Chapter 1

Getting Up to Speed on Vista Security

In This Chapter

- Seeing what new security features Vista provides
- Understanding what you should protect
- Filling up your security toolbox
- Common sense and security

Although the security of Vista will ultimately need to pass the test of time, it is obvious that Microsoft put forth considerable effort to develop a more secure operating system (OS). To the user, Vista improves on some familiar features found in previous OSes and offers a variety of new security features and functionality that do a fine job protecting your system and both personal and sensitive data.

In this chapter, I provide an overview of the features and functionality of these new and improved-upon security tools that Vista provides and also explain the various things that you should consider securing to give yourself optimal protection. You can find out about selecting those tools that make sense for you to fill your security toolbox so you can get the job done. To top it off, you also discover how to integrate a common-sense approach to security to help you protect your system, privacy, and sensitive information not just today — but for the future as well.

Seeing What's New in Vista Security

Vista is touted by Microsoft as its most secure OS to date and the first OS designed with the Security Development Lifecycle (SDL) methodology. Security Development Lifecycle is a software design methodology that promotes the Secure by Design, Secure by Default, Secure in Deployment, and Secure in Communications principles. These principles offer a more secure approach

to software and systems development and deployment, and are indicative of the Microsoft commitment to security. Here, in a nutshell, are the principles:

- **Secure by Design:** This principle addresses the overall design and architecture of the application. The application is built upon solid security principles that take into account various threats and security vulnerabilities.
- **Secure by Default:** This is a principle that is used to reduce the attack surface of an application or system. By default, features or services that aren't needed are turned off, and applications aren't given any more authority than needed. As more features are needed, they can be enabled. However, by default, the system is as secure as possible.
- **Secure in Deployment:** This principle is related to keeping systems and applications up to date with OS or application patches to reduce any vulnerabilities.
- **Secure in Communications:** This principle relates to how an organization communicates security best practices. This communication plays a critical part in an organization's ability to have a secure computing environment.

The Vista OS consists largely of new code that was written under the auspices of this methodology, and any existing code leveraged by Vista was reviewed and revised to make it more secure. A variety of new features and functionality are available in Vista that assist the user in restricting user access, defending against spyware and malware, protecting against network related threats, and more.

The Vista User Account Control

Microsoft added a feature in Vista that provides some mitigation to a common mistake made by many users: namely, frequently using an account with elevated privilege to perform everyday tasks. Users mistakenly provide an account that they commonly use to log on to their system with the ability to modify system settings, change the Registry, install software, and more. What they don't realize is that this creates a substantial vulnerability if a malware program is executed in the context of such an account. The malware can then have authority to perform tasks and cause damage that it might not have otherwise been able to do.

User Account Control is essentially an intermediary that requests user consent prior to performing a task requiring elevated permission, such as changing system settings, installing software, and so on. In this way, it effectively treats every user as a standard user by default. Even if an account has the privileges to perform these elevated tasks, the user is prompted (see Figure 1-1).

For more on setting User Account Control, see Chapter 4.

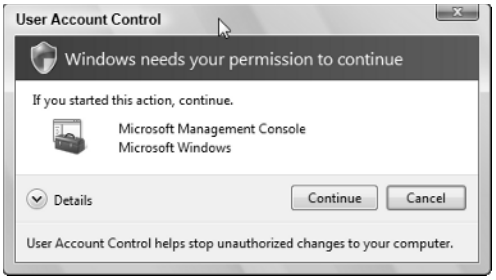

Figure 1-1: The User Account Control prompt.

Windows Defender

Spyware, a form of malware, has become one of the fastest growing external security threats in recent history, costing individuals and corporations considerable time and money. In its simplest form, spyware gathers Internet surfing habits and other information of user activity, without the user's knowledge, to be sold for marketing and advertising purposes. Outside of being considered by some as a violation of privacy, gathering this information consumes valuable CPU and memory resources of your computer, sometimes bringing your system to a crawl. Users often spend time and money to rid themselves of these intrusive programs to return their system to a normal working state.

The Microsoft answer to the spyware threat is Windows Defender (as shown in Figure 1-2), which is an easy-to-use and effective tool that can detect and deal with spyware both in real time and by means of on-demand scanning. Because Windows Defender is native to the Vista OS, you finally have a tool to deal with this growing problem without the need to purchase expensive third-party products. Some of the features in Windows Defender offer the following:

- **Easy-to-use interface:** Windows Defender provides an intuitive interface that is accessible via Security Center or independently.
- **Quick scan:** Defender affords you a quick and easy way to perform a scan of only those areas that most often hold spyware — such as specific areas of the Windows Registry and the Windows\System32, program files, and user directories — rather than scanning your entire system.
- **Full scan:** This gives you the ability to scan your complete system at the click of a button. The tool scans every drive and directory on your system.
- **Custom scan:** This option provides an interface for the user to customize a scan that better fits their needs. With a custom scan, you can select specific drives and folders that you want to scan.

