However, letting employees know that they are trusted doesn't diminish the need to establish internal security controls—there are too many compelling reasons to do so, such as establishing accountability and to meet regulatory requirements.

Recent Studies Examine Insider Threats


In May 2005, the United States Secret Service in partnership with the CERT Coordination Center, located at Carnegie Mellon University's Software Engineering Institute, released their most recent Insider Threat Study (ITS—http://www.cert.org/insider_threat/insidercross.html). This study analyzed incidents from a behavioral and a technical viewpoint. The ITS examined incidents committed by insiders, defined as current or former employees or contractors, who intentionally misused their network access authorization in such a way that they impacted the organization's business operations, data, or networks. The 2005 ITS analyzed 49 insider incidents in which the insider's primary goal was to “sabotage some aspect of the organization (for example, business operations, information/data files, system/network, and/or reputation) or direct specific harm towards an individual.”

 The ITS revealed the majority of the insiders who committed acts of sabotage were former employees who had held technical positions with the targeted organizations. Almost all the insiders examined were charged with criminal offenses. Most of the charges were for violations of United States federal law.

The key findings of the ITS are the following:

- A negative work-related event triggered most insiders' actions.
- Most of the insiders had acted out in a concerning manner in the workplace.
- The majority of insiders planned their activities in advance.
- When hired, the majority of insiders were granted systems administrator or privileged access, but less than half of all the insiders had authorized access at the time of the incident.
- Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.
- Remote access was used to carry out the majority of the attacks.
- The majority of the insider attacks were detected only once there was a noticeable irregularity in the information system or a system became unavailable.
- Insider activities caused organizations financial losses, negative impacts to their business operations, and damage to their reputations.


These findings are corroborated by the findings of the 2004 Ernst & Young study ([http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/\\$file/2004_Global_Information_Security_Survey_2004.pdf](http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf)) that indicates the damage from insiders is much greater than from outside the network. Most damage is from misconduct, omissions, oversights, or violating policies and procedures. The study reported one in five employees reported “personal awareness of other individuals stealing from the employer.”

 Many insider incidents are never discovered by organizations, so they are unaware that they are even being victimized.

Fraud Impacts Virtually Every Organization

The 1997 President’s Commission on Critical Infrastructure Protection report (http://www.cert.org/pres_comm/cert.rpcci.abstract.html) reveals some primary issues related to the insider threat:

- Insider problems exist within the critical infrastructure, including the military, telecommunications, and energy sectors.
- There is a tendency for managers to settle insider problems quickly and quietly, avoiding adverse personal and organizational impacts and publicity. Because of this handling method, we cannot really determine how widespread the problems are. What actually gets reported is likely only the tip of the iceberg.
- Organizations are at risk from repeat offenders. As computer criminals migrate from job to job, typically without background checks and with constraints upon employers in providing references, no significant consequences result from their offenses.
- The range of potential perpetrators and their motivations is broad. Disgruntled employees who are angry about layoffs, transfers, and other alleged grievances have committed computer sabotage and extortion. Other cases involve employees who take advantage of their position of trust for financial gain, attackers who are employed within the critical infrastructure caught engaging in unauthorized explorations, and “well-motivated” employees who claim they are acting in the best interest of their organizations. Other perpetrators include *moles*, individuals who enter an organization with the explicit intent to commit espionage, fraud, or embezzlement. Overall, case investigators report that the number of computer-related offenses committed by insiders is rising rapidly each year.

 The Association of Certified Fraud Examiners (ACFE—<http://www.cfenet.com/pdfs/2004RttN.pdf>) estimates that the typical United States organization loses 6 percent of its annual revenues to occupational fraud; in other words, fraud instigated by insiders. Using the United States Gross Domestic Product for 2003, this statistic amounts to roughly \$660 billion in total losses.

Multiple other studies have examined various aspects of the impact of insider acts on businesses:

- In the 1996 WarRoom Research *Information Systems Security Survey*, 62.9 percent of the companies surveyed reported insider misuse of their organization's computer systems.
- The Computer Security Institute and FBI (CSI/FBI) 1995 *Computer Crime Survey* reported the average cost of an insider attack was \$2.7 million. The 2005 CSI/FBI Survey reported that the average cost of an insider misusing the Internet was almost \$6.9 million.
- A study conducted by the United Nations Commission on Crime and Criminal Justice surveyed 3000 sites in Canada, Europe, and the United States, and found that "By far, the greatest security threat came from employees or other people with access to the computers."
- An April 2000 study about the insider threat to Department of Defense (DoD) systems by the United States Office of the Assistant Secretary of Defense reports for one set of investigations that 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization. Of 1004 criminal investigations associated with DoD information systems "87 percent were either employees or others internal to the organization."

The Perimeter is Porous

An explosion in outsourcing, mobile computing, wireless networking, business partner connections, and Web-based applications has created a spider web configuration of connections to virtually anyone, from anywhere, with any device. Perimeter-based security is no longer sufficient. It fails because there is no longer a clearly defined perimeter. With the large numbers of individuals with access to business networks who are not employees, it's difficult to determine who should have access to network resources and who needs to be blocked. Your "trusted" internal network environment is now likely connected directly to the Internet through a home or partner link or through an unapproved wireless connection.



The typical network perimeter is no longer like a steel fortress protecting against threats, instead it is like a stainless steel sieve.

