

Realtime
publishers

"Leading the Conversation"

The Definitive Guide™ To

Information Theft Prevention

sponsored by

Blue  **Coat**[®]

Dan Sullivan

| | |
|---|-----|
| Chapter 8: Best Practices to Prevent Information Theft | 151 |
| Enhanced Information Security Paradigms | 151 |
| Limits of Device-Centric Security Models | 152 |
| Parallel Models: Traditional Physical Security and Digital Security | 152 |
| Protecting Information Wherever It Goes..... | 153 |
| Protecting Information During Transmission | 154 |
| Protecting Information Once It Arrives | 156 |
| Emergence of On-Demand Security | 158 |
| Organizational Issues | 160 |
| Policies for Preventing Information Theft | 160 |
| User Education About Information Theft | 166 |
| Technical Responses to Information Theft | 168 |
| Comprehensive Security Management for Preventing Information Theft | 168 |
| Network Security | 169 |
| Managed Device Security | 170 |
| Unmanaged Device Security..... | 170 |
| Deploying On-Demand Security Systems | 171 |
| Summary | 171 |
| Download Additional eBooks from Realtime Nexus! | 171 |

Copyright Statement

© 2006 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.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 Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.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.

Realtimerepublishers.com and the Realtimerepublishers 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 Realtimerepublishers.com, please contact us via e-mail at info@realtimerepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 8: Best Practices to Prevent Information Theft

Information security is often understood as having three objectives: protecting the confidentiality of information, preserving information integrity, and ensuring information availability; security measures often help to address more than one objective. However, as a result of changes in the way organizations use and deploy information, there is a growing need for additional security measures directed at protecting the confidentiality of information.

This chapter concludes the examination of information theft prevention by exploring

- The need for a refined security paradigm to prevent information theft
- Organizational issues that influence the success of information theft prevention programs
- Technical responses to the threat of information theft

As information assets are used in new and more flexible ways, you must accompany those new uses with appropriate security to ensure confidentiality and privacy are not compromised.

Enhanced Information Security Paradigms


Security measures are dictated by the value placed on information and the ways in which the information is used. For example, when information is stored on physical media, such as paper, security focuses on protecting the tangible assets that store the information. When information is transferred between secure systems, additional measures, such as encryption, are required. When confidential information is copied to unmanaged devices with unknown security profiles, even more security measures are required.

Patterns of information access and use have changed, creating new points of vulnerability. This, in turn, has created the need for additional countermeasures to mitigate the risk from those vulnerabilities. To understand the scope and extent of these changes, let's examine three factors shaping the development of an enhanced information security paradigm:

- The limits of device-centric security models
- The need to protect information wherever it goes
- The emergence of on-demand security

Limits of Device-Centric Security Models

Securing information is not a new challenge. For generations, warring factions, competitive businesses, and most recently nation-states have taken steps to keep information confidential. Safes, or “iron chests” as they were called, were used to protect valuables from theft. Julius Caesar supposedly used a simple substitution cipher to communicate with his armies. Today, we use similar patterns for protecting our assets. If the asset is stationary, we lock it up; if we need to transmit information, we scramble it so that no one but the sender will understand it. This model has worked well and will continue to serve many of our needs but is not sufficient for protecting against information theft today.

 For more information about historical ciphers, see The Trinity College Historical Cryptography Web site at <http://starbase.trincoll.edu/~crypto/>.

Parallel Models: Traditional Physical Security and Digital Security

Consider a simple example of protecting written information. The need to do so has existed throughout history and is just as relevant today as it was when people first started keeping secrets in written form. If you have written information that you want to keep confidential, you can use tried-and-true physical security measures. Papers and folders can be locked in office safes or stored in locked vaults protected by security guards and surveillance equipment. If people need access to the information, they must go to it. In the process, they would presumably pass through multiple checks to verify that they have legitimate access to the information and that they are not bringing in devices that could damage the medium (for example, scissors, matches, and so on). They would also have to demonstrate that they are authorized to view the information, perhaps by knowing the combination to the safe that stores the documents. Finally, measures would be in place to ensure that they do not remove information from the secure area in an unsecured way; for example, the person could not make notes, copy documents, or scan materials. This model for physical security has been applied to electronic information.

The common characteristics between the physical security example and electronic and optical data storage include:

- Access to information is protected by multiple layers of controls
- Users must demonstrate that they are authorized to access information, such as by knowing the combination to a safe or having a username and password to access a system
- Authorizations are limited, for example, certain users can view information but not change it
- Activities are monitored, either by surveillance devices and physical alarms in the case of physical security, or through the use of audit trails and event alarms in the case of electronic information