- **Real-time scanning:** Windows Defender protects your system in real time so that if spyware infections occur, they can be detected and remediated.

Read about all these types of scans in Chapter 14.

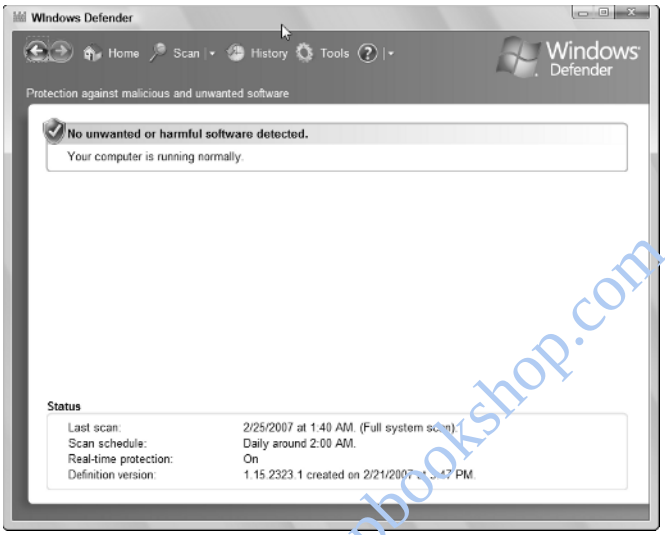

Figure 1-2: The Windows Defender interface.

Parental Controls

Like it or not, computing is becoming a fundamental part of our lives. Accesses to computer labs in elementary schools (and beyond) enable our children to become computer savvy at an early age. Students use computers to do research and homework, take quizzes, and communicate with their peers. Many would find it difficult to get through high school, even from purely an academic perspective, without access to an Internet-connected computer. Our children have a plethora of information available to them by a simple click of a mouse. Even though the Internet is a great resource, it does present certain risks. Now more than ever, our children have access to information and situations that may place them, or the data on our computers, in harm's way. Such situations have created a strong market for software products that monitor computer activity and block access to certain Web content, file downloads, and more.

Windows Vista offers the Parental Controls security feature (as shown in Figure 1-3) that provides monitoring and restriction capabilities to assist you in addressing this problem. Parental Controls provides the following capabilities:

- **The Vista Web Filter:** This function of Parental Controls allows you to block access to a specific Web site or specific types of Web content such as those rated as mature or for pornography, hate speech, drug-related, alcohol, gambling, weapons, and more.
- **File-download blocking:** Many know all too well the file-sharing sites that teens like to visit to download shared software, music, and movies. Such sites not only harbor illegally shared files but also serve as virus depots, infecting many of those unsuspecting people who download files. Parental Controls enables you to block a user from having the ability to download files from the Internet.
- **Time restrictions:** For those of you who worry about children getting out of bed in the middle of the night to chat online with their friends, Parental Controls allows you to grant or block access for certain users to the Internet during hours that you specify.
- **Gaming restrictions:** Parental Controls allows you to restrict a user's access to play a specific game or restrict a user's access based upon specific game ratings such as Early Childhood (EC), Everyone 6+ (E), Everyone 10+ (E10), Teen (T), Mature (M), or Adults Only (AO). Gaming access can also be restricted based on specific content, such as Alcohol, Blood, Gore, Cartoon Mischief, Crude Humor, Drug Reference, Fantasy Violence, Language, Lyrics, Mature Humor, and so on.
- **Monitoring capability:** Parental Controls allows you to monitor certain online activity of nonadministrative users. Reports can be viewed for the Top 10 Web Sites Visited, Most Recent 10 Web Sites Blocked, File Downloads, File Downloads Blocked, Logon Times, Applications Ran, Games Played, as well as certain e-mail, instant messaging, and Media Player events.

Parental Controls provides parents or a computer system's administrator some very nice features to monitor and restrict access of standard users. Parental Controls has functionality that has never been offered previously by an OS as well as perhaps enough functionality to circumvent the need to purchase third-party tools.

