

# SECURITY

## REFERENCE GUIDE



Keeping information  
confidential, intact and  
accessible when threats emerge

[CDWG.com/securityguide](http://CDWG.com/securityguide) | 888.510.4239



The Right Technology. Right Away.®

# SECURITY

## REFERENCE GUIDE

### WHAT IS A CDW•G REFERENCE GUIDE?

At CDW•G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology. Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

» We are pleased to also offer the **CDW•G IT Investment Guide**. It includes products and information to help you meet your security objectives.

#### TABLE OF CONTENTS

#### CHAPTER

<b>01</b>	<b>The Current Security Threat Environment.....</b>	<b>3</b>
	• New Approaches — Traditional Threats	
	• A New Security Focus — Data	
<b>02</b>	<b>Risk Assessment and Compliance.....</b>	<b>5</b>
	• Determining Risk	
	• The Process of Assessing Risk	
	• Compliance Considerations	
	• Security as a Process	
<b>03</b>	<b>Threat Prevention.....</b>	<b>9</b>
	• Reducing Risk	
	• Multilayered Security Approaches	
<b>04</b>	<b>Data Leakage Prevention .....</b>	<b>13</b>
	• Data Leak Opportunities	
	• Removable and Portable Media	
<b>05</b>	<b>Secure Remote Access .....</b>	<b>25</b>
	• Varieties of Remote Access	
	• Threats to Remote Access	
<b>06</b>	<b>Endpoint Security.....</b>	<b>29</b>
	• Varieties of Endpoints	
	• Threats to Endpoints	
	<b>GLOSSARY .....</b>	<b>33</b>
	<b>INDEX .....</b>	<b>35</b>

# THE CURRENT SECURITY THREAT ENVIRONMENT



## CHAPTER 1:

.....  
New Approaches — Traditional Threats  
.....

A New Security Focus — Data  
.....

For better or worse, the security field changes rapidly. It differs from mainstream IT work in that predicting the next challenge proves quite difficult. Threats appear to come out of nowhere, and incidents seem to strike at random.

On the other hand, like all areas of IT, security as a discipline constantly builds on itself, rarely taking a step backward. In particular, over the last year we've seen attacks used in new and complex combinations, growing sophistication in online criminal activities, and an escalation of the ongoing arms race between the developers of malicious software and the creators of defensive tools.

These developments have either overwhelmed some traditional security measures or made them irrelevant. As a result, organizations have had to change their tactics in order to cope.

## NEW APPROACHES — TRADITIONAL THREATS

Over the past year, attacks on websites have grown more sophisticated despite the fact that they don't involve new exploitation techniques. Instead, attackers are now combining older, well-known methods in new combinations.

One example of particular interest has been the use of SQL injection and persistent cross-site scripting flaws in websites to compromise end-user workstations.

A typical dynamic website divides its functionality into layers:

- The database layer stores the various facts and other information to be presented via the website (for example, products in inventory).
- The application layer accepts queries from users, retrieves information from the database and presents it back to users.

This extremely common architecture is prone to abuse if user input is not properly handled. The following is a typical exchange where a user requests a page. (For this example, the application is implemented in "classic" ASP and uses SQL Server as a back-end database.)

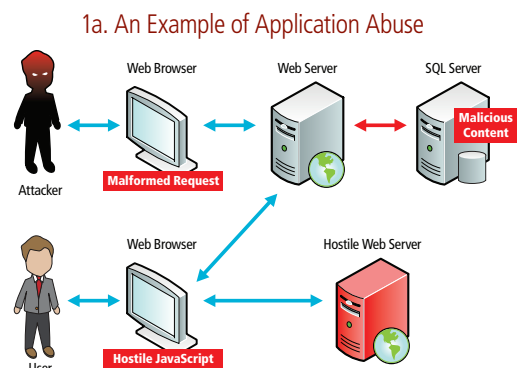
1. The user clicks on a link in the web page, generating a request to the web server.
2. The web server accepts the request, and the .ASP application composes a SQL query to the database in order to gather the information that the user seeks.
3. The query is submitted to the database and the results are returned to the web server.
4. The .ASP application formats the results into an HTML page, which is then returned to the web browser.
5. The web browser presents the web page to the user.

This design is perfectly serviceable. However, malformed user requests can alter the course of the queries submitted to the database if the application passes them through without proper validation.

Specifically, a properly constructed user request can cause the .ASP application to submit SQL to the database that will actually insert data, rather than retrieve it. Diagram 1a illustrates this course of action.

Here's how a hacker would execute an assault that takes advantage of this SQL vulnerability:

1. An attacker observes the website's functionality and constructs



a request designed to tamper with the SQL composed by the .ASP application.

2. The application submits the altered SQL to the database, inserting malicious content in such a way that it will be retrieved in the course of processing normal user requests.

3. A user makes a standard request from the website.

4. The .ASP application issues normal SQL to the database, of which the contents have already been altered; the malicious content — generally some HTML tags containing references to files hosted elsewhere — is returned.

5. The .ASP application formats the results of the query into an HTML page that contains the malicious tags and presents that page to the user's web browser.

6. In the course of rendering the HTML returned by the application, the user's web browser processes the hostile HTML tags, and requests materials — usually some malicious JavaScript — from a server hosted elsewhere.

7. The JavaScript is downloaded to the user's web browser and executed, essentially recruiting the user's system into participation in some unwanted enterprise: click fraud, membership in a botnet, etc.

This attack methodology has become commonplace in recent months. Frequently, the attacker resides overseas and targets a lightweight eCommerce site. The attacker probably knows nothing about the eCommerce business.

The real goal is to take advantage of the fact that vulnerable users visit the website. Again, there's nothing new about the means of attack — only the combined use of several methods into a single technique.

## A NEW SECURITY FOCUS — DATA

The fact that hackers keep coming up with new uses for old methods of attack calls attention to the fact that all of our systems will never be perfectly secure. Over the past several years, there has also been an erosion of network perimeters as organizations strive to enable roving users and facilitate interoperation with partners.

In addition, various regulatory requirements have upped the stakes for failure. A security lapse might now imply fines, operations sanctions or other penalties if the victim organization fails to live up to its responsibilities.

So the situation looks grim: attacks are getting trickier; we'll always have at least some vulnerable systems; we can't rely wholly on traditional defenses; and the cost of failure is rising. In response, many organizations have changed course. Instead of

devoting their efforts to protecting their computers, the focus has shifted to protecting the critical data residing on them.

At first glance, this might seem like a superficial change. After all, if computers are vulnerable, we would naturally assume that the information on them is also at risk. To some extent, this assumption is true.

However, changes in application architecture, host-based data leakage prevention tools and encryption technologies allow organizations to protect at least some information — even under conditions where an attacker has compromised portions of the target computer.

Organizations have also begun to look for ways to shift burdensome security tasks (such as monitoring security events or managing patch levels) from their own IT staff onto service providers. The economics of this move have begun to make sense.

Hosting and managed service offerings have matured to a stable and commoditized state. This fact allows organizations to weigh the cost of a service provider against the benefits of freeing their own resources for other work.

Risk transference is a second motivator behind this trend. If, for example, an organization can move all handling of payment card transactions to a third-party service provider, it can greatly reduce the scope of the process — and therefore also the cost — required for payment card industry (PCI) compliance.

The service provider market is based on the premise of sharing large investments in bandwidth, storage, tools, operational processes and physical reliability between customers. The same model supports the business proposition for risk transference.

If every organization required to do so completed its own PCI compliance initiative, the total amount spent would far outstrip that of one organization building a massive PCI-compliant infrastructure and renting out its capabilities.

The subsequent chapters of this reference guide offer a tour of some of the most pressing topics in IT security, but the major themes remain the same. Attacks have become increasingly subtle, and compliance requirements are increasing the pressure for organizations to have adequate security.

Defenses are beginning to organize more around data protection than system protection. These trends give rise to new directions in familiar areas such as security for network endpoints and remote access. ♦

# RISK ASSESSMENT AND COMPLIANCE



## CHAPTER 2:

Determining Risk

The Process of Assessing Risk

Compliance Considerations

Security as a Process

The basic aim of IT security is to make sound decisions that protect organizations from harm. However, a great deal of jargon has built up around this seemingly simple topic. The best way to quantify risk is to simply view it as the likelihood of harm.

Most descriptions of risk include some combination of the probability of an undesirable event and the impact of that undesirable event. Common sense supports thinking of risk in these terms. When an activity is described as “high risk,” we often take both of these factors into account.

A relatively unlikely event might be worth guarding against because of the severity of the consequences. For example, very few commercial airliners make emergency landings in the water. Yet all passengers learn about using the seat cushion as a flotation device before every flight.

Likewise, small-scale losses only merit real protection when they occur with such frequency that they begin to have an operations impact. For instance, as the price of gas has steadily increased over the past few years, so has the deployment of cameras to monitor potential drive-away thieves at the pump.

The field of risk management ultimately boils down to making wise decisions on the basis of well-considered risk. We want to invest in protection where the expected losses outweigh the cost of defending against them.

Finding that area, however, is a subtle problem. You can endlessly

debate both the probability and the impact of incidents. So let’s define the parameters of the discussion.

## DETERMINING RISK

The two most conspicuous components of risk have been identified as frequency and impact of incidents. These two factors can be considered amplifiers: If either factor increases, the risk becomes greater.

Most security products focus on reducing the frequency of incidents. Specifically, when an organization has concerns about a particular kind of problem (such as propagation of viruses, password cracking, etc.), it will deploy a countermeasure to prevent it, such as antivirus or two-factor authentication.

This approach already contains an inherent problem. If an organization truly wants to address risk effectively, it doesn’t make sense to focus only on the possibility of bad things happening.

The same degree of benefit might be derived simply by engineering the organization in a manner that would minimize the effects of an incident. For example, many modern automobiles have “crumple zones” designed to absorb impact energy in a collision. These measures do nothing to prevent accidents, but they significantly reduce the risk to passengers.

The two risk factors, impact and probability, control the magnitude of risk. In information security, however, it’s also

important to consider the source of risk. To do so requires the consideration of vulnerabilities. A system, whether a computer, a network or an application, has a security vulnerability if:

1. It contains a flaw in its design, implementation, administration or use
2. The flaw could negatively impact the organization
3. The flaw can be triggered, regardless of whether it is known to exist

In the absence of any one of these three factors, no vulnerability exists.

However, experience suggests that there are vulnerabilities in the systems all around us. Obviously, when vulnerabilities are discovered in an organization's systems it takes steps to address them. What scares organizations the most is the zero-day attack — exploitation of a vulnerability the organization didn't even know it had.

The third point in the previous list raises an important question: Is having vulnerabilities the same as being at risk? Vulnerabilities can lie dormant. They don't really get attention until someone takes advantage of them. Thus, having a vulnerability does not specifically equal being at risk.