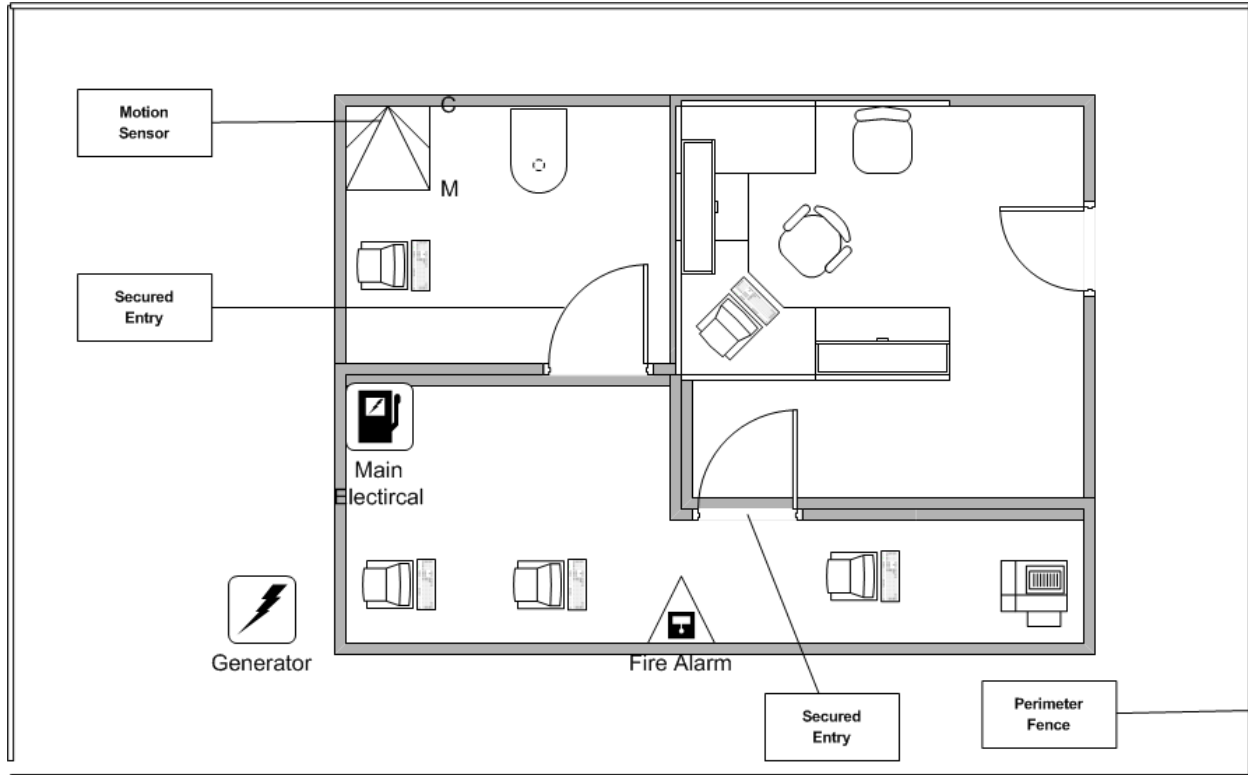


Figure 8.1: Physical security measures, such as locked doors and motion sensors have analogs in electronic security, such as access controls and audit trails.

This model is effective when the information is restricted to the protected area established with safes, vaults, guards, and other measures. How can information be protected when it is no longer in the protected area? Encryption is the standard technique for protecting information when it is not within a trusted area.

Protecting Information Wherever It Goes

When information is not within a trusted, secured zone, you must take additional steps to ensure it is not compromised. In broad terms, there are two points at which an attacker could steal or compromise information once it has left a secure area:

- During transmission
- After arrival

These require fundamentally different approaches.

Protecting Information During Transmission

You cannot prevent all possible ways in which an attacker might intercept information as it is transmitted from one secure point to another. For example, you cannot prevent an eavesdropper from gaining access to your ISP and monitoring your Internet traffic. Early wireless protocols are easily cracked. To complicate matters, someone could masquerade as you and engage in fraudulent activities using your identity.

Clearly, you need to deploy additional measures to protect your information and the integrity of your operations. At the very least, you want to ensure that the information remains confidential and that it is not changed in any way prior to receipt. Encryption, and related techniques such as message digests, provides the necessary protections, including:

- Keeping information confidential by transforming it from intelligible information, such as text or an image, to unintelligible string of bits.
- Allowing only those with keys to transform the unintelligible string of bits back to the original form so that even if a communications channel is compromised and someone intercepts the transmission, the interceptor will not be able to make use of the data.
- Allowing senders to digitally sign transmissions so that recipients can be confident that the message was sent by the apparent sender and has not been tampered with en route to the recipient.

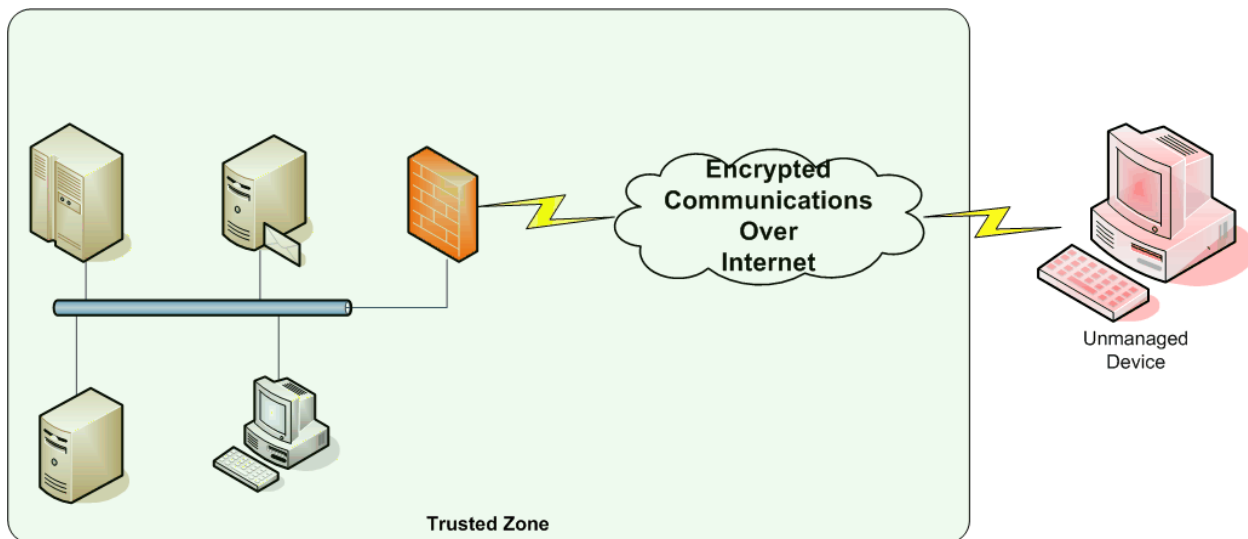


Figure 8.2: Encryption and related technologies, such as VPNs, extend the scope of trusted zones over the Internet but do not ensure security on unmanaged devices.