Wireless security enhancements

Wireless networking, which was once an expensive and relatively slow networking option, is on its way to becoming the preferred method of network connectivity for the home and office. Vista brings with it a variety of wireless networking enhancements, a few of which are related to security:

- Support for previous wireless protocols and the latest security protocols, including Wi-Fi Protected Access 2 (WPA2)
- Ability to define security polices to securely manage wireless connections at home or in the office

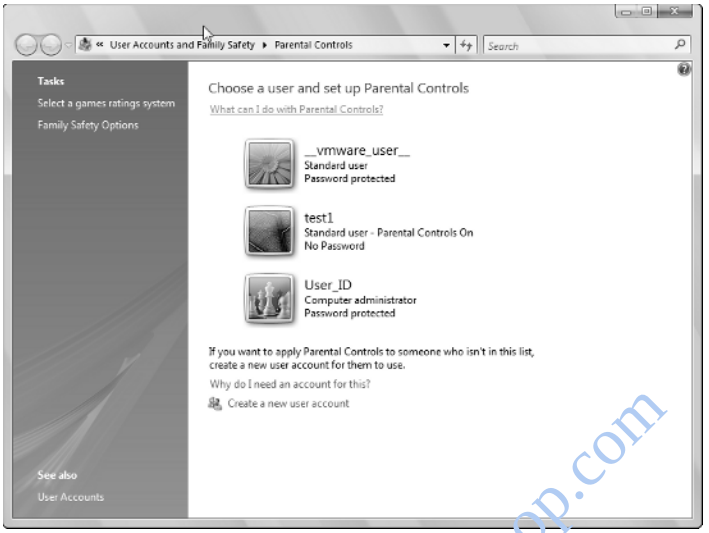

Figure 1-3: The Parental Controls interface.

Vista offers support for nonbroadcasting networks and even allows you to connect to a nonbroadcast network on your preferred list. However, don't be fooled into thinking that a nonbroadcasting network is more secure; sometimes, it is actually less secure. Even when you run the Vista OS and a nonbroadcasting network does not advertise its name (that is, the *service set identifier (SSID)* is set to a null value), some risk exists if other systems on the network are running Windows XP Service Pack (SP) 2. The problem is that systems running Windows XP SP2 will send a broadcast, even if your wireless network is configured as a nonbroadcasting network. Therefore, it is generally a bad idea to implement a nonbroadcasting wireless network as part of your security plan — security by obscurity is never a good idea.

Service hardening

Windows services are applications that provide OS functionality, are low-level application tasks, run in the background, and usually require no user interaction. Although services are essential to the operation of your system, they have historically presented a significant attack surface for malicious code writers. Service hardening is not necessarily a new security concept but has largely been the responsibility of the user — until now.

The Vista service hardening features are just one part of a multilayered security strategy that embeds security within the OS to reduce the risks associated with exploits that might target your systems. The real focus of service hardening isn't to prevent such attacks as much as it is to reduce the damage such an exploit can cause to your system if a service is compromised.

Vista service hardening provides security in the following key areas:

- **Least privilege service permission:** In previous Windows OSes, services ran largely under the local system account — which is, essentially, the most powerful account on your computer — even if they did not require such privilege. Vista allows services to run with the least privilege that they might require, such as Local Service or Network Service. Additional restrictions can be placed on a service to limit the areas of the Registry or file system that a particular system has the ability to write to.
- **Service isolation:** This allows a service to be *separated* (isolated) from other services or applications. Such isolation helps reduce the attack surface.
- **Firewall policy integration:** Vista allows firewall policies to now be applied to services. Because network-facing services are often the target of exploits, this feature can go a long way in limiting the attack surface of your system.

Vista provides a very comprehensive security approach to service hardening. With the exception of a few additional steps that can be taken to secure the Registry with regard to least-privilege permissions, Vista handles service hardening and requires no interaction by the end user.

For more on service hardening, see Chapter 7.

Internet Explorer 7

Although Internet Explorer 7 (IE7) is part of the Vista OS, it can be installed as a separate application independently from Vista. Microsoft has put a great deal of effort into making Internet browsing more secure and changes in IE7 certainly reflect that.