Business to Business Connections

Most organizations now have business to business (B2B) relationships with business partners in which the partners' networks are connected through a variety of methods. Such relationships certainly enable efficient business communications and processing (such as supply chain management, lead-time reduction, and other business process automation) by transmitting transactions through these connections. B2B can also automate transmissions to reduce the level of human interaction that used to be necessary to achieve these benefits and efficiencies.

EDI Was the Forerunner of Partner Connections

Not long ago, organizations used Electronic Data Interchange (EDI) as the primary way to share information with their business partners. Of course, EDI is still used widely today. However, because of the complexity and costs involved with EDI systems and software, many companies used EDI only to share information with a small percentage of their partners. Most business partners do not need such complex systems to share information, so simpler, less-expensive solutions are implemented that leverages the ability to share information over the Internet, or to connect the trading partners directly to a company's network. A large amount of sensitive and competitive information is typically transmitted through B2B relationships, so security is a major concern. Not only the security of the transmissions but also the vulnerabilities that the multiple and varied connections present to the organization's network.

B2B Connections Are Typically Inconsistently Managed

B2B connection implementations often fall through the cracks with regard to consistently having one group to manage and monitor the connection. Sometimes the IT group may be responsible for doing something minor for the connection, such as opening a port on the firewall to enable communication between the business partners. Sometimes the business partner handles the bulk of the connectivity. In yet other cases, the business unit takes it upon themselves to make the connection without the assistance, oversight, or authorization of the appropriate IT area. Support issues are often handled ad hoc. All these ambiguities can lead to unsecured pathways into your network. Regardless of how the connections are made, your company is still ultimately responsible for ensuring the security of the company network.

B2B Connections Create Holes in the Perimeter

B2B connections can create an unbelievable number of holes into your network, providing compelling motivation to implement security at more than just the perimeter. The following sections explore some of these potential holes.

Lack of Security Policy Creates Security Holes

Often a good security policy does not exist to govern B2B connections. Without such a policy, personnel responsible for these relationships will not know the security requirements with which they must comply. There is also no accountability for personnel who create B2B connections if there is no policy. You need to have a security policy that outlines the minimum security requirements for each B2B relationship with your organization. The policy should outline security requirements related to architecture, transaction processing, monitoring, and the groups that must be involved from initial discussions to actual implementation and monitoring.

Lack of Due Diligence Creates Security Holes

Due care activities need to occur to ensure B2B connections and information exchanges are secured. If information security is not involved in the due diligence process, the business partner might not have adequate measures to secure the B2B transactions. If the business partner will access your company's data or systems, significant security concerns exist related to confidentiality and integrity of information. To mitigate this risk, information security must participate in due diligence activities to validate and confirm security specifications and requirements prior to signing the final agreement.

Lack of Audits Creates Security Holes

Audits need to be performed on B2B connections to find vulnerabilities and prevent unauthorized access to your information. If internal audit is not involved when forming a B2B relationship, the final B2B infrastructure may not meet your organization's audit and control requirements, including regulatory requirements. Internal audit should be involved in the B2B process from start to finish to help ensure that your organization's audit and control requirements are met.

Lacking Security in Partner Connections Creates Security Holes


Connections may be made with business partners when they are not needed, or may be made in ways that do not support the corresponding business process. It is important to understand the business process any connection to your network is supporting, along with the criticality of the process. Is the purpose just to share information or to perform business transactions? Considering such issues will help determine the appropriate way in which to make and secure the connections.

Lack of Assigned Responsibility Creates Security Holes

If no one officially owns the B2B relationship management activities, it is likely such partnerships are not managed appropriately, and no accountability will exist to ensure contract requirements are met. Once your organization has signed a B2B agreement, someone needs the ownership of that relationship. This role needs to ensure that the requirements are met (including security requirements), act as a single point of contact with the partner, and work with appropriate groups within your organization to manage the relationship.

Lack of Service Level Agreements Creates Security Holes

Without a Service Level Agreement (SLA), the partner may not be accountable for service levels required by your organization. Your organization's information may not receive an appropriate level of security, and may potentially be accessed on your network through the holes in the partner's network. An SLA obligates the partner to meet your security requirements. It should outline the scope of your organization's relationship with the partner, roles and responsibilities, performance metrics, and so on. Penalties should be incurred for being non-compliant with the SLA.

 Some security-related issues to address within SLAs to help prevent incidents from occurring within the perimeter as a result of your relationship with the partner include:

- Allowable downtime
- Documented and tested disaster recovery plans
- Incident handling procedures and associated escalation lists
- Notification requirements for security incidents and information breaches
- Backup and recovery requirements for data
- Financial and non-financial penalties for SLA non-compliance
- Auditing provisions, including timing, notification, frequency, and so on
- Security requirements for the hardware and software used with the B2B connections, including such specifications as patch management and hardening standards
- Documented encryption requirements and standards

Lack of SLA Monitoring Creates Security Holes

If SLAs are not monitored, your organization's data may not be properly secured because the partner may not be meeting your SLA requirements. The person who owns the B2B relationship responsibility should also work with the appropriate areas in your organization to monitor the provisions of the SLAs.

Lack of Secure Information Exchange Creates Security Holes

If you are exchanging sensitive information that is not properly secured, it could be compromised and get into the wrong hands, and possibly result in detrimental impact not only to your organization, but also to your customers. Be sure to analyze and approve architectures for all planned partner connections. Important issues to address include, but are not limited to:

- Encrypting information during transmission
- Using digital certificates
- Establishing reasonable authentication measures

Lack of Network Traffic Analysis Creates Security Holes

If you do not establish security measures to ensure information coming from the partner network is valid and authorized, there is great risk of unauthorized access to your organization information and network. When your partner sends information to your organization, your partner must communicate with at least one or more of your systems. Your security considerations for these transmissions will vary based upon your organization, your partner, and the purpose of the transmission.