A threat is also needed. The term "threat" is used to refer to the agent that triggers the vulnerability. Threats come in many forms: natural disasters, renegade staffers, bots, etc.

Other factors can be weighed as well: the value of the assets to be protected, the cost and efficacy of the countermeasures deployed and so on. Clearly, the ultimate formula for calculating risk must incorporate many inputs, and its results can take many forms.

Everyone can agree that it makes sense to minimize risk, but at the same time, there will come a point where the cost of additional protection will outweigh the marginal reduction in risk. In order to find that point, some means of evaluating the situation are needed.

2a. The Bases and Consequences of Risk



**THE PROCESS OF ASSESSING RISK**

Risk assessment is the practice of measuring risk. In the field of IT security, this cannot be accomplished with quantitative precision because not enough data exists about the frequency and severity of incidents to make solid statistical predictions. As a result, IT risk assessments tend to emphasize qualitative analysis.

Various approaches to risk assessment can be adopted.

At one end of the spectrum, it's possible to do risk assessment mostly on paper. Such abstract approaches to risk assessment focus on the following issues:

1. Identifying the organization's assets and thereby determining what's at stake in the event of a security incident
2. Identifying likely areas of trouble, or "threat modeling," which involves brainstorming about potential sources of harm to the assets identified above
3. Attempting to prioritize the risks posed to the organization by ranking these potential troubles in terms of their likelihood and their potential impact

It's possible to complete the third step without either detailed actuarial data about security incidents or uninformed predictions of the organization's future security. Rather than attempt to produce an accurate spreadsheet of loss expectancies measured in dollars, it's sufficient to reach consensus about which risks pose a major threat to the organization and which are less important.

This strategy provides an advantage in that it offers a relatively quick and inexpensive path to valuable organizational knowledge. However, because it's conducted in a vacuum, it may not bear much relation to actual vulnerabilities or threats.

At the other end of the spectrum, it's possible to approach risk assessment from an applied technical perspective. A team of engineers with expertise in discovering and gauging the impact of vulnerabilities can effectively take a snapshot of the environment, and identify both assets that stand in jeopardy because of vulnerabilities and the types of threats that might affect them.

Essentially quantitative in nature, this tactic has the advantage of providing a more realistic measurement of the environment's resilience to the conditions of actual incidents. At the same time, a purely technical approach will often overlook important but intangible assets such as public relations and good will. For this reason, it's common to blend the two approaches.

Whether an organization wishes merely to establish a baseline from which to begin its security planning, determine whether its exposure to risk has increased or decreased since a prior assessment, or measure organizational compliance with a given security standard, it's a good idea to involve both operations and technical expertise.

## COMPLIANCE CONSIDERATIONS

Recently, compliance has become the focus of a great deal of security effort. Ultimately, this may not prove appropriate or effective. Compliance deals with the extent to which an organization conforms to a given standard.

Actual regulations form the basis for some compliance initiatives

— the Health Insurance Portability and Accountability Act (HIPAA) for healthcare-related entities, the Gramm-Leach-Bliley Act (GLBA) for banks, the Sarbanes-Oxley Act (SOX) for publicly-held entities and various state privacy laws.

At other times, industry drives the standards. The Payment Card Industry Data Security Standard (PCI DSS) is the most notable example of a nonregulatory compliance standard to which many organizations are subject.

It's important to bear in mind that while all these standards encourage good general security practices, there is a fundamental difference between compliance and security.

An organization concerned about security typically asks itself: "What do we have to do in order to be safe?" Another question determines an organization's behavior in the area of compliance: "What do we have to do in order to meet this set of requirements?"

Most organizations will find at least some differences between the answers to these two queries. More cynically, an organization focused solely on compliance might find itself instead asking: "How bad can we be and still comply?"

Despite the difference between compliance and security, overlap certainly exists. A compliant organization may or may not be appropriately secure, but a secure organization will generally be compliant with most mainstream standards.

Two other important points are worth noting. First, many organizations today are required to comply with multiple standards. A university, for example, can anticipate HIPAA, GLBA, the Family Education Rights and Privacy Act (FERPA) and PCI DSS issues at the very least.

When planning a compliance initiative, an organization can meet the goals of many standards often with a few simple directives or actions. It's wise to keep an eye out for opportunities to address multiple requirements with a single policy, procedure or technical control.

Finally, and most importantly, regulations themselves can be a source of risk. Many standards specify fines or other penalties for noncompliance. For this reason, an organization should definitely factor the concept of regulatory risk into its risk assessment activities.

At the same time, compliance has taken on such importance for many organizations that they easily forget that it differs from security. Security always deserves attention beyond just the minimum effort needed to comply with a standard.

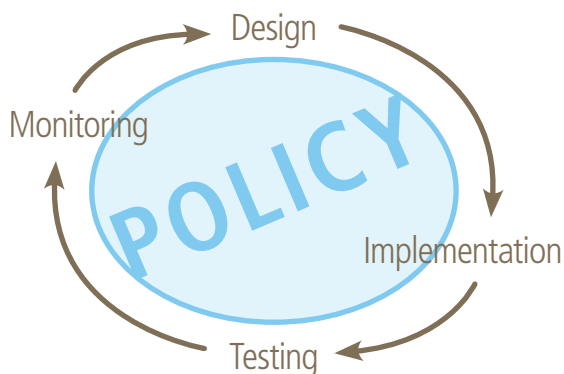
## SECURITY AS A PROCESS

The ongoing concern with compliance shows that security is not a static consideration that is quickly addressed and forgotten.

It's an evolving, never-ending process, both on an organization-wide scale and on the level of individual initiatives.

This notion may seem a bit overwhelming initially. Like any other organization activity though, security can be approached as a process, in a series of steps or phases. This process, or lifecycle, consists of four phases: design, implementation, testing and monitoring.

2b. The Security Lifecycle



A simple project management approach to security can make it very manageable. Please note that this section uses the word "system" in a very general sense: It can refer to an individual computer, a piece of software, a network, a business process, an entire organization or anything that might need to be secured.

### DESIGN

A system's security begins with a definition of its functional requirements and the development of a design able to meet them. Given that security is a fundamental property of a system, taking security into account at design time is essential. Adding security features onto a design as an afterthought is ineffective and costly.

Security needs to be a point of emphasis when system requirements are gathered. Requirements are what guide the project's design and implementation, and they're the yardstick used to measure whether what is developed and deployed adequately meet expectations. If security requirements are not documented, they will not be properly handled at the project's completion.

### IMPLEMENTATION

Even the best design may not turn out as planned when executed, so it's critical to pay attention to security concerns as a design is translated into a working system. In the case of a network rollout, this would include being thorough about changing default passwords on infrastructure gear before the network goes live.

For servers, this would mean ensuring that relevant patches are applied before a box is fielded. In the case of application development, security at implementation time would mean adherence to safe coding practices.

### TESTING

Once a system is ready to be deployed, it's crucial to verify that its security features function properly and don't expose the system to unnecessary risk. A security assessment can serve as an important sanity check or quality-assurance gateway before a new application or network site goes live.

Testing is an opportunity to answer the question: "Do our security measures accomplish what they're intended to do?" Security testing is often quite different from ordinary functional testing. As a result, outside expertise is frequently needed to make sure that the testing covers all the areas it should address and that it is sufficiently rigorous.

### MONITORING

It's important to remember that accounting is a key component of a system's security capabilities. Nearly everything in the IT environment has the capacity to keep some sort of log or send alert messages. Once a system is deployed it should be monitored so that it's possible to detect and respond to security incidents.

Operational responsibilities also include general system administration tasks: adding and deleting users, applying software updates and periodically reviewing security to make sure that changes in the threat environment have not exposed the system to new risks.

Keep in mind that over time, each of these areas will need to be revisited. Organizations change, new technologies are released, operations needs evolve and the threat environment is in continuous flux. From time to time it's necessary to tweak system design, implement the changes made, then test to make sure the changes are successful. This cycle must be ongoing if security is to be effective. ♦

# THREAT PREVENTION



CHAPTER 3:

Reducing Risk

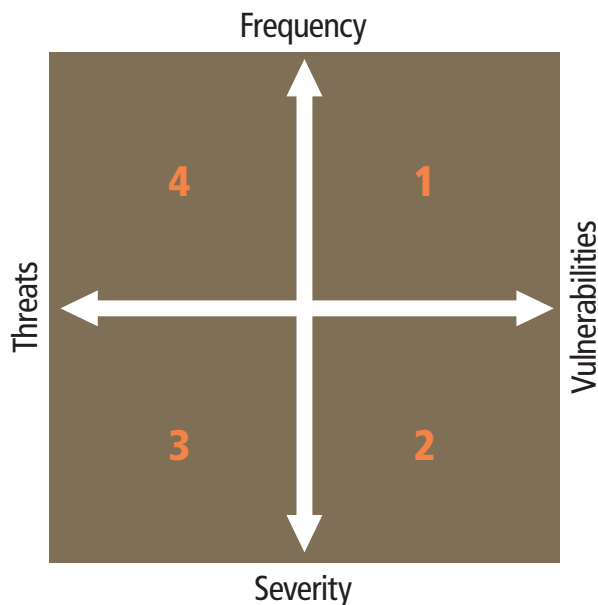
Multilayered Security Approaches

The previous chapter on risk assessment and compliance covered the difference between threats and vulnerabilities. However, a closer look at this difference is required before discussing threat prevention.

## REDUCING RISK

It's useful to classify security measures in terms of the ways that they reduce risk. Recall that risk can be defined as an annualized

### 3a. Quadrants of Risk



loss expectancy, which is the product of the frequency of security incidents and the severity of security incidents.

These two factors function as *amplifiers* of risk: If either of them increases, risk increases. Likewise, if we can decrease the probability of security incidents or limit their impact, risk decreases.

Along the same line of reasoning, we can think of threats and vulnerabilities as *sources* of risk: Security measures are applied to reduce risk by negating one or both of these factors.

Both of these pairings — threat/vulnerability and frequency/severity — can be viewed as axes on a coordinate plane, allowing us to use the quadrants of that plane (labeled 1, 2, 3 and 4) to better understand the nature of the security tools at our disposal.

Every security measure addresses two of these factors. Here are some examples fitting into each quadrant:

**Quadrant 1. Patch management:** A critical element of a strong security program, patch management ensures that systems are not running software with known vulnerabilities. It reduces the likelihood of system compromise by lowering the frequency of security incidents.

**Quadrant 2. Breaking password trust relationships:** Once an attacker gains access to a system, the next step is to see where else that access might lead. On the assumption that users tend to use the same password in multiple places, an attacker will typically crack the passwords of system users and try them out on other likely targets.