Internet Explorer 7 provides the following security features:

- **Protected Mode:** This defense-in-depth security feature restricts where files can be downloaded and executed, or the ability to invoke other programs without the user's consent.
- **ActiveX protection:** ActiveX are small, Microsoft application components that provide functions to the end user via their Web browser. Internet Explorer 7 provides security mechanisms that reduce potential risks of ActiveX exploits, such as ActiveX Opt-In and the ability to control ActiveX for a particular zone or site. Chapter 13 covers ActiveX security in more detail.
- **Cross-domain scripting protection:** Cross-domain scripting attacks have presented a significant security threat in previous versions of Internet Explorer and Windows OSes. Internet Explorer 7 forces scripts to run in

their original context, even if they are redirected to run in another security domain, mitigating much of the risk associated with cross-domain scripting attacks.

- **Security status bar:** This feature allows you to differentiate an authentic Web site from one that is considered to be suspicious. The status bar also provides you with digital certificate information that can help you determine whether a site is trustworthy enough to make an e-commerce transaction.
- **Integration with Parental Controls:** Internet Explorer 7 integrates with Parental Controls security features, allowing more control over Internet browsing and downloading functionality.
- **Phishing protection:** The IE7 Phishing Filter provides some impressive functionality to protect you against an Internet phishing scheme that just might make you that next identity theft victim. Web sites that you visit are analyzed. If the site is a known phishing site or otherwise has characteristics that are commonly found in phishing sites, you will be warned of the potential danger.
- **Protection of personal data:** Internet Explorer 7 offers the ability for one-click cleanup of information entered in Web sites, browsing history, temporary Internet files, and so on that could potentially hold tracking or otherwise Personally Identifiable Information (PII) of the user.
- **URL display:** Crooks commonly attempt to mask a site for which they are directing you. One of the ways how crooks try to hide this is by displaying a pop-up without an address bar so that the URL of the site is not displayed. Internet Explorer 7 now requires an address bar in every window so that you can more easily identify whether the site you're being directed to is a trusted source.

For more on Internet Explore 7 security features, see Chapter 13.

Encryption with EFS and BitLocker

Now, more than ever, we use our computers to process or hold sensitive information. Whether our financial files, medical information, or private e-mail messages, this information has the potential to be the golden nugget to crooks trying to perpetuate identity theft or other crimes of fraud. To add to the problem, more of us are on the move, using portable computers that are more easily lost or stolen, ultimately putting our personal or corporate data at risk.

Vista offers the Encrypting File System (EFS) and BitLocker Drive Encryption to help you protect your sensitive information that is resident on your computer from theft.

- **Encrypting File System (EFS):** Offered in the Business, Enterprise, and Ultimate editions of Vista. Encrypting File System provides file and folder level encryption of user data. For more on Encrypting File System, see Chapter 9.
- **BitLocker:** Offered in Enterprise and Ultimate editions of Vista. BitLocker (as shown in Figure 1-4) provides data protection by preventing unauthorized users from accessing a lost or stolen computer. The entire windows volume — such as all user and system files — are encrypted. For more information on BitLocker, see Chapter 10.

Figure 1-4: The BitLocker interface.

Windows Security Center enhancements

Windows Security Center (WSC) made its first debut in the Microsoft Windows XP OS. It returns in Windows Vista with a similar look and feel but with some enhanced functionality. Windows Security Center (shown in Figure 1-5) continues to provide a single interface to manage multiple security functions, some of which are native to the Vista OS and some (such as third-party antivirus software) that are not. New WSC enhancements in Vista include the following:

- **Other Security Settings category:** Offers you the ability to monitor and manage IE security settings and User Account Control (UAC)
- **Malware Protection category:** Provides the ability to monitor and manage antivirus and anti-spyware settings

- **Manage multiple products:** Allows you to manage multiple firewall, anti-spyware, or antivirus products either native to Vista or third-party tools
- **Vendor resources:** Provides direct links to vendors of the products that you have installed to get updates or other fixes to remediate issues

For more on Windows Security Center, see Chapter 3.

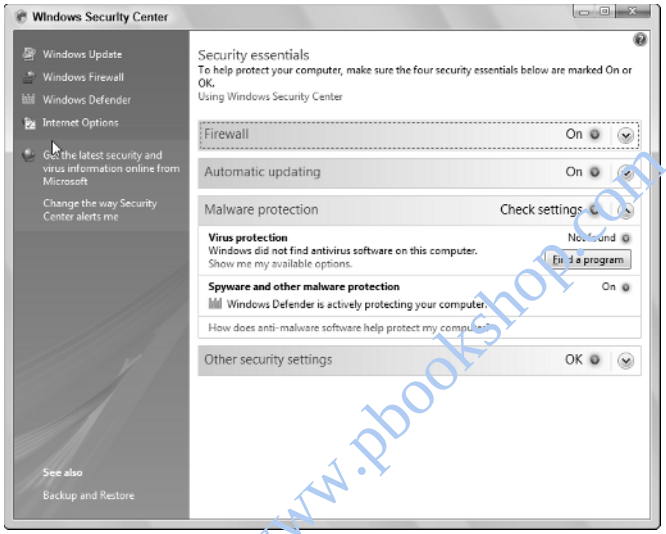

Figure 1-5: The Windows Security Center interface.