Encryption protects information until it is decrypted. At that point, the level of protection provided by the decrypted data is based on the security of the area or the device that contains the information. If a secret message from an overseas diplomat is decrypted in a secured facility managed by an intelligence agency, there is probably little concern about the information leaking. It is a different matter if confidential legal documents are downloaded to an attorney's home PC, which happens to be shared with her teenage children who are fond of using peer-to-peer file-sharing programs.



Remember one of the fundamental principles of information security: A system is only as secure as its weakest link.

Limits of Cryptography

Cryptography is the practice of developing secret codes to protect information. Modern ciphers, or algorithms used to encrypt data, employ parameters known as keys. Unless one knows the appropriate key, one cannot decrypt a message. All ciphers are vulnerable to brute-force attacks, which try all possible keys to find the one that decrypts a message. To mitigate this risk, cryptographers use keys so long that it is impractical to try all possible combinations. The only problem is that the definition of "impractical" changes over time.

Consider the Data Encryption Standard (DES) encryption algorithm. The algorithm was adopted as an ANSI standard in 1978 using 56-bit keys. DES continued as a popular encryption mechanism for both government and commercial use until 1988 when it was no longer endorsed by the National Security Agency (NSA). In 1998, the Electronic Frontier Foundation used a custom parallel computer and broke DES encryption in 3 days. (Details of the project are described in the book *Cracking DES*, available for free online at <http://cryptome.org/cracking-des.htm>). Another group of researchers cracked DES in 1997 using a distributed system that used computers on the Internet. (See "A Brute Force Search of DES Keyspace" at <http://www.interhack.net/pubs/des-key-crack/> for more information.) DES is no longer used for secure communications and has been supplanted by several others, including:

- Triple DES, which is based on DES but is much more secure, using a 168-bit key
- Rijndael, which replaced DES as the national encryption standard, was selected for the Advanced Encryption Standard (AES)
- Blowfish, a block cipher with keys up to 448 bits
- RC5, a block cipher with keys up to 2048 bits

The new encryption algorithms use such long keys that brute-force searching is not practical by today's standards. Other techniques, however, can be used to try to break code. These include:

- Differential cryptanalysis, the study of how changes to the input stream cause changes in the encrypted message
- Integral cryptanalysis, used on ciphers not vulnerable to differential cryptanalysis
- Linear cryptanalysis, which studies linear bit-wise functions that relate input and output bits

Even with these techniques, modern ciphers are expected to withstand all but the most determined attacks. In the future, other techniques, perhaps based on quantum computing or another theoretically possible method, may make brute-force attacks on large key encryptions practical.

Protecting Information Once It Arrives

Device-centric security protects information as long as it is not transmitted outside of a secured zone that contains only secured devices and secured communication channels. Encryption protects information during transmission. What about information that has been transmitted from a secured device, over a secured channel, and decrypted on a device with unknown security measures?