Breaking password trust relationships between systems — whether by enforcing specific password policies, implementing two-factor authentication or eliminating local password databases

— falls into quadrant two. These measures don't necessarily prevent system compromise, but they drastically reduce the impact of such an event.

**Quadrant 3. Back-end database restructuring:** Many web applications start out as public-facing front ends to databases designed for an organization's internal use. Examples include university alumni websites, healthcare patient scheduling websites and the like.

Such web applications become an attractive target for attack by identity thieves because the database contains some information, such as Social Security numbers, critical to some internal organizational operations but not strictly necessary for the public website's functionality.

Restructuring the website's back-end database to include only information needed for web functionality doesn't address whatever technical vulnerabilities the web application may have. It nevertheless reduces the impact of a security incident by making the website a far less interesting target for attackers.

**Quadrant 4. User education and awareness:** Ensuring that users remain well-informed doesn't address any technical vulnerabilities, but making them wary about existing threats reduces the probability that they will fall prey to fraudulent e-mails.

Each of these quadrants represents a different approach to the same goal: reduction of risk. The field of threat prevention

deals with quadrants 3 and 4 on the left half of diagram 3a. It realistically acknowledges that systems will always have vulnerabilities and focuses on keeping risk at a tolerable level by finding ways to address potential exploits.

## MULTILAYERED SECURITY APPROACHES

The products that organizations use will always be potentially vulnerable to attack. The security products organizations deploy to defend themselves are no exception. A wise security approach tends to include multiple layers. For example, it was once a commonplace principle of large network design to incorporate two brands of firewalls at the network border.

Often called a "firewall sandwich," this approach (see diagram 3b) presumed that sooner or later a hacker would discover a flaw in any given firewall product, and perhaps bypass the firewall by exploiting that flaw. In that event, the organization would have another brand of firewall as a second line of protection because the same flaw would likely not affect both.

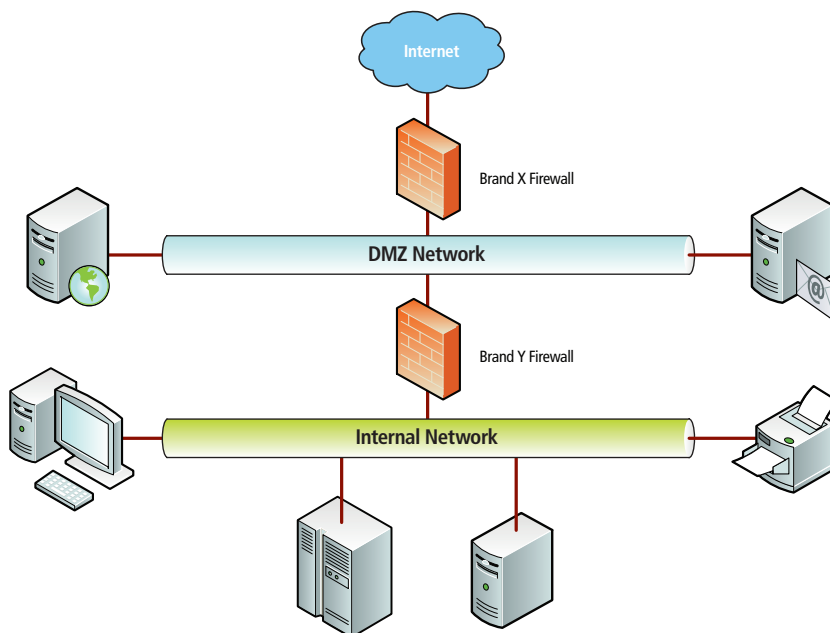
While firewall sandwich designs are still sensible for networks with specialized needs, they're out of favor for a variety of reasons, including the complexity of administration and the expense of extra hardware. In addition, many organizations now have multiple Internet uplinks and it's impractical to sandwich all of them.

The existence of multiple Internet connections poses a challenge for security management. Even in a hub-and-spoke network where remote sites only use the Internet for virtual private network (VPN) connectivity with the central site, each remote site necessarily has an Internet connection.

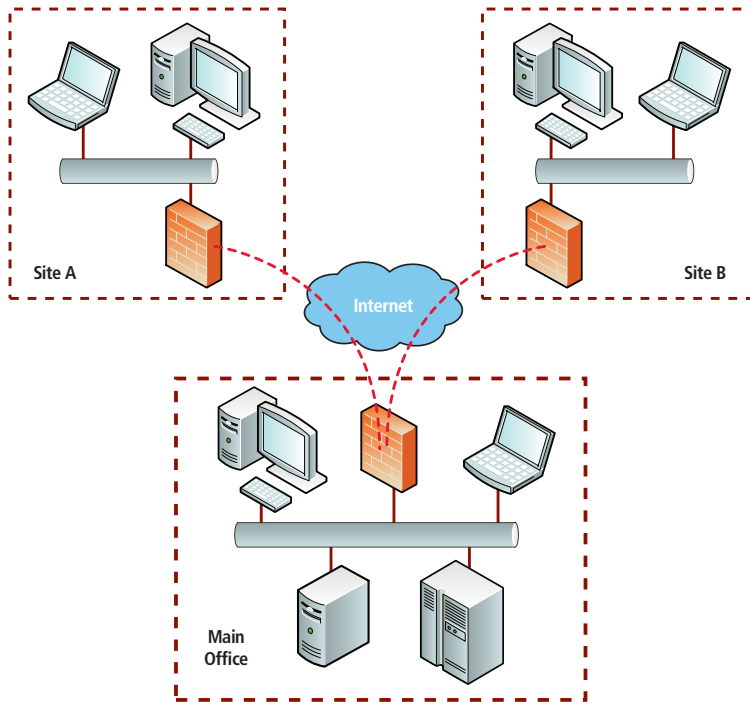
The more remote sites an organization has, the higher the probability that one will experience a security incident. Additionally, it's harder to keep track of security alert information from multiple sites. Finally, in terms of security, the remote sites' edge devices represent a single point of failure: The compromise of one may provide an attacker with an entry to the entire internal network.

Over the past few years, the manufacturers of network infrastructure gear have anticipated these problems. They increasingly

3b. A Firewall Sandwich Security Setup



### 3c. A Typical Hub-and-spoke Network



embed valuable security capabilities in the products they offer.

Diagram 3c represents a single central site with satellite offices interconnected by a hub-and-spoke VPN. Though the diagram shows only two remote sites, one can imagine any number.

The inquisitive mind of the security engineer looks at diagram 3c and begins to ask many questions:

- What happens if someone at Site A brings in an infected notebook? Does that affect the main office? What about Site B? Sending support staff to remote offices is expensive. If the diagram were expanded to include sites C through Z, a single infected remote system might precipitate tremendous cost.
- What happens if someone out on the Internet compromises the firewall at Site B? Can that person access systems network-wide? It's unreasonable to expect each site to have the resources to monitor firewall logs and respond to alerts.
- What about the main office housing the organization's critical servers? Can a database server, for example, be taken down if a worm that exploits Windows networking services gets inside the organization?

Threat prevention applies multiple layers of defense to address

these areas of concern. Specifically, based on the problems noted above, the following measures can reduce threats significantly:

1. Apply access control lists on the remote site firewalls to restrict outbound traffic to only necessary services — typically those provided by the server virtual local area network (VLAN) at the main office. Preventing remote sites from talking to one another will help to block an infection at one site from spreading throughout an organization.
2. Apply access control lists to the main site firewall, restricting inbound traffic from the remote sites to only the application protocols served up by the central servers. This measure will ensure that some protection still exists for critical assets even if one of the remote firewalls becomes compromised.
3. Implement a configuration management system to keep the many remote site firewalls, routers and switch configurations in sync. Remote sites tend to be duplicates of one another. Automating the process of making changes will reduce the probability of human error and ensure thoroughness and consistency.
4. Turn on the intrusion detection feature sets in the remote site firewalls. Nearly all modern

firewalls have at least modest capabilities in this area. However, especially in large multisite networks, these capabilities often remain unused because dealing with the stream of information they generate can prove a challenge. Still, employing the intrusion detection feature sets will at least ensure network sensitivity to changes in security conditions.

5. Implement a security event management system to collect and analyze log and alert information from infrastructure devices across the network. Doing so will give security administrators situational awareness, allowing them to react promptly and intelligently to trouble.

Note that each of these measures in some way complements the others. An organization that takes these steps will find itself prepared to deal with a broad variety of problems. Again, threat prevention's basic philosophy assumes that we can never have full control over vulnerabilities in our environment.

A prudent strategy, therefore, employs a combination of security techniques and supplements them with pertinent administrative tools in order to make the work manageable and effective. ♦



## Finding technology to meet your needs can be difficult. It's a good thing we enjoy a challenge.

When you have huge demands on technology, it's like music to our ears. CDW-G is there to take on your technology challenges. And to help us succeed, we have one of the largest selections of top-name products around, along with a personal account manager to guide you through all your options. If you have in-depth questions, we have technology specialists ready with answers. And when you need something a little more specific, we have a custom configuration center to get you new customized technology. So give CDW-G a call today, because we're up for the challenge.



The Right Technology. Right Away.®  
CDWG.com • 800.808.4239

# DATA LEAKAGE PREVENTION



CHAPTER 4:

.....  
Data Leak Opportunities

.....  
Removable and Portable Media  
.....

When organizations take stock of their digital assets, they quickly conclude that data is their most valuable resource. For a few organizations, the primary asset is actually the availability of some service or the capacity for certain throughput. But as a general rule, we buy servers, design applications and build networks with the goal of collecting and manipulating data.

And if information is our chief asset, we need to keep at least some of it confidential. As various members of an organization handle private data, it tends to accumulate in unexpected places, is handled unsafely, or is disclosed inadvertently. Data leakage prevention deals with these risks.

## DATA LEAK OPPORTUNITIES

Let's walk through a brief scenario. Staffer A works in the home office of state agency XYZ. Staffer B works in the agency's collections department downstate. One afternoon, staffer B calls staffer A with a question about the latest purchase order from Acme Corp., a vendor that has been having trouble with payments.

Because of the time difference, staffer A isn't at his desk, so staffer B leaves a voicemail. Unified messaging brings the voicemail to staffer A's smartphone, from which he listens to it. Staffer A then uses his phone's web browser to check the status of the order via the agency's extranet, and forwards from his inbox to staffer B an e-mail containing the relevant information.

This scenario represents a typical transaction in today's fast-paced work environment and serves as a perfect example of how well-integrated technologies enable projects to move forward,

even when people are out for an espresso. After looking more closely though, there are potential problems.

While diagram 4a (located on the following page) falls far short of identifying every possible juncture where data can leak, it does demonstrate that each step in the conversation involves some sensitive information that is subject to potential compromise.

The diagram delineates at least three zones in the transaction described above: the home office, the remote office and the coffee shop from which staffer A handles part of his job. It also clearly shows that portions of critical information migrated from zone to zone in the process of answering staffer B's question.