Windows Firewall enhancements

Like WSC, Windows Firewall (as shown in Figure 1-6) also made its debut with Windows XP. It, too, returns in Vista as a significantly enhanced tool. The new Windows Firewall enhancements include the following:

- **Easily configurable through two different interfaces:** Windows Firewall is configurable via Security Center and also through the Microsoft Management Console (MMC) snap-in for those who want to implement some advanced settings. The advance settings provide a more resolute approach.
- **Filtering of incoming and outgoing traffic:** Vista Firewall, unlike previous versions, allows for outbound filtering.
- **IPsec integration:** This provides an advanced security-setting console that integrates IPsec and firewall management and allows for IPsec server isolation and other customizable IPsec settings.
- **Firewall profiles:** Although the previous version of Windows Firewall did allow for profile configuration, Vista Firewall provides for more profile

options, such as Domain, Public, and Private Profiles for yet even more tenacious security than its predecessor. Such tenacity allows you, for example, to provide certain settings to your office connection yet quite different settings to your home connection.

For more on Windows Firewall, see Chapter 11.

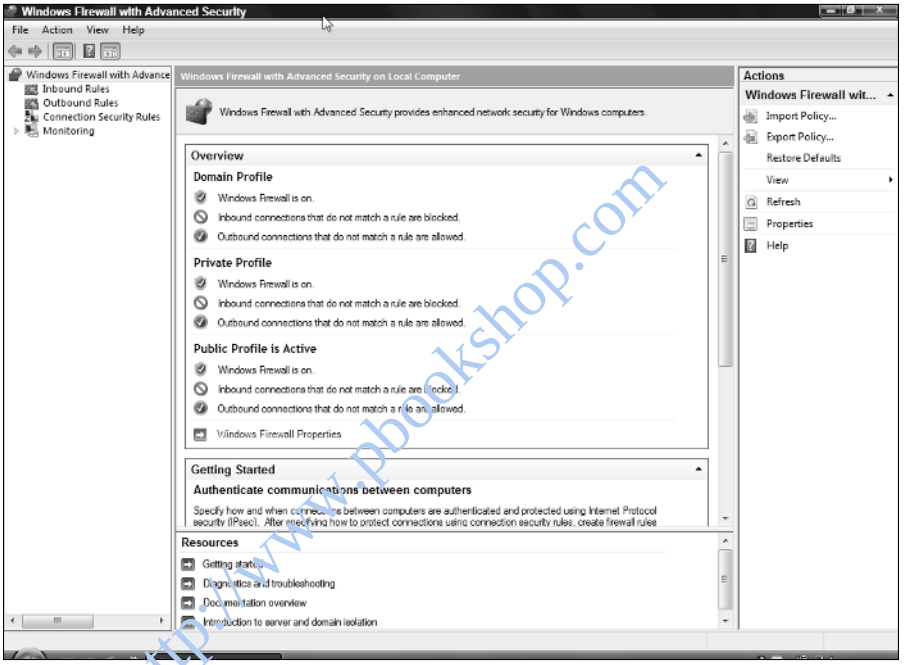

Figure 1-6: The Windows Firewall interface.

Knowing What to Secure

So you have available to you one of the most secure Windows operating systems offered by Microsoft to date. Now what? Although Vista has many security enhancements beyond earlier Windows OSes, it can't read your mind and magically protect those things that are so very important to you. Before you can implement the Vista security features that make sense for you, you must first understand what it is that you need or want to protect.