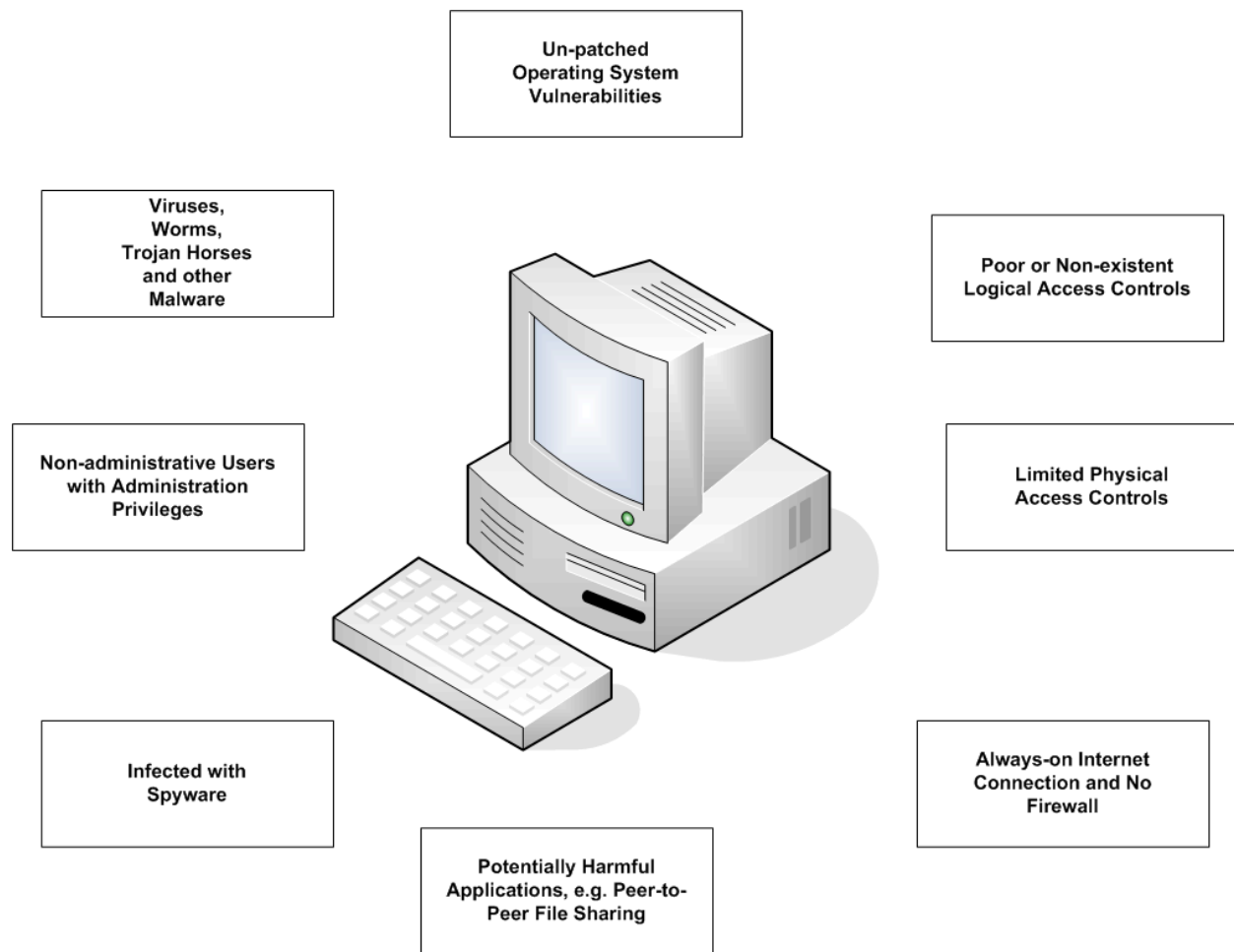


Figure 8.3: Unmanaged devices are subject to a wide range of vulnerabilities.

There are several potential problems, including:

- Unencrypted information could be intentionally stored on an unsecured device allowing unauthorized users to view the information. For example, a manager may download a strategic plan and save it to the hard drive of a hotel business center PC.
- Unencrypted information is stored unintentionally on an unsecured device. Internet browsers often cache pages for rapid retrieval; a confidential email message read using a Web email application may stay in the cache long after the recipient has left.
- A device may be infected with malware designed to steal information. Keyloggers and video frame grabbers fall into this category.
- Confidential information may be downloaded to devices that have not been sufficiently patched and are vulnerable to a variety of attacks to which the device originally storing the information is not subject.
- Confidential information may be included with backups performed on the device, leaving existing copies of documents that can no longer be tracked and governed by document retention policies and procedures

These problems occur because the security measures you have come to depend upon are device centric. Consider the common security mechanisms that Table 8.1 shows and the methods by which they enhance security.

| Security Measure | Purpose |
|--------------------------------|---|
| Firewall | Limit network traffic based on protocol, origin, and other properties |
| Intrusion prevention (network) | Detect and block attacks on network services |
| Intrusion detection (host) | Detect unauthorized changes to critical OS and application files |
| Content filtering | Block access to banned sites; detect unwanted content, such as spam and phishing messages |
| Anti-malware (network) | Filter network traffic for viruses, worms, Trojan horses, keyloggers, rootkits, and other malware to prevent it from reaching servers and workstations |
| Anti-malware (host) | Filter incoming email, instant messages, and other traffic that may contain malware—this is especially important for mobile devices that may not always have the protection of network-based anti-malware solutions |
| Access controls | Limit access to systems and information to known users and control the operations users are allowed to perform on various resources |
| Audit controls | Log information about important activities such as login failures, changes to OS parameters, and deleted or modified data |

Table 8.1: Device-centric security measures and their functions.

These security measures are tied to devices that are under the control of organizations. You must add to this repertoire measures that apply to unmanaged devices as well.

Emergence of On-Demand Security

On-demand security is based on the idea that security should be associated with information and devices rather than devices alone. It also entails the idea that security measures should not require elaborate installation and maintenance on access points to information.

The evolutionary precursor to on-demand security is VPN technology. VPNs are widely deployed for protecting a wide array of applications and data. VPNs are essential elements to many IT infrastructures. Although VPNs are useful and will continue to be so in many cases, there are some limitations, including:

- The need to install client software on access devices. This, in turn, often requires administrator privileges. IT managers then have the choice of either granting elevated rights to users so that those users can install the application (generally a bad idea to say the least) or incurring additional support costs to have IT service personnel install the software.
- VPNs provide secure tunnels for communication but do not verify or ensure the security of the client devices.
- VPNs that are based on application-layer HTTPS reverse proxies may not support all applications that could use an Internet connection.
- A VPN connection may be established on devices that are running keyloggers or frame grabbers, potentially defeating the purpose of the VPN by exposing confidential information after it is decrypted and used on the client device

Information security is a constantly developing field, so it should be no surprise that VPN technology can be improved. It is those improvements that distinguish on-demand security. The fundamental characteristics of on-demand security measures are:

- Security is tightly coupled to data as it moves through a networked environment.
- Prior to exposing protected information to potentially insecure devices, security checks are performed to ensure compliance with security policies.
- Suppression of information stealing programs, such as frame grabbers and keyloggers, enables protection from those programs copying information.
- Permanent changes are not made to the client device; on-demand security measures exist only as long as the session.
- Application integrity checks and whitelists and blacklists prevent the use of programs that violate security policies. For example, confidential files may not be downloaded while a peer-to-peer file-sharing program is running on the client device. Integrity checks can be done with message digest checks to ensure programs have not been modified, maliciously or unintentionally.
- Security can be applied on a session level. For example, a salesperson can have a secured session working with the corporate customer database while using an unsecured browser session for researching customer information on public Web sites.