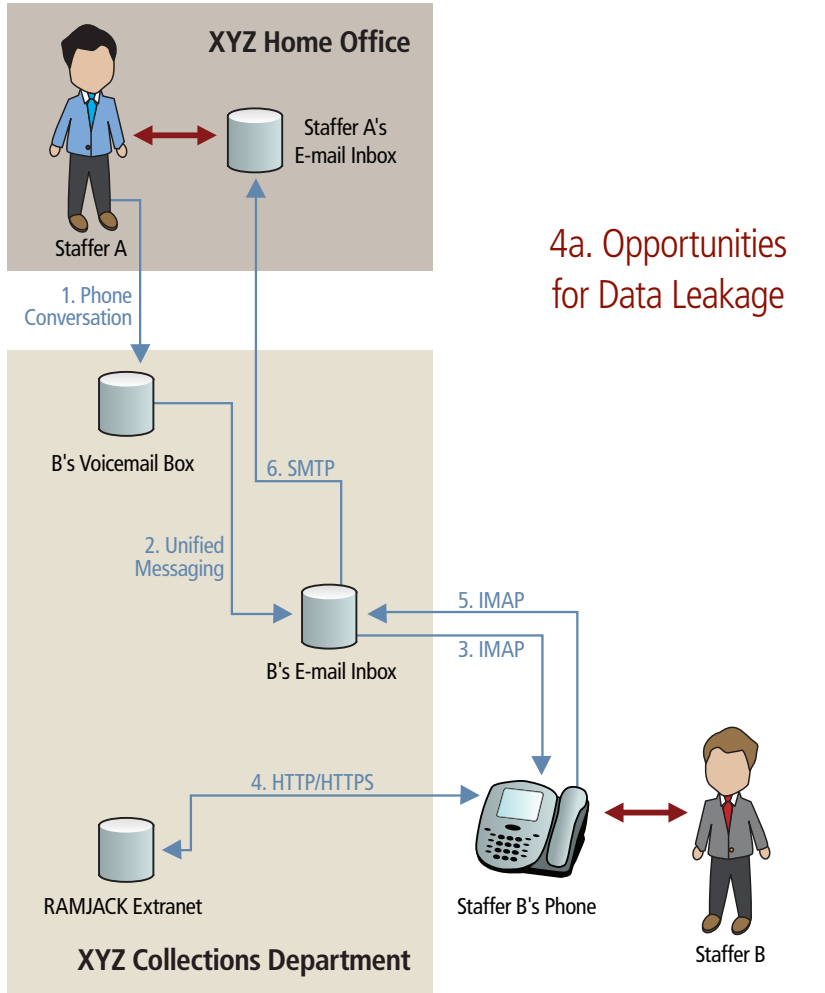
Every time a file or document is stored or moved, the potential exists for it to be intercepted or simply left out for later discovery. Data leakage prevention usually focuses on restricting the flow of private information across organizational boundaries. We want to set policies that govern how information is handled.

For example, a policy may prohibit sending e-mails that contain Social Security numbers or financial information over instant messaging systems that are not logged. Ideally, organizations could enforce such policies by technical means, but often this strategy is not completely feasible.

## LEAKAGE VECTORS

Sadly, most data leakage is self-inflicted. Information simply proliferates too quickly and in too many ways for users to keep track of it. The most common data leakage pathways all have two fundamental things in common:

- Technology that makes it very easy to exchange information



### 4a. Opportunities for Data Leakage

misplace. Unfortunately the more small physical objects we need to keep track of, the easier it is to misplace or lose them.

It's also hard to know what happens to media once a user is finished with them. If we use a USB drive to bring a file with us to another site, what happens to the file once it has been copied? Most often, it still resides on the USB drive.

If the USB drive is lost, the contents go with it. Likewise with CDs, DVDs and floppies. When copying the contents onto hard drives, we rarely take the additional step of destroying the disks or wiping them clean once they're no longer needed.

These various physical objects get handed around, left in unprotected places and eventually lost. When this happens, the private data clinging to them like lint becomes a potentially serious liability. Many organizations have deployed smartphones with "remote-kill" functionality or full disk encryption on their notebooks to counter this risk.

These measures certainly help, but they have limitations. If a phone can't receive the instructions to wipe its memory, it will never do so. With this in mind, law enforcement officers have begun placing phones that they confiscate in bags lined with wire mesh to ensure the recoverability of whatever information those devices contain.

Likewise, whole disk encryption protects only the copy of a device's data written to the hard drive. If a device is captured while powered on, a great deal of sensitive information may reside in memory in decrypted form.

This section does not aim to cause panic about each and every lost CD or thumb drive. Rather, it sheds a little light on the many ways that sensitive information comes and goes from our organizations.

### E-MAIL

E-mail is an even worse problem for data leakage than portable media. When replies to messages get chained together, the person who forwards an e-mail thread seldom checks to see whether the whole thread is suitable for the recipient. Files of all sorts get

- Security limitations on the technology that make it unsafe for certain types of information transmission

Risk results when users handle sensitive data in unsafe ways — because they don't know better, because they think it will be expedient or because operations processes force them to do so.

### REMOVABLE AND PORTABLE MEDIA

How many times have we carried our notebooks to another site, downloaded contact information to a phone, copied a file to a USB drive or burned a CD of data for a colleague? Every time we do so we put information into a form in which it can be lost or stolen.

These storage media tend to be portable and therefore easy to

attached to e-mail, and these can contain sensitive information as well.

In fact, the sender of a file may not even be aware of its full content. For instance, spreadsheets can contain hidden rows. Word-processing documents may contain historical data about changes and edits. Presentations can contain embedded objects and metadata that give clues about confidential data.

In addition, it's just too easy to hit "reply all" without checking the full list of recipients. Doing so can result in the inadvertent sharing of comments beyond the audience one had in mind. In some cases, the list of recipients itself might even be confidential.

Finally, many users remain unaware of the types of information they should avoid exchanging via e-mail. What is considered acceptable e-mail usage within an organization might not be safe for transmission across the Internet.

The most important thing to remember is that once e-mail is sent, it can't reliably be recovered or erased. It can linger indefinitely in inboxes over which we have no control, and others can forward it onto recipients we have not authorized.

While e-mail serves as a critical communication tool for almost all organizations, it also makes the leakage of private information possible in new ways and on a new scale.

## OTHER TRANSMISSIONS AND SYNTHESIS

Instant messaging has become an increasingly popular means of professional communication. It too can include more than just text, and unfortunately, even plain text can prove an issue.

Many organizations have deployed technologies that inspect outbound e-mail for suspicious content, which may range from malware and spam to credit card numbers, Social Security numbers and keywords related to confidential internal research or projects. Instant messaging can bypass these controls and thereby provide another avenue for exporting the organization's internal secrets.

Instant messaging isn't the only communication pathway besides e-mail, of course. Blogs and social networks are also prominent areas of interest. By now, most organizations have implemented some policy or other for staffers who participate actively in these sorts of online activities.

Even if users carefully refrain from posting any private data, an attentive observer might draw inferences that amount to a disclosure of sensitive data.

Web logs, for example, contain the IP addresses of visitors. Even if a discussion in an online forum never mentions the name of a participant's organization, the source IP address may provide a dead give-away.

Whenever an organization has serious confidentiality obligations, as many governmental organizations do, it's important to keep in mind that photos or comments posted to the Internet will be archived.

The amount of information cataloged by search engines, in other words, will only increase over time. As a result, a comment that contains no specific harmful or incriminating information today might have a completely different meaning when placed in the context of a long series of posts from the same commenter over time.

This risk, sometimes called "information synthesis," is not a new one by any means. It's receiving new attention because of the volume of online content now catalogued and searchable.

Researchers have already demonstrated some techniques for "de-anonymizing" contributions to public forums such as movie review databases and online shopping wish-lists. It's likely that the same searching and data-mining techniques could be used to infer aspects of an organization's private information from large volumes of seemingly innocent communications by an organization's members. ♦



# STRESSES



## ON THE GATEWAY

Firewall protection isn't what it used to be. Neither are Internet-based threats and intrusion attempts. Organizations seeking improved security face pressures from several directions. Motivated by financial gain, hackers have grown a lot more sophisticated. They now press against all entry points. They rapidly exploit published and unknown operating system vulnerabilities, launch multiphased attacks, hijack PCs you might believe are secure and lure users into betraying passwords through insidious strategies such as phishing. Even if they don't succeed, these attacks can devour your organization's valuable resources and slow your performance. And when they've done their damage, hackers vanish into the shadows, often impossible to track.

Regardless of where the threat originates, the harm comes as it moves through your gateway. A strong gateway means attackers can't get in and proprietary information can't get out.

Protecting your gateway is now a multilayered task. The number of functions your security systems must perform can be mind-boggling.

You have to consider network firewall capabilities, which at a minimum include:

- Stateful packet inspection (SPI) to identify and block network headers claiming to be solicited responses
- Network address translation (NAT) to hide the IP addresses of your internal systems so they can't be targeted for bot infestation
- Continuous monitoring and logging to help you stay on top of your security needs

Given the damage spam, malware, internal leaks and inappropriate downloads can cause to your systems, look carefully at your content filtering capabilities. These include:

- Bot, virus, spyware, spam and phishing protection (anti-X protection) that incorporates continuous updates for the latest virus signatures and system vulnerabilities
- URL filtering and drive-by download protection
- Outbound as well as inbound content scanning
- Blocking against unwanted applications such as IM and games

Access control and the security and privacy of authorized network connections are also important, so consider:

- Strong authentication protocols for authorized users
- Secure virtual private network (VPN) technology

And finally, because you must protect end-user devices such as notebooks and Blackberrys, you need endpoint security software, including individual firewalls and content filtering. If you have multiple locations or branch offices to protect, you'll need integrated defenses at those sites as well.

### Getting help

If you decide that you can best evaluate your security exposure and develop an appropriate strategy with outside help, you can find a strong ally in CDW•G. We provide free consultation with our experts in NAC, plus the deepest selection of hardware and software available, so your every technology need is met.

# SECURITY BREACHES SPARK DEMAND



## FOR BETTER DATA PROTECTION

High-profile security breaches and cases of identity theft that compromised the privacy of millions have led to numerous federal and state regulations aimed at protecting sensitive data and imposing transparency on accounting and data security practices. Most experts agree that more regulations are on the way.

There is also a voluntary international standard for security compliance; the International Standards Organization's ISO 17799, a comprehensive set of controls comprising best practices in information security. ISO 17799 has two parts; a code of practice and a specification for an information security system. In principle, the regulations all require affected organizations to implement policies and procedures for storing, backing up, securing and providing audit trails for confidential data.

Although some organizations still take a wait-and-see position regarding security compliance, many will be compelled to invest in security systems and processes that comply with regulations and deliver the level of security you've probably been campaigning for all along.