Lack of Business Partner Security Creates Security Holes

There is a wide spectrum of risks related to your business partner not having adequate security. They can range from minor impacts due to operations all the way to huge fines and penalties resulting from non-compliance with applicable regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and many others. Incidents on your partner networks could have significant impact to your organization's reputation, availability, and financial success (or failure).

Lack of Adequate Access Controls Creates Security Holes

Risks related to inadequate access control measures can have significant impact on the confidentiality of your data, potentially resulting in financial and/or reputation damage. Your partners should provide access to data and applications based upon a business need and as it relates to the kind of relationship and contract you have with the partner. Be very careful about providing blanket access to everyone within the partner organization or by having identifiers for your system shared by multiple business partner personnel; this setup results in lost individual accountability.

Lack of Employee Termination Procedures Creates Security Holes

Terminated partner employees could still have access to your organization's data and systems. They could wreak havoc on your network, making it inaccessible for business processing, surreptitiously take data from your network and give or sell to your competitors, or try to ransom it to your organization. When your partner employees are terminated, all their access to your organization should be removed. This is another good reason to not use group identifiers—it increases the likelihood terminated employees who used such an identifier will still have access to your systems.

Lack of Identifier Clean-Up Creates Security Holes

If you do not purge identifiers, individuals who no longer need access, including terminated employees, may still have access to the B2B applications and your networks. You should establish a procedure to periodically purge all identifiers from your systems that have not been used for a specific period of time, in addition to reviewing identifiers to determine whether they are still necessary, even if they have been used recently.

Business to Consumer Connections

Business to consumer (B2C) connections are those by which consumers purchase goods or services over the Internet, or some other public connection, from your company, or otherwise communicate or share information with you. Until recently, many organizations put up a Web site with information about their products and services so that consumers could learn about the company's offerings. However, organizations now overwhelmingly make services and products available for purchase, in addition to giving customers access to their account information, through public networks. Consumers use such connections extensively because of the convenience and often lower prices. However, many consumers still avoid making online purchases or accessing their account information through the Internet because of security concerns and the recent reports of identity theft, insufficient security on Web sites, reported attacker exploits, and concerns that Web sites are not legitimate. Such concerns are understandable.



If you have customers who look at your online catalogs, make purchases from your Web site, and supply information such as their name and address, they are participating in a B2C communication with your organization.



B2C connections create entry paths to your organization's systems and data.

Security risks related to B2C connections include:

- Unsecured transmission of customer information
- Unsecured storage of customer information
- Inadequate transaction integrity and legitimacy
- Insufficient security of the architecture supporting the B2C connections, such as the Web servers and the back-end systems
- Unavailability of the B2C systems components

The risks created by B2C connections could significantly impact your organization. B2C connections create a variety of pathways into your systems. Some of the potential impacts to your organization from a B2C connection security incident include:

- Your business operations could be delayed or even completely shut down through a Denial of Service (DoS) attack.
- If your customer information is stolen, your organization could face legal penalties, fines, and civil suits.
- Security and availability issues for your network can have immediate and significant financial impact on your organization. If your customers cannot make purchases, you lose money.
- If a breach occurs through a B2C connection, or any connection for that matter, and the incident is publicized, it will likely damage your organization's brand and reputation. The degree of damage will depend upon the nature of the incident and the severity.

B2C connections can create huge risks and an unbelievable number of holes into your network. The following sections explore some of the ways these risks and unsecured connections occur, providing still more persuasive reason to secure inside the perimeter.

Lack of B2C Security Policy Creates Security Holes

Without a policy to govern B2C processes, B2C architecture and applications will likely be developed with inadequate security. Trying to add security onto architecture and applications after deployment can be expensive and take much more time than if it was built in right from the start. Additionally, a policy provides a mechanism for enforcing effective B2C security practices.

Lack of B2C Knowledge Creates Security Holes

If organizations do not know the financial and brand impact of B2C connections, they will likely not plan appropriately to ensure the connections have the appropriate level of availability. Organizations need to determine the percentage of overall revenues the B2C connections generate as well as whether the Web site providing the B2C connection has had a security breach that would impact the organization financially or its brand.

Lack of Security Breach Documentation Creates Security Holes

If you do not know about past security breaches through B2C systems and how they impacted your organization, you cannot know how to prevent the same breach from occurring again. Knowing about past security incidents and how they were handled will help to implement measures to prevent them from happening again.

Lack of B2C Accountability Creates Security Holes

If no one owns the B2C connections responsibilities, there is no accountability—a dangerous situation for a revenue-generating activity. Lost or corrupted B2C connections have a significant impact, including lost revenue and lost customers. Ownership of the B2C connections must be established so that all associated activities can be consistently managed. Such a role should ensure updates occur, the content is appropriate, the network architecture for the connections is appropriate, and that customer Web sites are available, functioning appropriately, and are secured.

Lack of Database Ownership Creates Security Holes

If no one has documented ownership of the databases supporting the B2C operations, it's likely they will not be properly secured, resulting in unauthorized access and potential data integrity compromises. B2C databases are critical to the B2C infrastructure, and typically contain very sensitive and confidential information that falls under potentially multiple regulatory requirements for protection. This information must be adequately secured.