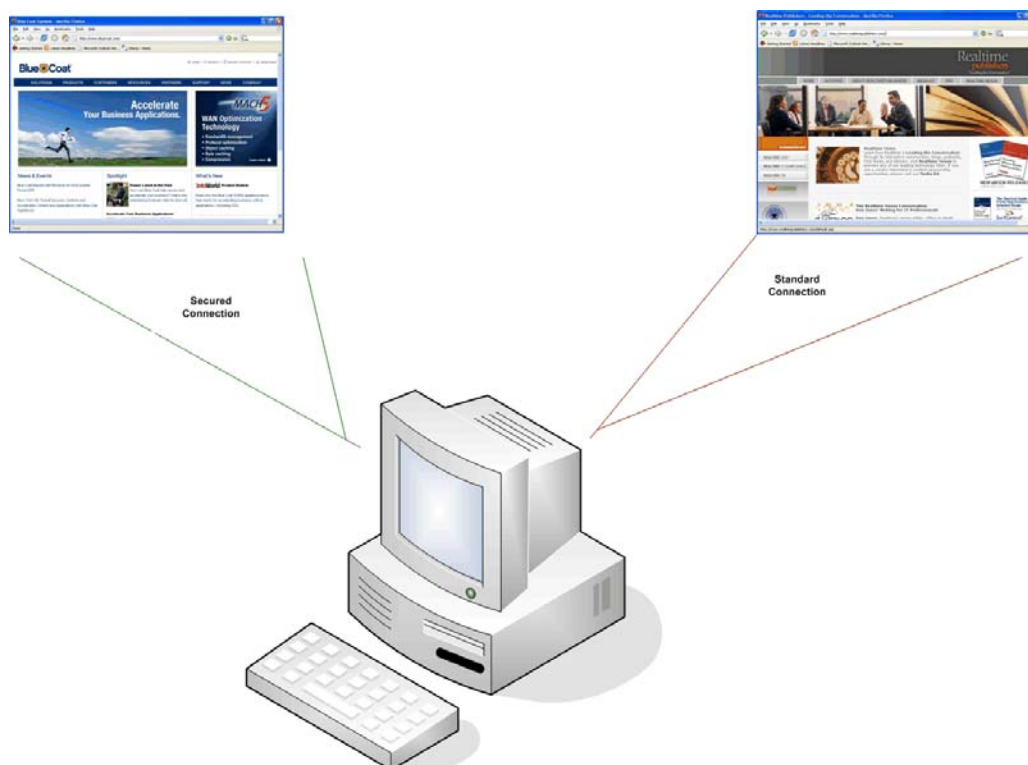


Figure 8.4: On-demand security should provide session-level security that does not interfere with other operations.

The traditional model of information security is device centric. Security measures are deployed on networks, servers, and managed devices to protect the information that moves through those systems. Encryption technologies, such as VPNs, are used to protect information as it moves through unprotected channels, such as the Internet. When information moves from a trusted zone (such as a corporate headquarter network) to another trusted zone (such as a regional office), the information is always protected to the level dictated by organizational policies and implemented by IT procedures.

This model does not address how to secure data when it leaves a trusted zone and is made available in an unencrypted form on an unmanaged device. From a security perspective, you can say nothing definitive about the security of the client, except that you do not know whether your information is secure.

By definition, unmanaged devices are controlled by someone else. You cannot dictate security policies for those devices. Business partners may have higher risk tolerances when it comes to information security; employees may be perfectly comfortable running a personal computer without a firewall and with out-of-date antivirus programs. On-demand security has emerged as a means of balancing the need to protect information assets with the need to sometimes provide that information on devices that may be compromised. One of the first steps to implementing on-demand security is formulating the policies and procedures that will govern its use.

Organizational Issues

On-demand security can be deployed in many ways and the methods that work best for one organization may not work for others. Customization of on-demand security can be broken down into two basic steps:

- Developing policies for preventing information theft
- Educating users on the need for information security

Although these two steps are outside of the technical realm that is often the focus of information security discussions, these are just as important. Remembering that any security system is only as strong as its weakest link, you must attend to the need for policies to drive implementations and the need for training to minimize the chances of unintentionally undermining the security measures put in place.

Policies for Preventing Information Theft

Security practices should be guided by policies. The policies, in turn, should be developed based on the needs, risk tolerances, and resources available to an organization. In the case of on-demand security, the factors that will influence the formulation of policies include:

- The amount of information exposed to unmanaged devices
- The sensitivity of information exposed to unmanaged devices
- Regulatory and other compliance requirements related to information exposed to unmanaged devices
- The types of applications made accessible from unmanaged devices

The more information that is exposed to unmanaged devices, the greater the need for formal policies governing what security measures are required. Volume alone is not sufficient for determining security requirements. For example, if users are accessing internal Web sites that provide basic human resources information, submitting vacation requests, and performing other administrative functions, security requirements are lower than cases in which sensitive information is transferred to unmanaged devices. Sensitive information includes customer account information, personnel data, marketing plans, design documents, and other confidential or proprietary information. These are the type of factors that will drive the direction of security policies.

Several policies should be defined in relation to on-demand security:

- Third-party access policy
- Remote access policy
- Mobile device policy
- Information sensitivity policy
- VPN security policy

These will provide the foundation for implementing on-demand security and related measures to minimize the threat of information theft.

Third-Party Access Policy

A third-party access policy defines the requirements on external users and the limits to their potential use of information resources. This policy should begin with a definition of what general security measures are expected of third parties. The policy should not define how third parties implement security within their own infrastructures, but it can define the minimal levels of security expected. For example, the policy may state that third-party users agree to use basic security measures, such as firewalls and antivirus software, to protect any device used to connect to the target network and servers. Whether the third party uses personal firewalls on individual machines in addition to a network VPN or local antivirus or network-based antivirus measures is up to them.

The policy should also call for a description of how the third-party access will be used and for what business purpose. IT security personnel should review the plan to ensure that the plan does not create unnecessary risks. Third-party organizations should agree to notify the organization granting access if the employee, contractor, or consultant accessing the target system is terminated or for another reason no longer needs to use the target system.

The policy should define the responsibilities of application managers and systems managers responsible for systems with third-party access. These can include:

- Periodic review of access control logs
- Audits of active accounts
- Use of host-based intrusion detection systems

Some of these same principles apply to remote access policies as well.

Remote Access Policy

A remote access policy generally applies to employees, contractors, and consultants who work both on and off site, or primarily off site. As with the third-party access policy, the goal is to ensure that those with access to the system understand their responsibilities and the limits of acceptable use as well as to define what is expected of IT staff in maintaining the security of remote access. The remote access policy should include:

- A statement about the acceptable use of a remote connection. For example, remote connections should be used only for the same types of activities that are performed when using on-site devices.
- A description of what measures the employee, contractor, or consultant is expected to take to preserve the security of remote devices.
- A list of any restriction on the remote access device. For example, only company or agency issued devices can connect to the network. The user cannot access other sites while connected to the target network using split tunneling. The user cannot access public email sites, such as Yahoo!, Hotmail, and AOL, while remotely connected.
- A description of any access control limitations on remote access. For example, root or administrator access may be disabled for remote connections.
- Appropriate use of wireless networks

Remote access policies also apply to mobile devices, but mobile devices have additional security issues that should be addressed in another policy.