### **Building and sustaining a compliance program**

To start, you should have a well-defined security management policy in place. The plan should be as specific as possible, addressing such questions as user access levels, remote-access security protocols, security updates and application control. Fortunately, guidelines outlined in the regulations themselves usually provide a blueprint you can incorporate into your existing policy.

### **Here are the basic steps to build a compliance program:**

- Learn which regulations, if any, apply to your organization.
- Conduct an audit to identify deficiencies in your current security policy.
- Implement controls to plug gaps identified by the audit.
- Revise your organization's IT security policy to incorporate compliance.
- Conduct frequent audits as dictated by the regulations.

### **Compliance can be complex. Let CDW•G help.**

To implement a fully compliant data and IT infrastructure, you'll have to have adequate storage capacity, security measures and access control policies in place. You also have to think about data archiving. It can be a lot to consider, but CDW•G can help. Our security technology specialists can assess your current strategy and assist you in developing the right compliance approach for your organization. Call your CDW•G account manager to get started. If you don't have an account manager yet, call 800.808.4239.

# GUARD AGAINST



## IDENTITY THEFT



Identity theft is on the rise, and it's not just big banks and credit card companies that need to be concerned about protecting customer and employee information. Organizations of every size collect and store data that is attractive to thieves: social security numbers, account and transaction records, and other personal information about employees and clients.

By establishing a few fairly simple data ground rules, organizations can prevent the theft of identifiable personal information — or at least decrease the chances of such attacks occurring. A best-practice approach to avoiding identity theft requires an organization to make smart use of information technology, establish a data protection policy and take physical security into account.

### Layers Of Security

Preventing identity theft essentially requires the use of multiple layered security and systems policies. The federal government's National Institute of Standards and Technology suggests the best approach to protecting personal data from tampering is to make access difficult and to use knowledge-based authentication to grant users access on a need-to-know basis.

According to a recent NIST bulletin, an authentication system that requires users to provide something for all three of the following categories offers the highest security:

- Something that the user knows, such as a password;
- Something that the user has, such as an ID badge or token;
- Something that is unique to the user, such as a fingerprint or face.

Authentication using biometric factors can help to reduce identity theft and the need to remember passwords or to carry documents, which can be counterfeited. When biometric factors are used with one or two other factors, it is possible to achieve new and highly secure identity applications.

### Under Lock and Key

Protecting personal data is more than just an IT and policy issue. Organizations also need to think about physical protections for their hardware, particularly portable systems and storage devices that tap into or host files containing personal information.

Contact your CDW•G account manager today for more information on how to safeguard your data and protect your staff from identity theft.

# STAYING AHEAD



## OF SECURITY THREATS

It's almost impossible to make it through a day without encountering news about hackers, computer viruses and increasingly ingenious methods of identity theft. Today, government agencies face a world fraught with risks and growing concerns about security. It is estimated that viruses cost organizations approximately \$55 billion in damages in 2003. Overall, the Computer Security Institute (CSI) reports that the average cost of a security breach is now \$204,000. Government is particularly at risk because many agencies operate data warehouses and databases containing large volumes of information.

Maintaining a high level of security is no simple proposition. Over the last few years, attacks have grown in sophistication and malware has become far more dangerous, unpredictable and widespread. Not only have hackers stepped up their assaults on government agencies, they've become smarter and more creative, using buffer overruns, spoofing, stolen IDs, SQL Injection techniques and an array of other approaches.

Because so many pieces to the security puzzle exist, many organizations find themselves allocating growing money and resources to a variety of security flash points, including infrastructure, virtual private networking (VPN), intrusion detection, monitoring tools and actual code. While these security solutions are sometimes expensive, organizations increasingly view them as a basic cost. In fact, many understand that they're no longer an option but a necessity.

Some organizations are turning to a sophisticated hardware approach to protect networked and non-networked endpoints by providing users with access to a fully secured virtual private network. A Secure Sockets Layer (SSL) VPN enables universal access to protect mobile and office endpoints from worms, viruses, spyware, keyloggers, Trojan horses or hacking.

Authentication is also a key to preventing security breaches. Establishing strong logon passwords and short time-out periods to restrict access to sensitive data is an important start. In addition, a growing number of agencies are using IP address restrictions to limit exposure to inappropriate or restricted materials.

Finally, IT must oversee increasingly complex patching requirements. It's essential to apply current security patches and updates on a regular basis — and in a consistent manner — in order to address security flaws, bugs and usability problems. Larger patches, also known as "service packs," address a number of issues simultaneously and play a key role in reducing the vulnerabilities of a system.

Although each organization must discover its unique route to security and build a framework that suits its needs, best practice organizations place an emphasis on standards, conduct a thorough and ongoing analysis of systems, invest in tools and processes that provide maximum protection, and provide employees with the training and skills to use systems effectively and safely.

**Contact your CDW•G account manager today to learn more about how we can help you stay ahead of security threats.**

You can't predict  
every server mishap.  
Good thing CDW•G has a plan.



When the unexpected happens, you need to be ready. CDW•G can help you devise a plan and put it into action. We have a team of experts who work with you to identify your unique needs and determine which warranty upgrades and extensions ensure you're protected. Whether you need onsite repair or a disaster preparation solution, we can help make sure you're covered.

Plan for the unexpected. Call 800.808.4239  
or visit [CDWG.com](http://CDWG.com)

The Right Technology. Right Away.®



# SECURE REMOTE ACCESS



## CHAPTER 5:

Varieties of Remote Access

Threats to Remote Access

A few IT professionals still remember the days when it was essential to be in the office in order to perform most work functions. Today, we're instead expected to be able to keep up with some tasks while on the road or at home, and notebooks have become standard-issue in many organizational environments.

This means that people will be accessing organizations' networks remotely. For this reason, remote access must to be secure. There are a number of key issues to ensuring this security.

Perhaps the most important is that many organizations don't have a good handle on all the types of remote access they need to be concerned about. Another important issue, traffic interception, is covered in Chapter 6 because the problem of eavesdropping isn't unique to remote access.

## VARIETIES OF REMOTE ACCESS

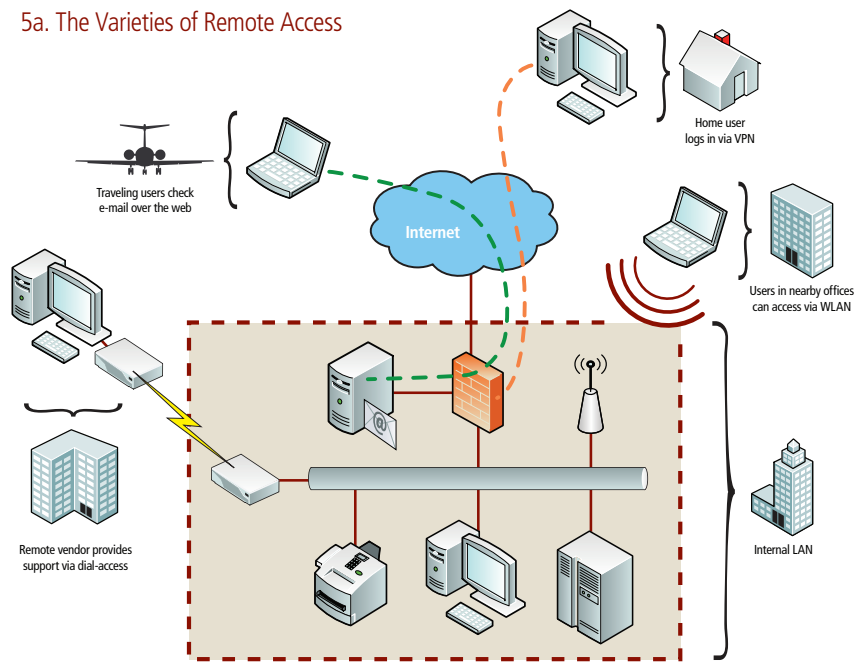
Strictly speaking, remote access encompasses any access to private network resources from beyond the organization's physical perimeter. This broad characterization of remote access includes some modes that most organizations aren't taking into consideration in their security planning.

Figure 5a illustrates a variety of possibilities.

Remote access includes the following scenarios:

- Users may log or dial in via virtual private network (VPN) to do work on the organization's internal systems. When people speak of remote access, they often have this scenario in mind.

5a. The Varieties of Remote Access



- Vendors and other partners may have access to support or administer systems on the organization's network. In certain organizations, this kind of remote access is frequently accomplished by dial-in access. In others, VPN and leased-line connectivity are more common. Regardless of the topology used, the fact remains that persons or systems outside the organization's perimeter are accessing data and systems within it.
- Traveling users might make use of lightweight remote access solutions such as web e-mail or various support tools. Often we fail to think of these systems as being true remote access because we intentionally make them accessible through our firewalls. At the same time, these systems often pull information

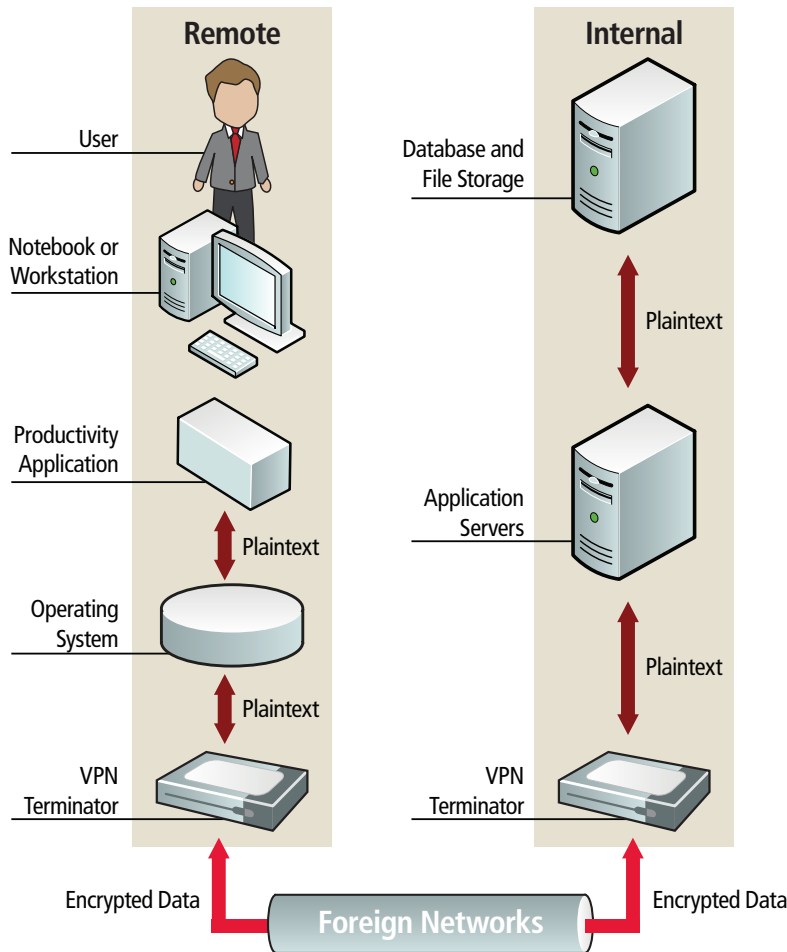
from within our networks, granting accessibility to data that we consider internal.