Lack of Access Restrictions Creates Security Holes

Without strict access controls on the B2C databases, unauthorized access to sensitive information in the database can occur or the integrity of the database could be damaged. Access to the database should be limited to only those who need it to perform their job responsibilities.

Lack of Due Diligence Creates Security Holes

If due diligence is not performed to ensure proper security of B2C processes, the application may not have the necessary security features. As a result, there could be unauthorized access to the application transactions or integrity loss to the B2C data. When purchasing a Commercial Off the Shelf (COTS) application, security is often overlooked. It is important to review the application package and consider access control capabilities, information flow with other applications and systems, and other security-related issues unique to the application.

Lack of Security for In-House Developed B2C Applications Creates Security Holes

If security is not built in from the beginning, there is a risk the application will not adequately ensure the integrity and confidentiality of the data. The costs associated with additional development and re-engineering of the processes when trying to add security as an after-thought could be significant. Implement policies and procedures to require security as part of the systems development and modification process. Consider automated tools to help developers build security into applications during the development process.

Lack of Web Server Security Creates Security Holes

If the Web server is not hardened or patched, vulnerabilities could be exploited to attack the B2C application. This attack could lead to Web site unavailability, defacement, access to internal systems, and so on, resulting in lost revenues, customers, reputation damage, confidential data breaches, and other significant business-impacting incidents. Best practices for hardening Web servers can be found on the corresponding vendor Web sites as well as on information security Web sites. Procedures should be implemented to perform hardening and patching activities on an ongoing basis.

Lack of Alerts Creates Security Holes

Without an intrusion management system in place, potential attacks could go unnoticed until after significant and potentially irreversible damage occurs. This could lead to lost revenue, lost customers, and damaged reputation and brand. Procedures must be in place to detect when something inappropriate is happening at the B2C Web sites. Consider using intrusion management systems, which can help detect potential attacks on a 24×7 basis. Some such systems also have the ability to stop certain types of attacks.

Lack of Segregation Creates Security Holes

If the B2C database and application sit on the same server, and the server is compromised or attacked, both the database and application could be compromised, resulting in customer and other sensitive information being exposed, permanently lost, or stolen. This risk is much greater if the application and database actually reside on the Web site server. To reduce risk, the application and database should not reside on the Web site server, but each on two separate servers behind your organization's firewall. Of course, the front end of the application will need to sit on the Web site server, but non-customer-facing functions of the application should sit in another network segment behind the firewall.

Lack of Firewalls Creates Security Holes

The lack of firewall, or an incorrectly placed or configured firewall, could result in unauthorized traffic into your organization's network. Oftentimes, the firewall is the only security feature of a B2C application. Implement policies and procedures to require firewalls to be used for every B2C application, and document the minimum requirements for establishing the firewall rules based upon the activities of the B2C application.

Lack of Cache Clearing Creates Security Holes

If sensitive B2C information is cached, another person could potentially log on to public computers or kiosks as the preceding person, leading to fraudulent activity. Client software should not allow authentication data, or other confidential data, to be cached. Additionally, cookies should not contain confidential information and should expire upon session termination.

Lack of Proper Logout Creates Security Holes

If an application does not logout properly, individuals could obtain unauthorized access to each other's accounts. Such is especially a risk in public places such as at kiosks or on public computers such as in libraries or in Internet cafes. Each B2C application should have a logout function to allow users to logout out of the application completely and disallow others using the computer from using an active session.

Lack of Secure Protocol Creates Security Holes

When information is sent in clear text across the Internet, it can be intercepted and used to gain unauthorized access to other accounts without any trace that this activity even occurred, let alone who captured the information. All sensitive information should be sent using secure protocols that encrypt sensitive information.

Lack of Password Masking Creates Security Holes

If they are not masked, the B2C passwords could be seen by others nearby and used to subsequently logon as another person, leading to fraudulent activity, loss of customer trust, and brand damage, not to mention potential regulatory non-compliance and resulting fines, penalties, and potential civil suits. All passwords should be masked on the end user's screen whenever they are typed.

Lack of Strong Passwords Creates Security Holes

Weak passwords can easily be exploited to gain unauthorized access to the B2C application as well as to customer account information. The B2C application must force users to create strong passwords and provide ways for legitimate, identity-validated customers to obtain or change their passwords if they forget them.

Lack of Logon Security Creates Security Holes

Without a lockout feature, malicious users could use brute force methods to gain unauthorized access to B2C applications and customer information. A lockout feature will help to prevent this from happening. The account should be locked until the account user contacts your company to reset the account, or otherwise provides valid proof of identity to unlock the account.

Lack of Identity Verification Creates Security Holes

If customer identity is not properly authenticated prior to resetting passwords and providing other account information, an unauthorized person could obtain this information then use it to gain access to the valid customer's account. Password resets should be performed only after following a consistent procedure to verify the customer's identity. Such procedures should also apply to responding to customers' requests for information about their accounts.

Lack of Administrator-Level Controls Creates Security Holes

If you do not limit administrator or root access to only those few who need it to administer the Web server, accidental or malicious damage to the Web site is a possibility. This is a significant risk if disgruntled employees have access. Administrator access to the Web server allows full access rights; an administrator can make any change or see anything stored on the Web server. Ideally, only one person should have this access as a primary responsibility, with another person serving as a backup. The person performing administrator activities should have a different personal account they use for all other activities that are not related to Web server administration.