Mobile Device Use and Access Policy

The purpose of a mobile device policy is to define steps users should take to protect information on mobile devices, such as notebook computers, PDAs, and smart phones. The policy should address:

- What types of organization information are allowed on managed devices, such as company-issued notebooks, and unmanaged devices, such as employee-owned smart phones
- Requirements for encryption on mobile devices
- Requirements for patching the OS and applications
- Requirements for running anti-malware software, at least when the mobile device is not connected to a secured network
- Procedures for reporting the loss or theft of a mobile device that holds confidential information.

Mobile devices often use wireless network connections and are therefore subject to wireless communication policies.

Wireless Communication Policy

A wireless communication policy should be designed to minimize the risk of rogue wireless devices accessing the network or attackers eavesdropping on communications between devices.

A wireless communication policy should include:

- A list of acceptable encrypted wireless protocols; for example, Wi-Fi Protected Access (WPA) may be acceptable but the weaker Wired Equivalent Privacy (WEP) is not
- Responsibilities of systems administrators for registering and monitoring wireless access points
- Requirements for vulnerability testing and auditing of wireless devices
- Access control rules, such as only devices with specific MAC addresses are allowed to use the wireless network

The wireless policy may also include statements about the importance of not installing unapproved wireless access points, even for short periods of time. If they are not configured properly, they could become an avenue for stealing information. This is especially problematic when sensitive information is transmitted on wireless networks.

Information Sensitivity Policy

Not all information is equally important, useful, or confidential. An information sensitivity policy defines categories of information based on the amount of protection each group should be given. The military, for example, use a 5-category classification:

- Unclassified
- Sensitive but unclassified
- Confidential
- Secret
- Top secret

Commercial and non-military government agencies might use another scheme such as:

- Public
- Sensitive
- Private
- Confidential

The information protection requirements of these categories vary from minimal, or even non-existent, to extensive.

Public Information

In this categorization scheme, public information is freely available outside the organization. Press releases, product catalogs, and regulatory filings are examples of public information.



Public information is not just what is freely disclosed; compulsory disclosures dictated by government regulations can fall into this category as well.

Public information does not require special protection.

Sensitive Information

Sensitive information is information that an organization would rather not have disclosed but would not cause significant harm if it were disclosed. For example, a company may be negotiating with several suppliers for office furniture and would rather keep the names of the bidders within the company; however, if the names of the bidders were revealed, it would have minimal impact on the company, perhaps by influencing how bidders respond knowing the competitive position of the other bidders. Sensitive information is protected with some measures of access controls but not subject to the level of control reserved for private and confidential information.


Private Information

Private information is personal information about employees, customers, patients, clients, or others doing business with a company or agency. Private information includes:

- Names
- Home addresses
- Social Security numbers
- Protected healthcare information
- Salaries
- Personal financial information

In response to growing concern over the loss of privacy and the threat of identity theft, privacy regulations have increased. The response has come from all levels of government; from state to federal governments to transnational governing bodies, and includes:

- California Senate Bill (SB) 1386, which enacted legislation requiring organizations to disclose to individuals if a security breach disclosed personally identifying information.
- U.S. federal government, which has enacted targeted regulations such as the privacy and security rule of the Health Insurance Portability and Accountability Act (HIPAA), which addresses protected health information, and the Gramm-Leach-Bliley Act, which regulates financial services companies.
- The countries of Canada and Australia, which have enacted personal privacy protection laws.
- The European Union, which has issued directives on the collection and distribution of personal information on citizens of member countries.

 For more information about privacy regulations, refer to the following sites:

HIPAA at <http://www.hhs.gov/ocr/hipaa/>

California SB 1386 at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Gramm-Leach-Bliley Act at <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

Canada's Privacy Act at <http://lois.justice.gc.ca/en/P-21/255104.html>

Australia's Privacy Commissioner at <http://www.privacy.gov.au/>

European Union Privacy Directives at http://www.cdt.org/privacy/eudirective/EU_Directive_.html

Private data may be dictated by government regulation, but confidential information is often dictated by business requirements.

Confidential Information

Confidential information includes trade secrets, strategic plans, pending marketing campaigns, and a host of other information that, if revealed, could cause serious harm to a company or agency. Information in this category requires the most stringent protection. Access to this information should be on a need-to-know basis. The copying and distribution of this information should be strictly controlled. Confidential information should not be revealed to individuals who have not agreed to non-disclosure terms defined by the owner of the protected information.

How organizations decide to categorize information will vary and, over time, may even vary within the organization itself. The important point of the information sensitivity policy is to establish a method for identifying different types of information with regards to sensitivity and to ensure that information is protected to the appropriate level. One of the measures typically taken to protect all categories of information when it must be transmitted to remote locations is to use a VPN.

VPN Policy

A VPN policy defines when and how virtual private networking is used. Some key elements of a VPN policy are:

- Access controls, specifically, how will users authenticate to the VPN; for example, is two-factor authentication required?
- Which devices are allowed to use VPN software. Many organizations will only allow VPN client software on managed devices and not, for example, on personal notebooks or home computers.
- Restrictions on activities that can occur while the VPN connection is active; for example, users may not surf the Web on another connection to the Internet.
- Expectations for preserving the integrity of the client device, such as the need to run antivirus, anti-spyware, and personal firewalls.