- In some cases, remote access might be provided unintentionally. Wireless networking signals, whether from access points or from endpoints, seep out of buildings. Whether on purpose or accidentally, outsiders may receive those signals and connect to systems on internal networks.

Though this list touches on the major modes of remote access, each of these might have many variations: VPN, for example, can encompass Internet protocol security (IPsec), Secure Sockets Layer (SSL), point-to-point tunneling protocol (PPTP), secure shell (SSH) and other protocols.

Of course, the specific technologies in play at a given organization each have different strengths and weaknesses, but their purposes remain similar. Our goal is to facilitate access to internal resources without exposing them to risk.

### 5b. VPN Remote Access



### THREATS TO REMOTE ACCESS

Having identified the basic types of remote access; it's time to start thinking about what might go wrong. Envision a typical remote access scenario — in this case, a VPN — as depicted in figure 5b.

The diagram calls attention to the various participants in a remote access event: the remote side, the internal side and whatever networks carry information between the two. Both sides have some device or software that manages the remote connection.

Typically, this task is handled by software at the remote user's end and an appliance on the organization's end, but variations abound. The illustration highlights the fact that threats to remote connectivity can target the establishment of the connection, information in transit, the endpoints themselves or the ability of either end to transmit or receive.

### DENIAL OF SERVICE

Denial of service refers to an attempt to make remote connectivity usage impossible. Many ways exist to accomplish this goal:

- **Resource consumption:** An attacker can overwhelm the systems that provide connectivity either with traffic floods that crowd out legitimate transactions or with requests for services from the endpoints (for example, to establish a new connection). Resource consumption aims to exhaust processing resources.
- **Crashing:** An attacker can send specially crafted network traffic designed to disrupt the operations of either endpoint, generally by crashing the system or rendering some portion of it inoperative.
- **Lockout:** With a list of users, an attacker can supply intentionally incorrect passwords for each account until all users are locked out. Though the system itself remains unaffected by this tactic, it is still rendered unusable.

As a rule, denial-of-service attacks are directed at central resources such as the organization's VPN concentrator, for example, rather than the many remote clients. The unavailability of remote access functionality can have a serious impact on an organization's security, however, if the organization relies on remote access for any critical tasks.

## TRAFFIC ANALYSIS

Even though a remote access solution might protect the contents of communication from eavesdropping, traffic interception can still prove a problem. An eavesdropper can learn a great deal from encrypted traffic, despite the fact that the actual contents of packets might not be accessible.

First and foremost, the eavesdropper can see what the endpoints of the conversation are. For some organizations, this is potentially very dangerous. Some real life examples suggest how endpoint vulnerabilities can put organizations at risk:

- Undercover law enforcement agents communicating about cases can be observed connecting back to Department of Justice VPN servers.
- Missionary groups abroad in countries where religious freedom is not tolerated may run tremendous risks in communicating with the organizations that sent them.
- Investors working for a mergers-and-acquisitions organization need to maintain secrecy about the potential clients and prospects with whom they communicate.

In each of these examples, the contents of any given interaction might be innocuous, but the mere fact that communication is taking place might expose a person or project to risk. Even if the existence of encrypted traffic doesn't pose a problem in itself, an observer can often make powerful inferences about patterns in operations by looking for deviations from normal patterns.

Someone sniffing a private wireless network for encrypted traffic might not be able to read the contents of communications, but they might be able to deduce where and when users work, bank and shop. Someone sniffing traffic inbound to an organization's VPN concentrator might be able to deduce the locations of remote users.

For many organizations, such possibilities may not represent a major source of risk. It's important to remember though, that traffic that is encrypted isn't completely concealed.

## ATTACKS ON AUTHENTICATION CREDENTIALS

The possibility that unauthorized users might access sensitive resources remotely poses a second serious risk. Specifically, by supplying the right credentials, an attacker could join the VPN, or establish a dial-up connection, or get onto the wireless network, and proceed further from there.

An organization can handle authentication for remote access by a variety of means. Standard user name/password login, two-factor tokens and digital certificates are the most common, but others exist.

Under each of these approaches, users prove their identity by providing some combination of secrets (or information based on secrets) that only a legitimate user should have. Several possible vectors of attack exist:

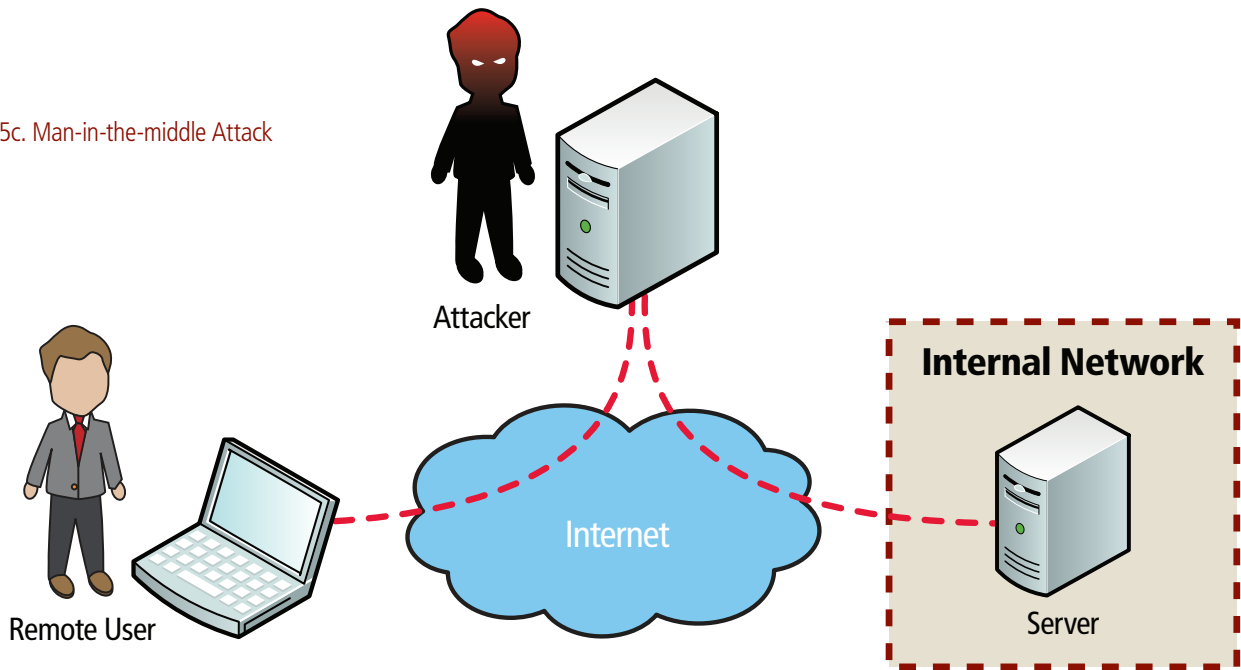
- **Brute force:** With a legitimate user name, an attacker can systematically begin supplying guesses as to the secret information, with the goal of eventually trying all possible alternatives.

Countering a brute-force attack generally involves either intruder lockout features (for example, an account is locked after some threshold number of incorrect login attempts) or by making the secrets to be supplied so complex that guessing them becomes highly improbable. Authentication schemes based on digital certificates tend to have this property.

- **Shallow dictionary:** If an attacker can access or generate a list of user names, it's easy to supply a list of simple guesses. A typical attack might involve supplying the following guesses for each account: blank password, password is "password" and password is the same as the user's name. Assuming that the intruder lockout threshold is five guesses, this attack would probably go by unnoticed.

The attacker can then wait a day (until the lockout counter has reset) and try a new set of guesses: the current month, the name of the organization, the name of a local sports team. This type of attack doesn't target any particular account. Rather, it relies on the probability that in a large enough user population, at least one account will have a trivially guessable password.

5c. Man-in-the-middle Attack



Even with a secure underlying means of transporting data, a remote access solution can easily be compromised if authentication mechanisms are weak.

**MAN IN THE MIDDLE**

So far we've looked at threats to remote access system availability and attempts to impersonate users, but we must also consider the threat of impersonating the remote access system itself. In a man-in-the-middle attack on a remote access system, the adversary convinces the remote user that an imposter system is, in fact, the legitimate source of remote-access connectivity.

When the user connects, the attacker simply takes the same credentials and passes them along to the actual remote access onramp, impersonating the user's endpoint system, as in figure 5c.

This is a particularly insidious attack: the interceptor can inspect and alter all traffic on its way between the user and the organization's internal network. Neither side has an easy way of detecting the problem.

Man-in-the-middle attacks generally demand both technical sophistication and access to important network resources (such as DNS servers or routing infrastructure).

Man-in-the-middle attacks are also less feasible against systems with strong mutual authentication protocols.

For example, if both ends of the connection prove their identities by means of digital signatures, a man-in-the-middle attack is unlikely to succeed. On the other hand, the bar moves significantly lower if only the user side has to prove its identity. ♦



# ENDPOINT SECURITY



## CHAPTER 6

### Varieties of Endpoints

### Threats to Endpoints

The real value of technology lies in the degree to which it enables coworkers to work with information or engage in transactions that would otherwise remain inaccessible. Despite the fact that the servers that store and process information may be locked in the data center, the vast majority of our meaningful interactions with computers take place on network endpoints: workstations, notebooks, PDAs and the like.

As users, we type in our passwords, access public networks, view sensitive reports, engage in private communications and generally conduct our business on our own network endpoints. As IT professionals, we recognize that the involvement of network endpoints in the storage and processing of sensitive information means they need protection.

## VARIETIES OF ENDPOINTS

Before diving into what it takes to secure a network endpoint, it's important to define what an endpoint is. Figure 6a (on the following page) depicts a fairly typical network ecosystem and calls attention to the variety of systems that might be considered endpoints.

The list of endpoint varieties is longer than most people expect:

- Workstations, terminals and notebooks are the most obvious endpoints and represent the main means by which users interact with network resources. As a general rule, end-user systems on an organization's network belong to the organization and have standard operating system builds, password policies, antivirus protection and so on.
- Workstations and notebooks can also be used remotely and might not belong to the organization. For instance, a staffer might check e-mail from a hotel or an airport kiosk; an IT worker

might log in from a home computer; or a vendor might connect remotely to support a particular product or system.