Lack of Change Management Processes Creates Security Holes

Applications built in-house must go through a formal change management process before being put into production. Without formal change management procedures, vulnerabilities can be introduced to the B2C application as a result of inadequate testing and quality assurance. Vulnerabilities can lead to unauthorized use of the application or other types of security breaches. Formally documented change management procedures must be followed for all B2C applications, including those built in-house.

Lack of Information Access Controls Creates Security Holes

Access to product and service information offered on the B2C Web site must be strictly controlled. If such access is not controlled, critical service and product offering information and pricing could be changed inappropriately, resulting in customers placing orders with the wrong prices or the wrong descriptions. Formal policies and procedures must be in place to ensure service and product information cannot be modified without proper authorization. All edits should be logged and reviewed by quality assurance and management personnel.

Lack of Vulnerability Assessments Creates Security Holes


Vulnerability assessment of the B2C applications must take place. Without vulnerability assessment, significant vulnerabilities could be present and exploited when the application is moved to production. Tools are available that can be used to evaluate application code and security vulnerabilities. Code reviews can also be performed to identify faulty logic that creates vulnerabilities.

Lack of Logs Review


Someone must have assigned responsibility for reviewing the B2C Web server, database server, intrusion detection, and firewall logs. If logs are not reviewed, you will not know about potential security breaches in a timely manner, and will not be able to take proactive action. Periodic review of logs can help detect problems early while they are still manageable. Using automated tools for log analysis can help organizations that are short on human resources to perform the reviews. Another option is outsourcing log analysis.

Mobile Workers

An increasingly larger number of workers are becoming mobile. Personnel are carrying notebook computers, PDAs, smart phones, and Blackberries so that they can continue to work while they travel. More employees than ever are working from their homes. This increased mobility has enabled some individuals to be more effective in winning new business, transacting business on the spot, and delivering more timely and personal customer service.


 An American Interactive Consumer report stated that there were 23.5 million teleworkers in the United States in 2003. The International Telework Association & Council (ITAC) and research partner Dieringer Research Group estimated there were 44 million United States teleworkers in 2004.

The nature of telecommuting inherently adds more work for an organization's IT and information security staff. According to Gartner, fewer than 30 percent of handheld computing devices are officially sanctioned or administered by IT. Support for such devices can take huge and unexpected amounts of time to address.

 Large numbers of unauthorized personal computing devices are being used to perform business processing.

Securing the computing devices and storage media for mobile workers is dramatically more complex and difficult than securing a closed network. The more mobile workers an organization has, the more likely there are connections to their networks from external locations, and the more risks from each of these potential points of entry to the network. Recent studies from InfoBeads report most mobile workers work with information that is highly confidential and mission critical to the organization and has great impact on the business.

Mobile workers need to be well trained in the security requirements of computing while traveling and while working from their homes. They need to understand that they have ultimate control over the security of the business information while they are outside of organization facilities. Unfortunately, most mobile workers, especially those working primarily or exclusively from their homes, have notoriously lax security measures in place for their home-based business computers. A large majority now use cable and DSL modems for connections, effectively putting them online every hour of every day, subjecting them to the same types of attacks as the corporate networks but without the sophisticated firewalls and security tools in place to protect them.

 ITAC and Dieringer Research Group reported the use of broadband by home teleworkers grew by 84 percent in 2004.

Think about how mobile workers actually work:

- Use telephone lines, DSL, and cable connections to link to corporate networks and business information
- Typically locate their home work areas where other members of their household and their houseguests can access their computing devices, storage media, and see their business printouts
- Often allow family members to use their business computing devices for school, other jobs held by household members, Internet access, volunteer work, and other activities
- Are vulnerable to the physical security hazards associated with children, pets, cleaning activities, roughhousing, and other common general living activities
- Have no one from the office ensuring they make backups or overseeing where the backups that actually get made are stored
- Can easily lose their computing devices and storage media that contain critical business information—often such losses are not reported or are reported only to the physical security office to write off as an asset loss for the depreciated value of the computer and associated software

This type of insider threat within your virtual perimeter can have dire consequences. Consider an exercise performed by Pointsec Mobile Technologies in 2004 (*Digital Secrets Up for Sale*, The Birmingham Post, June 15, 2004.) Pointsec purchased 100 laptop computers for pennies on the dollar over a 2-month period from Internet and public auctions. The amount of unsecured confidential business information contained on these computers was staggering:

- 70 percent of the hard drives (all of which were advertised as having been “wiped clean” or “reformatted”) were readable.
- 77 Microsoft Excel documents were found containing customer email addresses, dates of birth, home addresses, telephone numbers, and other highly confidential information.
- A laptop purchased in Sweden contained confidential information from a large food manufacturer, including customer information, 15 PowerPoint presentations with “highly sensitive” company information, and more than 1500 private photos.



It is common practice at airports and mass transit facilities, such as Gatwick and Heathrow airports and on the Eurostar, for found items, including laptops, PDAs, and computer storage media, to be put up for auction if they are not reclaimed within 3 months.

Consider the damage not only to your organization’s reputation, brand, and revenue, but also to your customers if your employees sold their computers containing business information. Consider also the potential serious legal ramifications of such an incident resulting in your company being charged with non-compliance with any number of regulations as well as potentially facing civil lawsuits.

It is critical for organizations to invest more time, attention, and resources in the security practices of their mobile workers and for the tools they use. Policies and procedures need to be implemented to effectively control the vast amount of business information processed outside of the network facilities.