Policies are the starting point for defining an information security strategy. The advent of on-demand security requires a host of policies for technologies and practices that support on-demand security. On-demand security is easing the burden of implementing these policies, especially information sensitivity policies, but it does not eliminate the need for them. One important aspect of policies that can be overlooked is that users need to be made aware of the existence of policies and may need training on how to implement them.

User Education About Information Theft

Users can play an enabling role in acts of information theft. Choosing weak passwords, leaving confidential information unencrypted, and sharing accounts are all ways a well-planned security program may be compromised. Training users about information theft prevention should include:

- Organization policies
- Information classification
- Security practices
- Responses to security incidents

These four areas form the foundation of securing information from the unintentional consequences of careless or uninformed user actions.

Educating on Organization Policies

Once policies are defined, users should be made aware of them and the most relevant details, from their perspective, should be highlighted. Some elements of a security policy will not be relevant to users, such as systems administrators' responsibilities for monitoring logs, but others directly govern allowable user actions. For example, when a VPN is used to access the corporate network, users should not simultaneously surf the Web using another network connection. The most important topics to point out to users include statements governing:

- The need for up-to-date antivirus and firewall programs
- The need to update OS patches as soon as they are received (presumably service support determines which patches are necessary and pushes them to the client devices)
- Restricted activities while connected to the organization's network, such as accessing public email systems like Yahoo!, Hotmail, and AOL
- The use of encryption for confidential information on mobile devices, including notebook computers and PDAs

The last point is especially important. Recent disclosures about laptop computer thefts have highlighted the need to protect confidential information on mobile devices.

Information Classification

Users of information must understand its sensitivity. It is not sufficient to protect access to information with elaborate authentication and authorization mechanisms if users copy or print controlled information and distribute it by other means. Consider the example of a health insurance company that contracts with a third-party claims processing company. To protect its customers' protected healthcare information, the insurance company may require multi-factor authentication, VPN-only access to database applications, and strict policies on the use of patient's healthcare information. An employee of the third-party claims processor prints reports, works on some in the office, and takes others home to work on but forgets his brief case on the subway ride home. The well-protected information is now exposed and out of the control of the companies responsible for it.

Employees, contractors, consultants, and business partners should be trained on:

- Information classification in the organization
- What kinds of information fall into each category
- Acceptable uses with information in each category
- Restrictions on what can be done with sensitive, private, and confidential information

Poor understanding of information sensitivity can render users of information the weakest link in the security system.

Security Practices

Users should not need to become experts in computer security, but they should have a basic understanding of the threats that exist. By now, most people are aware of viruses. They may not be aware of the technical details of how malware works or even the various types of malware, but they know that viruses exist and countermeasures are available to combat them. That is base level of understanding you should expect. The other areas that users should understand are:

- The need to protect mobile devices from theft. Private and confidential information can be compromised unless it is encrypted.
- Unapproved applications should not be installed on managed devices; they may introduce Trojan horses or other malware.
- Social engineering techniques, such as an attacker pretending to be a service desk technician and calling a user asking for a password or masquerading as an agent for a courier delivery service and asking to pick up a laptop for delivery to another office.
- Phishing attacks are becoming more sophisticated. Users should not disclose personal or company confidential information on Web sites unless they are sure of the authenticity of the site.
- How to respond to a suspected security breach

The last item warrants a formal procedure.

Response to Security Incidents

Incident response requires its own well-defined policy and set of procedures that govern how IT staff should handle a security breach; however, in this context, the concern is with non-IT users who suspect a possible security incident. Users should understand the basics of responding to a possible security breach, including:

- Notifying information security staff immediately if a device is stolen or an account password is compromised. Security staff and systems administrators may be able to take steps to control the damage. For example, if a notebook computer is stolen, the MAC address of the device could be denied access to all wireless networks in the company.
- Disconnecting a device from the network if suspect suspicious activity is suspected.
- Not deleting any files or data; computer forensics staff may be able to better understand an attack by analyzing tracks left by the attacker. If legal action is pursued, the forensic evidence may be needed.

The burden of responding to security breaches rests with IT, the goal of user education is simply to ensure that IT's job is no more difficult than it is already.

Preventing information theft depends in part on an organization's preparation. Having well-defined policies and procedures in place, along with keeping users informed about security threats and their responsibilities to minimize those threats, is one element of a comprehensive information security practice. Another element is the technical measures taken to counter those threats.

Technical Responses to Information Theft

As the previous sections of this chapter have demonstrated, there has been a fundamental shift in the way information is accessed and therefore, how it must be protected. Organizational policies that address new models of access, including the use of VPNs and on-demand security, are one part of the response to the evolving threat of information theft. The technical responses, implemented as part of the process of executing security policies, are the other component of the response. Let's turn our attention to best practices in comprehensive information security management with particular attention to deploying on-demand security systems.

Comprehensive Security Management for Preventing Information Theft

A comprehensive program for preventing information theft should address security measures that protect devices that store and transmit information as well as measures that protect information when it moves from managed devices. Such a program can be divided into three areas:

- Network security
- Managed device security
- Unmanaged device security

Each area may be managed with a series of best practice measures.

Network Security

Network security addresses two problems of protecting information: ensuring its confidentiality and integrity as it is transmitted and ensuring the network is not used to attack information or devices. Well-established components of network security are still relevant today, and include:

- Firewalls
- Intrusion detection and prevention devices
- Content filters
- Web and email proxies
- VPNs

Some of these devices, especially content filters and proxies, are becoming more sophisticated in response to increasingly complex threats. A proxy, for example, acts as a gatekeeper between the secured network and the outside network. A traditional packet-filtering firewall does the same thing but at a lower level. As Figure 8.5 shows, the higher up in the network stack the countermeasure operates, the better it can assess threats.