- Though often overlooked, network-connected printers and fax machines function as endpoints as well. Such devices represent a major path for sensitive information to enter and exit networks.
- Smartphones, PDAs, music players and other multifunction devices also represent endpoints. Less full-featured than workstations, they nevertheless often have large storage capacities and can be used to handle confidential files or e-mail.

Each of these families of devices have different security limitations. Consequently, varying constraints exist around what network and system administrators can do with them. With this in mind, we can dive into the threats facing network endpoints.

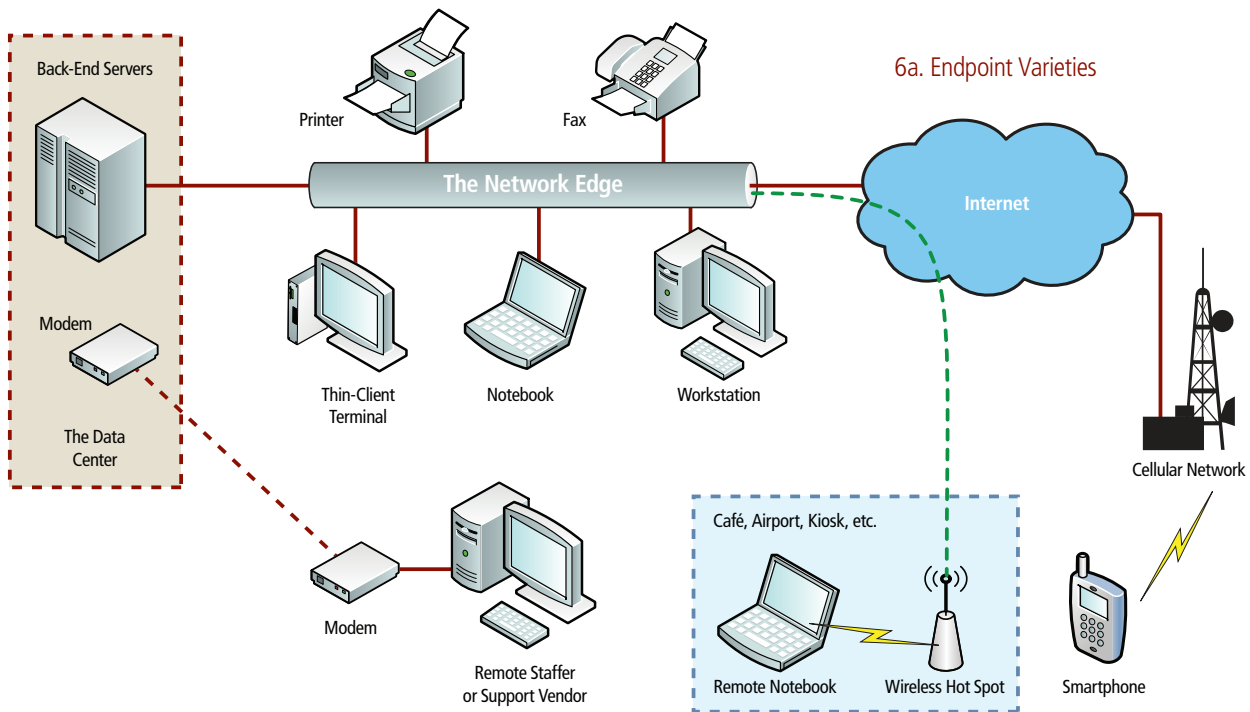
## THREATS TO ENDPOINTS

Because we tend to focus attention on centralized services or massive repositories of critical data, network endpoints are often neglected security-wise — but they need protection. Attacks on network endpoints can put an organization's private information at risk just as surely as attacks on the central resources themselves.

## UNAUTHORIZED ACQUISITION

The loss of physical equipment, while unsettling, might prove insubstantial compared with the loss of the information that it houses. Nearly all endpoint devices store some valuable information, whether proprietary data, internal communications or cached passwords.

Most printers and multifunction copiers contain hard drives where



images of recently processed documents might persist, perhaps along with network credentials. The potential exists for someone in physical possession of one of these devices to extract sensitive organizational data from them.

Many organizations consider and address the threat of equipment theft, but they should also pay attention to the ways in which they approach systems repaired and expired asset disposal. Each of these junctures represents a potential opportunity for an outsider to gain access to stored data.

The most common method of protecting against unauthorized acquisition of physical devices is to encrypt the data on them. Properly managed cryptosystems can protect private information from unauthorized access in the event that the physical device or media falls into the hands of someone without authorization to access it.

Some strategies involve encrypting all data on a device (such as whole disk encryption), while others selectively encrypt only sensitive materials. The difficulty with the latter approach is that it's not always easy to ensure that all sensitive information receives protection.

### SUBVERSION

Encryption might serve as a suitable protection for information stored on powered-off systems, but information is generally

unencrypted when in use. As a result, if an attacker gains control of a system while it is up and running, a great deal of information that would otherwise be encrypted might be accessible.

Spyware, for example, generally has access to whatever materials the logged-in user can see; bots running as background services might be able to access anything that the operating system can. If a hacker finds a means to execute code on a network endpoint, it becomes possible to read files, log keystrokes and capture screenshots of any user's activity.

Also, the compromised system might contain stored passwords that would give the hacker access to other systems: help-desk accounts, cached domain login credentials, service account passwords, passwords to websites, VPN authentication materials and so on.

These possibilities make it critical to protect network endpoints against attack. Host-based intrusion prevention, antivirus/malware products, local firewalls, diligent system administration and user awareness training are all key components in a program to protect network endpoints.

As in any security situation, one can never presume that any effort will prove 100 percent successful. Instead, one should approach the compromise of network endpoints as a realistic possibility and plan for it with strategies such as security information management, network segmentation and network admission control.

## EAVESDROPPING

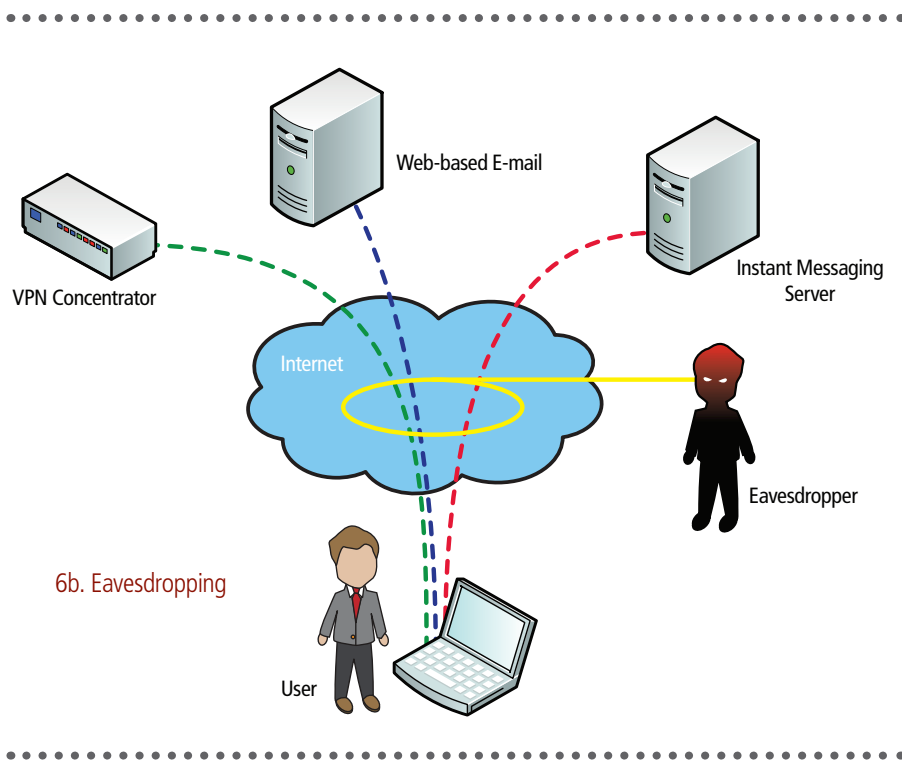
Network endpoints rely on other network resources in order to be productive. This characteristic means, as a rule, that sensitive information (the files and data that the endpoint handles, as well as authentication credentials) necessarily traverses the network.

Consequently, network traffic always remains vulnerable to some degree of eavesdropping. Passively listening to network traffic can, in fact, reveal a great deal of private data, system administration practices and even passwords for services.

Remote network endpoints have always dealt with the problem of eavesdropping: VPNs and cryptographically protected application protocols such as secure shell (SSH) or hypertext transfer protocol over Secure Sockets Layer (HTTPS) make it possible to conduct private transactions on public networks without major information leakage.

However, these measures also create a false sense of security because users often don't realize all the avenues for disclosure of their passwords. In figure 6b, a user fires up a notebook, connects to the Internet, checks web-based e-mail, hops on the organization's VPN and signs into an instant messaging service. An eavesdropper captures all of this traffic.

The VPN logon is secure, but the other two may not be. Moreover, the instant messaging logon might happen automatically, without the user even thinking about it.



6b. Eavesdropping

If the user employs the same password for more than one of these systems, the eavesdropper might well have the ability to read the user's e-mail. The potential may also exist for the eavesdropper to access resources over the VPN since, in addition to the instant messaging credentials, they have likely seen the addresses of the VPN concentrator and the web mail server.

Despite how well-known this attack technique is, people with security expertise still fall prey to it — even in obviously hostile network environments. The “Wall of Sheep” experiment at the annual DEFCON hacker convention amply demonstrates that potentially important credentials leak out all around us (for more info: [blogs.zdnet.com/Ou/?p=660](http://blogs.zdnet.com/Ou/?p=660)).

Sensitive data may be at risk in foreign environments where we already know enough to be wary, but the problem is present in subtle forms within our own networks as well.

Nearly every organization has some pool of highly confidential data: Social Security numbers, health records, student grades/transcripts, tax and property records, and so on. Access to these materials is often carefully restricted so that only a small group of people can view a database or folder of files.

The organization feels safe because these users only print to a printer in their area, with physical access to that area well controlled. Yet print jobs are rarely protected as they traverse the network on the way to the printer.

Anyone physically in a position to capture this traffic — and software to capture network packets is freely available — would be able to reconstruct the print job and produce their own copy of the document. How easy would it be to intercept that traffic and extract the pertinent information?

## IMPERSONATION

Impersonation represents a final issue facing network endpoints. When a network endpoint sends a user name and password, how does it know that the mail server to which it sends is the intended recipient and not an imposter? All too often, the endpoint simply requests the address of a remote system from a domain name server (DNS) and takes the

resulting response on faith.

We're familiar with the requirement that remote users need to prove their identities before they can have access to private systems. In fact, nearly everything requires a password, a certificate, a two-factor token or a thumbprint. On the other hand, a great many application protocols don't require that the remote system prove its identity to the user. Some do, of course.