Mobile Workers Create Holes and Entry Points into Your Network Perimeter

Organizations must make sure mobile workers:

- Process and access from their remote locations only the business information that they need to perform their business activities. They should not be able to access all the resources that they are able to access while logged onto the network from within corporate facilities.
- Use only business-owned computing devices to do work. When personnel use computing devices they personally own for business processing, the risks of having sensitive and confidential information mishandled and falling into the wrong hands increases dramatically.
- Receive the training and tools needed to maintain the security and confidentiality of business information while they are traveling and working from home locations.
- Have their remote computing devices configured in such a way as to allow information security and IT staff to be able to ensure the integrity of the information being transmitted from these multiple remote areas to inside the corporate networks as well as to ensure availability of the information when it is need within the business systems.
- Dispose of computing devices they no longer need securely, preferably through your organization's information security and/or asset management area. Such devices should never be donated to charities, given to family members to use, or auctioned off unless the storage media is first completely removed.
- Use hard disk encryption and access controls.

Mobile Computing Devices

The very nature of mobile computing devices puts them at a greater risk of theft than other types of computing devices. Your network hardware is typically located within secured facilities, but your mobile devices, which have access through your network perimeter, are typically located outside your organization's physical security perimeter. As previously discussed, mobile workers rarely work in an environment as secure as your business offices. Mobile devices are used in cars, airplanes, trains, and buses; stuck in purses, bags, and jacket pockets; and many times are forgotten and left in overhead storage compartments, restaurants, bookstores, and libraries.

 What if your CEO's or security administrator's mobile computing device fell into the hands of a competitor, a criminal, or the news media? Would they be able to read confidential email, customer information, or access your internal network using the device?

What Is a Mobile Computing Device?

A mobile computing device is any device or medium that has computing capabilities, such as a PDA, laptop computer, or smart phone, or a device capable of storing electronic data, such as a CD, a USB thumb drive, a backup tape, and so on. Examples of mobile computing devices include:

- Notebook, laptop, and PDA computers
- Smart phones with storage, video, and/or computing capabilities
- Blackberries and other types of wireless email devices
- Laptop computer hard disks
- PDA memory drives
- Digital media cards, such as CompactFlash, SmartMedia, Secure Digital Memory Card, and MultimediaCard
- USB (or Firewire) storage devices
- Removable media such as CDs, DVDs, diskettes, and tapes
- Cell phone memory
- System Identification Module (SIM) cards for cellular phones
- MP3 players
- Digital cameras

Business Use Is Increasing

According to a 2004 IDC report, virtually all enterprise employees own cell phones and/or handheld computing devices. More than 22 million smart phones capable of running enterprise applications shipped in 2004, and IDC projects this number will reach 100 million by 2008. As the numbers increase, such handheld devices will become attractive targets for theft.

Frost & Sullivan research reports mobile professionals represent 75 percent of data users in the United States. The value of the business data and credentials stored on these devices has increased along with their ability to run critical business applications, ranging from email and instant/text messaging to field support and sales force automation. The top-tier executives are among those most likely to make extensive business use of mobile computing devices; they are also the personnel with the most critical and confidential business information.

Mobile Devices Store Increasingly Large Amounts of Data

Handheld storage capabilities were originally very limited, typically to just a few kilobytes of RAM. However, these devices are now capable of storing megabytes of information. Small removable compact flash devices and multimedia cards have tremendously expanded storage capacities. If a mobile computing device or memory stick falls into the wrong hands, it is likely to expose huge amounts of business information, potentially including customer information, business email, corporate plans and strategies, and so on.



A handheld device belonging to a power company employee in Japan containing confidential personal information for 665 families was stolen in 2005. In 2003, a Blackberry that had belonged to a Morgan Stanley executive was sold on eBay that contained dozens of business emails and other confidential information.

Easier than Ever to Compromise

The more advanced and feature-rich mobile computing devices become, the more ways there are to compromise them. With capabilities such as built-in cameras, text and media messaging, and always-connected Internet access, these devices are more versatile and usable than ever before, but they are also making it easier to download ring tones, images, games, malicious code, and shareware. When personnel use these advanced technology mobile devices without understanding the associated risks, it puts your business at increased risk to exploits from inside your perimeter.



Smart phones with Bluetooth connections can be victims of Bluesnarfing (remotely reading and writing the phone's address book, initiating calls, sending text messages, and so on.)

Easier than Ever to Lose Mobile Devices

Because of their increasingly small sizes and diminishing prices, mobile computing devices are often not handled carefully and end up being lost. People typically view such inexpensive devices as being easy to replace, and some almost treat them as disposable or in nonchalant ways. More and more vendors give away USB drives and PDA devices at trade shows as marketing gimmicks. It's no wonder the perceived value of such devices can tend to be negligible without giving thought to the value of the information contained within them.



A 2005 FusionOne poll revealed 43 percent of mobile users had experienced theft, loss, or damage of their mobile computing devices. Gartner estimates that 90 percent of mobile computing devices containing business information do not have security implemented, such as power-on passwords or encryption to protect the information.

Mobile storage media is often overlooked as a source of concern by organizations, but it contains some of the most sensitive and confidential business information. The risks are great:

- An information thief can quickly remove and potentially replace such media by an information thief with a dummy device so that the owner does not immediately realize the information was stolen.
- Small items such as these media devices can easily be misplaced, lost, or forgotten.