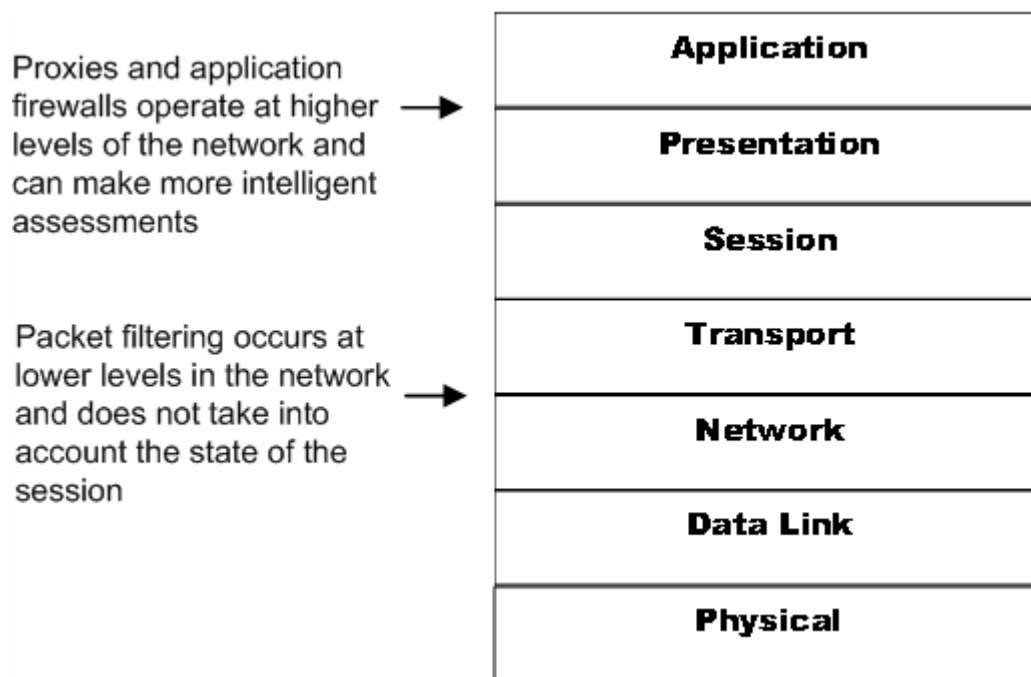


Figure 8.5: One response to increasingly complex threats is to deploy countermeasures that work at higher levels of the OSI model network stack.

Best practices in network security require a combination of countermeasures, each designed to counter particular types of threats. Even with a protected network, it is important to deploy security measures to individual devices as well.

Managed Device Security

Managed devices are under the control of security policies and should take advantage of a variety of security measures. Client devices, such as workstations and notebook computers, should use all or most of the following:

- Antivirus software
- Anti-spyware software
- Personal firewalls
- Access controls
- Password policies that enforce minimal strength of password, password lifetime, and reuse of passwords

Servers should deploy these same measures as well as additional measures, such as

- Host intrusion detection
- Auditing of significant OS events (dependent upon organization requirements)
- Triggers and alarms to notify administrators in cases of significant security events
- Audits of access controls, including user accounts, file permissions, and shared drives

With managed devices, IT can define and implement appropriate security measures for devices.

Unmanaged Device Security

There are several core steps to protecting information before it is sent to an unmanaged device, these include:

- Installing initial components of on-demand security mechanisms. This should be done without user intervention and not require elevated privileges, such as local administrator rights, on the unmanaged device.
- The unmanaged device should then be scanned for spyware, video frame grabbers, keyloggers, and other malware that could enable information leaks. If problems are detected, the malicious program should be disabled or the session terminated.
- Determine the security posture of the device by checking for anti-spyware, personal firewalls, and an appropriately patched OS.
- Authenticate the user. Based on the user's authorizations and the security posture of the devices, disable functions that pose security vulnerabilities. For example, a user may be allowed to read email from a kiosk computer but not download and save attachments to a locally connected USB drive.
- Encrypt all communications between the unmanaged device and servers using a VPN.

Once the user has established a secure zone within the unmanaged device, the user can proceed to access applications and information. For additional security, information that must reside on the unmanaged device—for example, in a Web browser cache—should be encrypted. When the session terminates, all information related to the session should be purged from the unmanaged device.

Deploying On-Demand Security Systems

On-demand security systems complement VPNs and other security measures taken to protect information security. Like VPNs, on-demand security devices can operate as appliances within the network. Unlike some VPNs, which require client software installation, on-demand security by its nature should be downloadable and configurable without administrative rights to an unmanaged device. Ideally, on-demand security components would be integrated with VPNs, minimizing the number of devices that must be supported.

Like other network appliances, the deployment of on-demand security devices requires:

- Well-defined policies that describe how the system is used
- Placement within a secure area of a network (that is, behind a firewall) to protect the integrity of the device
- Monitoring and patching as needed
- Reviews of event logs to both detect significant events and to understand trends in the use of the on-demand security system

On-demand security systems will require information about users and their authorizations. Additional user attributes may be needed in organization directories (such as Active Directory—AD—or a LDAP directory) to allow for finely tuned policies controlling the features enabled on unmanaged devices. Advances in IT are creating new ways to steal and unintentionally leak information; however, similar advances are improving our ability to counter those threats.

Summary

Information theft is a legitimate concern for organizations. Personal information could leak leaving a company liable for violation of privacy regulation. Trade secrets could be stolen or exposed unintentionally, risking the loss of an important competitive advantage. IT professionals have deployed a wealth of security measures and defined policies to mitigate risks and adapted these as changing circumstances warrant. Today, the need to protect information extends beyond the network perimeter to home computers shared by employees and their children, customers accessing their accounts online, and business partners with varying degrees of security.

IT has long protected information assets, at first by controlling physical access to computers and then deploying basic access controls in shared computing environments. As networks proliferated, network security measures such as firewalls were added to create perimeter defenses. The perimeter is now more porous than ever, and IT professionals are responding with new security measures using on-demand security. Information security is no longer tethered to managed devices, security controls can go where information goes.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.