HTTPS, for instance, uses SSL certificates to prove that remote web servers are what they appear to be. Unfortunately, incorporating such authentication measures is often impossible or requires additional layers of configuration. Prominent examples include post office protocol v3 (POP3), file transfer protocol (FTP), telnet, terminal services and tabular data stream protocol (TDS), which is used for communicating with Microsoft SQL Server.

If an attacker can control DNS, a great deal of mischief can ensue. Moreover, a great deal of network interaction takes place

behind the scenes. In particular, antivirus software, software update facilities, instant messaging applications and many other applications pull information from the network, sometimes without any means of verifying the authenticity of the source.

The problem does not end merely with network name lookups. It extends to the network itself. We're accustomed to selecting the wireless networks to which we'll connect by name — or allowing our notebooks to do this automatically. What assurance do we have that the access point broadcasting a particular ESSID (network name) truly belongs to the network we have in mind?

By cryptographically protecting the network, we can breathe easier. Open wireless networks, on the other hand, can be easily impersonated. Once again, if a notebook or other device is configured to connect to a given network automatically, the system could come under attack without the user's knowledge. ♦



# GLOSSARY



This glossary serves as a quick reference to some of the most essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

---

## ACCESS CONTROL LIST (ACL)

An ACL is a data set that dictates user permissions and access to particular objects within a network. The list consists of users and what actions each user is permitted to perform on a network object.

## BRUTE FORCE ATTACK

This kind of attack involves an attacker who possesses a legitimate user name for remote access and systematically attempts to guess the password login until the correct one is determined.

## DATA LEAKAGE

This term refers to the vulnerability of an organization's data confidentiality. Portable media, such as notebooks and USB drives, and shared communications, such as electronic documents, e-mails and instant messages, are all vulnerable points for data leakage and need to be secured.

## ENDPOINT

Network endpoints are devices such as workstations, notebooks, smartphones and PDAs (as well as printers and fax machines) that connect users into the network. They all require unique security consideration because of their access to the network.

## FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

FERPA is a federal law passed in 1974 that regulates access to student educational records.

## FIREWALL SANDWICH

A firewall sandwich is a term for implementing two different brands of firewalls at a network's perimeter, offering the added layer of protection of a second firewall if an attacker was able to discover a vulnerability in the first. This approach has fallen out of favor because of hardware costs and the complexity involved in administering such a setup.

## GRAMM-LEACH-BLILEY ACT (GLBA)

GLBA is a federal law enacted in 1999 that sets out rules and provisions for financial institutions that protect a citizen's financial records and information. These provisions include doing security assessments; developing and implementing security solutions that detect, prevent and allow timely incident response; and performing auditing and monitoring of the institution's security environment.

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA is federal legislation passed in 1996 that includes a privacy rule creating national standards to protect personal health information.

## INFORMATION SYNTHESIS

This term refers to the security problem posed by the proliferation of online content being catalogued and, therefore, searchable. An organization's private information can become vulnerable via data-mining and search strategies that collect a broad range of information on the organization.

## INTERNET PROTOCOL SECURITY (IPSEC)

IPsec refers to a suite of protocols that are used to secure IP communications via authenticating and encrypting each IP packet within a data stream. IPsec supports both transport and tunnel encryption modes.

## MAN-IN-THE-MIDDLE ATTACK

This term refers to an attack where the adversary impersonates a remote access system itself. Remote users are led to believe that an imposter system is, in fact, the legitimate source of remote-access connectivity. The attacker can inspect and alter all traffic between the remote user and the organization's network.

## PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

A set of security standards created to guide credit card processing companies in defending against fraud, hacking and other security threats. Processing companies must be PCI DSS compliant if they are processing, storing or transmitting credit card payments.

## POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

PPTP is a VPN protocol that ensures transmissions from one VPN node to another are secure. This protocol does not guarantee confidentiality or encryption, but relies on the fact that it's tunneled to ensure privacy.

## RISK AMPLIFIERS

The *frequency* and the *severity* of security incidents are two amplifiers of risk. If either of them increases or decreases, the security risk reflects this change.

## RISK ASSESSMENT

Good risk assessment identifies assets, includes threat modeling to identify sources of harm and prioritizes risks posed to an organization in terms of their likelihood and their impact. It should also include a team of engineers who examine a network for vulnerabilities and make suggestions on protecting assets and prioritizing risks.

## SARBANES-OXLEY ACT (SOX)

SOX is a federal law passed in 2002 that defines legislative audit requirements for corporations' financial reporting and improve the accuracy and reliability of corporate disclosures. From an IT perspective, SOX pushes corporations to archive and store any finance-related document or e-mail.

## SECURE SHELL (SSH) PROTOCOL

SSH is a protocol used primarily with Linux and Unix systems. It sets up a secure channel and encrypts the transmissions to ensure confidentiality and integrity of data over the Internet.

## SECURE SOCKETS LAYER (SSL)

SSL is a cryptographic protocol for communications over TCP/IP networks. This protocol encrypts segments of the transport layer protocols for an end-to-end connection across the network. SSL has been proceeded by Transport Layer Security (TLS).

## SHALLOW DICTIONARY ATTACK

This term refers to an attack where the attacker has a list of user names and attempts to guess the password for each user account. This kind of attack goes largely unnoticed and relies on the probability that at least one of the user accounts will have a trivially guessable password.

## TRAFFIC ANALYSIS

Traffic analysis is a security threat when carried out by outside parties. Even if the contents of the traffic remain encrypted, eavesdroppers can make inferences simply because the traffic is going on, and potentially put an organization at risk.

## VIRTUAL LOCAL AREA NETWORK (VLAN)

A VLAN is a logical local area network that extends beyond a single traditional LAN to a group of LAN segments. A VLAN acts as if it were connected even though it may actually be physically located on different segments of a LAN.

## WHOLE DISK ENCRYPTION

Whole disk encryption can happen via either a hardware or software solution. This approach encrypts every bit of data on a disk. The term "whole" refers to the fact that this is an all-or-nothing approach to encrypting. Users cannot pick and choose the files that they wish to encrypt; everything on the disk is secured.

# INDEX



Access control list.....	10	Multilayered security.....	9
Brute force attack .....	27	Payment Card Industry Data Security Standard (PCI DSS).....	7
Compliance .....	7	Point-to-point tunneling protocol (PPTP).....	26
Data leakage.....	4, 11-12	Remote access .....	25-28
Denial of service.....	26-27	Risk amplifiers.....	5, 8
Eavesdropping .....	25, 27, 31	Risk assessment.....	5-7
Endpoint .....	26-28, 29-32	Risk factors .....	5-6
Family Education Rights and Privacy Act (FERPA) .....	7	Risk transference.....	4
Firewall sandwich .....	9	Sarbanes-Oxley Act (SOX).....	7
Gramm-Leach-Bliley Act (GLBA) .....	7	Secure shell (SSH) protocol.....	26, 31
Health Insurance Portability and Accountability Act (HIPAA).....	7	Secure Sockets Layer (SSL) .....	26, 31, 32
Impersonation.....	31-32	Security process .....	7-8
Information synthesis.....	13	Shallow dictionary.....	27
Internet protocol security (IPsec).....	26	Traffic analysis.....	27
Man-in-the-middle attack.....	28	Whole disk encryption .....	12, 30

## Disclaimer

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.com. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. For all products, services and offers, CDW® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. CDW®, CDW•G® and The Right Technology, Right Away,® are registered trademarks of CDW Corporation. All other trademarks and registered trademarks are the sole property of their respective owners. CDW and the Circle of Service logo are registered trademarks of CDW Corporation. Intel Trademark Acknowledgement: Celeron, Celeron Inside, Centrino, Centrino Inside, Centrino Logo, Core Inside, Intel, Intel Logo, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Viiv Inside, vPro Inside, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. AMD Trademark Acknowledgement: AMD, the AMD Arrow, AMD Opteron, AMD Phenom, AMD Athlon, AMD Turion, AMD Sempron, AMD Geode, Cool 'n' Quiet and PowerNow! and combinations thereof are trademarks of Advanced Micro Devices, Inc. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a \$250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding security technology. CDW•G makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding security implementation. Furthermore, CDW•G assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication. The content contained in this publication represents the views of the authors and not necessarily those of the publisher. ©2009 CDW Corporation. All rights reserved.



CDWG.COM/SECURITYGUIDE  
888.510.4239



# ABOUT THE AUTHOR

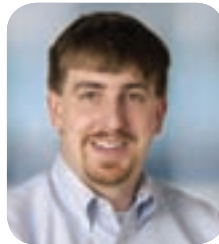
.....

## ORGANIZATIONS HAVE CHANGED COURSE.

Instead of devoting their efforts to protecting computers, the focus has shifted to protecting the critical data on them.

– Peyton Engel,  
CDW security expert

.....



« PEYTON ENGEL leads a team of security engineers at CDW. With the CDW (formerly Berbee) team since 1998, he has been responsible for its growth and management, including sales and marketing, since 2001. Peyton has presented his security research at national conferences including DEFCON (2004, 2006), ToorCon (2002, 2005) and USENIX/ LISA (invited speaker: 2003, 2005). Peyton’s chief technical interests are software security and the security relationships between systems in large networked environments. He works in Madison, Wis.

## SECURITY REFERENCE GUIDE

090318 • Flyer 59323CD

### LOOK INSIDE for more information on:

- Protecting against data leakage
- Conducting accurate risk assessment
- Deploying a multilayered defense strategy
- Securing endpoints and portable media



ISO 9001:2000 certified



CDWG.COM/SECURITYGUIDE  
888.510.4239



# ABOUT THE AUTHOR

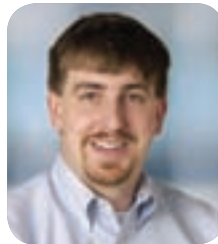
.....

## ORGANIZATIONS HAVE CHANGED COURSE.

Instead of devoting their efforts to protecting computers, the focus has shifted to protecting the critical data on them.

— Peyton Engel,  
CDW security expert

.....



« PEYTON ENGEL leads a team of security engineers at CDW. With the CDW (formerly Berbee) team since 1998, he has been responsible for its growth and management, including sales and marketing, since 2001. Peyton has presented his security research at national conferences including DEFCON (2004, 2006), ToorCon (2002, 2005) and USENIX/LISA (invited speaker: 2003, 2005). Peyton's chief technical interests are software security and the security relationships between systems in large networked environments. He works in Madison, Wis.

## SECURITY REFERENCE GUIDE

090318 • Flyer 59323AB

### LOOK INSIDE for more information on:

- Protecting against data leakage
- Conducting accurate risk assessment
- Deploying a multilayered defense strategy
- Securing endpoints and portable media



ISO 9001:2000 certified