Dealing with Theft and Loss

An organization must immediately deal with a variety of issues when a mobile device is stolen or lost. The cost of replacement hardware is often insignificant compared with the potential financial costs from the primary security considerations:

- The information stored on the device is available to any third party who comes into possession of the device if the information was not encrypted. If the device contained proprietary or confidential information, this presents a serious risk to an organization.
- If the device holds credentials, such as unsecured digital certificates for use in accessing the corporate infrastructure, the device could be used to compromise corporate resources. Theft of credentials threatens data confidentiality.
- A lost device results in the user being without the ability to use it and the information it stores. They may now be incapable of performing their duties until the device and its data are recovered or replaced.

Your organization should have a documented policy for responding to the loss or theft of mobile computing devices. There should be a procedure to quickly report the loss, and device owners must be aware of this procedure. Information security must clearly and periodically communicate a clear message to the user community about the risks of mobile computing devices and stress the importance for users to report the theft or loss of a device immediately.



Mobile devices provide entry points to your internal network. Organizations must implement controls on mobile devices appropriate to the associated risks. When determining risks you need to review:

- The value of the data stored on mobile devices
- The specific vulnerabilities of the mobile devices in use
- The specific threats to the organization

Wireless Connections


Most mobile computing devices provide a wide range of wireless communications capabilities, such as Infrared, Bluetooth, Wireless LAN, GPRS, and even dialup over analog cell technology. All of these capabilities provide routes into your organization and network systems. They all are also vulnerable to communications interception in varying degrees. When mobile devices are used to transmit sensitive information, there are risks that the information can be inadvertently disclosed or intercepted. Virtual private networks (VPNs) are often deployed to address and control these risks.

Connections Made Outside the Network Perimeter

Wireless connections can easily, and are often, made to other outside untrusted networks. Such connections can be made from within your network or facilities. Mobile workers also often connect to untrusted networks using wireless in such locations as at an airport or using a broadband Internet connection within their own homes. Such devices are typically connected directly to the Internet without the protection of firewalls or intrusion detection systems (IDSs). This setup exposes the device, business information, and subsequently your organization, to a great range of threats, including direct attack from entities on the Internet, whether they are human or malicious code.


Wireless LANs Have Significant Risks

Businesses are jumping on the wireless network bandwagon in droves. However, there are a great number of risks inherent to wireless LANs for which business leaders are many times not aware. Some of these risks include unsecured default configurations, unsecured network architecture supporting the wireless LAN, encryption weaknesses, and physical security weaknesses.

 An August 2005 CIO Insight survey reported that 83 percent of 357 IT executives indicated they use wireless networking.

War Driving

Most wireless networks are configured by default to allow any wireless system to access the network without authentication. Individuals can easily drive around with a wireless computing device and pick up many network connections, a practice called war driving. War driving is widely used to locate free Internet access or—even worse news to your business—to access information on corporate networks. Wireless LAN administrators may not know just how vulnerable they really are. If you have a wireless network, you must protect it against war driving.

 When someone gains access to your wireless network, the only things keeping the person from accessing unauthorized servers, applications, and information are strong internal security controls. If internal controls are weak or non-existent, an unauthorized individual could easily gain access to your corporate wireless LAN, then possibly take over control of your network by exploiting weaknesses.

DoS attacks are also a threat to wireless networks. If you have mission-critical systems running on your wireless network, an attacker doesn't even need to gain access to a system to cause damage or financial harm. All the attacker has to do is flood your network with transmissions to cause a DoS attack.


To help prevent the risk of inside attacks from occurring through wireless networks, you need to take two primary actions:

- Limit the network access to only authorized users
- Protect wireless traffic from sniffing

Legal and Regulatory Compliance


Regulations affecting the implementation of information security controls are becoming more common. For organizations in many sectors (such as healthcare, power generation, and financial services), there is specific legislation with which they must comply. These regulations do not focus on requirements for securing the perimeter of an organization's network. Indeed, they apply to all levels of an organization's information infrastructure. Relying upon securing the perimeter would likely lead to non-compliance with these regulatory requirements.

For example, consider the United States HIPAA regulation. The two sections within this regulation that impact information security professionals are the Privacy Rule and the Security Rule. Both require a variety of controls to be in place for ensuring the confidentiality and security of Protected Health Information (PHI). The Security Rule has very specific requirements for administrative safeguards, physical safeguards, and technical safeguards that must exist within all areas of the organization and network in which PHI is handled, accessed, or stored. Penalties and fines for non-compliance with these requirements can have huge impact upon an organization.

 For noncriminal violation of the HIPAA rules, including disclosures made in error, civil penalties of \$100 per violation up to \$25,000 per year, per standard, may be issued. Additionally, criminal penalties may be applied for certain violations done knowingly as follows:

- Wrongful disclosure offense: \$50,000 fine, no more than 1 year in prison, or both
- Offense under false pretenses: \$100,000 fine, no more than 5 years in prison, or both
- Offense committed with intent to sell information: \$250,000 fine, no more than 10 years in prison, or both

Also consider California's SB1386. This law requires any organization (state agency, person, or business) conducting business in California and processing personal information for California residents to disclose any information security breach to California residents whose unencrypted personal information was obtained by an unauthorized person. This legislation applies to information located anywhere, including inside the perimeter, on mobile computing and storage devices, and in any form. In 2005, 32 other states had proposed similar laws, with at least 19 states passing breach notification bills as of August 15, 2005. Different versions of the United States federal breach notification laws were also proposed. All these laws compel organizations to implement more security protection around personal information wherever it is stored.

 Privacy Rights Clearinghouse has chronicled 82 different publicized personal information breaches that have occurred since February 15, 2005—starting with the ChoicePoint incident—through September 29, 2005. They estimate close to 51 million people had their personal information compromised within the accumulation of all these incidents.

Besides HIPAA and California SB1386, other regulations such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, the European Union Data Protection Directive, and Japan's Personal Information Protection Act require many companies to protect personal information from unauthorized access, regardless of where the information is stored or handled on the network. Companies are not compliant by merely taking actions to secure their network perimeters. Information must be secured and controlled throughout the entire enterprise, and access must be controlled within the workforce to only those who have a business responsibility for the information. Organizations often give little thought to the information stored on mobile computing devices, accessed by business partners, or through any of the numerous wireless, dial-up, or third-party connections.

The number of regulatory requirements enacted to address the security of financial and consumer information continues to grow. This increasing number of laws makes it necessary for business leaders to reassess the security strategies and goals for what they have historically considered their trusted network components; those components exist within the perimeter defenses where information has until recently always been assumed to be safe. This places more responsibility upon IT security administrators to meet regulatory requirements by performing more activities with the same amount of resources. The resulting stress upon these personnel not only lead to regulatory non-compliance because of lack of resources and time but also to unhappy workers, who in turn themselves become insider risks to your internal network.

Inappropriate Technology for the Purposes Being Addressed

Oftentimes in exasperation of having no all-encompassing security solution available, organizations try to apply other technologies to address the internal network security challenges:


- Inappropriate existing encryption solutions meant to be used with email are often tried as solutions to encrypt databases in storage.
- Systems and applications are developed with security added as an afterthought, at a much higher price resource time and dollar-wise than it would have been if security had been built into the project from the very beginning.
- Routers are used internally for access control solutions within the network.
- Home brewed security “solutions” are hard-coded into applications, resulting in applications working inappropriately, or security being easily compromised.
- If the technology is new, it may not be sufficiently strong or flexible to produce the desired results or adequately protect the intended resources.
- Departmental or application-specific firewalls are used within the enterprise network core.
- Access control for large populations of users is attempted by blocking individual IP addresses.

To be effective, security solutions must be appropriate to the risks, threats, and vulnerabilities being addressed. This security within the perimeter will be layered and will typically contain the following:

- Security policy
- Incident response plan
- Host system security
- Auditing
- Intrusion detection systems
- Router security
- Firewalls
- Vulnerability assessments
- Encryption
- Applications security

Increasing Data Value Increases Threats

Data is more valuable than ever before—another significant reason for protecting data everywhere it is located. In the past few years, there has been a dramatic increase in the value of data, particularly personal data, that has led to an explosion in the number of incidents for unauthorized access to and use of information.

 The United States Federal Trade Commission reports the dollar volume of identity theft crime was \$52.6 billion in 2004. Approximately 10 million Americans had their personal information misused, costing consumers roughly \$5 billion and businesses around \$48 billion. In addition, the United States Secret Service reported actual losses to individuals and financial institutions involving identity fraud totaled \$442 million in 1995. This is an increase of 12,615% in 9 years!

There are large numbers of unscrupulous individuals who are more motivated than ever to obtain personal information to sell for profit. The black market for personal information is quite lucrative. For example, the June 21, 2005 *New York Times* reported change of billing (cob) account information is particularly valuable for information thieves; Discover Card cobs with any balance go for around \$50 for each account, and American Express, a more exclusive and potentially more profitable account, line the pockets of the information thieves for around \$85 each. There are even multiple sites, such as the now defunct sites iaaca.com and carderportal.org, that even provide lengthy tutorials to their subscribers about how to steal personal information and make massive profits.

The potential to make millions of dollars is strong motivation for many people to take advantage of the weak controls and security a company has implemented for the personal information it collects and processes. When motivated information thieves find vulnerability anywhere within a company that allows access to personal information, they take action to obtain the information. Trying to protect information only at the perimeter of a network is inadequate for trying to keep information thieves from getting to your data anywhere, any time, and using any means.

Summary

Protecting information resources within the perimeter is a business necessity. It is no longer possible to establish a network perimeter that can be a bastion of solid, impenetrable security to protect all the data safe and snug within. The perimeter is porous—this idea is no longer a debatable opinion, it is a fact. Tribal thinking must change. Smart business leaders can no longer blindly trust all their personnel; not everyone within your organization wants, or plans, to be a permanent member of your team. Mobile computing has expanded your information universe—you now have highly valuable information boldly traveling and going far beyond your perimeter to locations and storage devices like never before and like you never expected.

The time is now for business leaders to take a holistic approach to securing the entire enterprise that complements and supports regulatory requirements as well as protects each internal component of the network. Doing so in harmony will minimize costs and improve productivity.

Multi-dimensional security provides a holistic approach to securing your enterprise data. Multi-dimensional security protects information assets and associated resources within all areas of your enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter but also wherever information is stored, processed, or transmitted. Multi-dimensional security employs not only technology solutions but also operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

Organizations must change their thinking from a secure-the-perimeter-only perspective to one that is a multi-dimensional enterprise-wide security strategy. They must start viewing their organizations as being comprised of numerous islands of information, each of which must be appropriately secured. We will explore this strategy in the next chapter.

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/>.