Hardware and software

When you think about what it is that you want to protect, it isn't necessarily intuitive that you might consider hardware and software — especially when thinking about it under the context of selecting security features in an OS. Even

still, as you lay out your security plan and find out about Vista security features and functionality, keep in mind what value you place on your computing hardware and software. Consider the following relative to hardware and software security:

- **Hardware:** Protection against theft or damage from natural disasters isn't something that Vista can provide; however, as you develop your security plan (see Chapter 2), you need to be cognizant of hardware. Throughout the book (particularly in Chapter 18), I cover some of the third-party security tools that can help you mitigate some security risks associated with your hardware.
- **Software:** Vista provides various security features that enable you to further secure the configuration of your software applications and better protect your system and data from compromise. In addition, as part of your security plan, consider properly securing physical access to your software and associated licensing information. Although Vista can't help you with this, it is an important part of your security plan. For more information regarding your security plan, see Chapter 2.
- **Availability:** Protecting the availability of your system is ensuring that your hardware and software are available to you when needed. If you, like many of us, depend on your system to perform essential functions, then having it unavailable might not be a mere inconvenience but perhaps translate into real financial loss. Vista offers various security features that provide you some protection and ability to restore your system quickly in case of an OS or software failure. Various third-party tools are also available that can provide you some level of availability protection; see Chapter 18.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information that can be used to uniquely identify you, such as your name, address, driver's license, Social Security number, medical records, financial files, and more. Even if you might not fully understand how valuable your personal information is, crooks who perpetrate lucrative crimes (such as identity theft) will and do go to great lengths to harvest it. A piece of your information here, a piece there — pretty soon they have enough of your information to pretend to be you. Perhaps getting a utility service in your name, posing as you when receiving a traffic ticket, getting a credit card in your name, or even purchasing a car or house in your name! Sounds far-fetched? Think again — it happens every day.

For many of us this personal information, or bits and pieces of it, is often contained in various documents, spreadsheets, or other programs on our personal computers. After all, we have our computers so that we can be

productive — do our taxes, our budgets, process medical claims, do online banking, and more. I'm not suggesting that you not use your computer this way, but I am suggesting that you take protecting your personal data seriously.

The market for your personal information has never been greater. Crooks who don't use it themselves can get a nice price for it on the black market, selling it on the Internet in just a matter of minutes. This means that you must protect your personal information that resides on your computer ferociously. Luckily, with the help of Vista and this book, you'll be able to do just that.

Sensitive information from work

You're not the only one that has sensitive information. Corporations also have proprietary business information that is as sensitive to the business as your PII is to you. This proprietary business information might include, but is not limited to

- **Physical security:** As a trusted employee or business owner, you might have access codes to offices, safes, alarm codes, or other information related to physical security at your workplace saved on your computer.
- **Customer or sales information:** Employee computers commonly have sensitive contract information, customer databases, rate schedules, and sales and marketing information.
- **Vendor information:** Such data might be information regarding vendor supply terms, contact information, or other information that pertains to various vendors and suppliers that should not be public knowledge.
- **Employee-related information:** Such data might include payroll information, healthcare plan information, or personal information of other employees of a business.
- **Trade secrets:** Certain employees might have digital research data, patent, or design information on their computer systems that they want to protect from their competitors.
- **Company financials or assets:** This information could be the financials of the company, business tax information, departmental budget information, or information on other physical or intellectual assets.

As an employee or business owner, you might either now or later have sensitive information from work on your computer — and you need to understand how to secure it. With the help of Vista, perhaps some third-party tools, and this book, you will have everything that you need to amply secure this information.

Other information that can be used adversely

Here is the stuff of nightmares for a lot of us: an e-mail of a delicate or untoward nature that gets made public or falls into the wrong hands. You know, that e-mail you sent to a co-worker describing those annoying tendencies of your boss, or the document that you wrote to your significant other, or information on that Web site that you visited looking for a better job, or those off-color jokes that you've been e-mailing around the office.

Our computers might hold data other than that considered to be business propriety or PII. Yet, it might be information that is of a personal or private nature and, if made public, could cause us embarrassment or otherwise get us in hot water. Like other sensitive information, this information should be protected as well. Although its compromise might not lead to someone driving around in a car in your name, it certainly might adversely affect you if it were to become known to others.

Filling Up Your Security Toolbox

If you're going to effectively protect your hardware and software, PII, sensitive work-related information, or any other data that, if compromised, could have an adverse affect on you, having the proper tools to do so is critical. Just like carpenters, plumbers, and other craftsmen stock their toolboxes so that they can effectively practice their crafts, you, too, must fill your security toolbox with the proper tools to get the job done.

Understanding your requirements

As much as you want to jump in and get started filling up your security toolbox, understand what requirements you have. Not only will you select the right security tools to get the job done *today* — but perhaps for some time to come. When you understand your requirements, you can better prepare yourself down the road to address security threats as they present themselves. The following are some considerations in understanding your requirements:

- **Up-front work:** Before you can fill your toolbox with the right tools, you really need to understand your requirements. Much like that carpenter who needs to understand what type of work he will be performing so that he grabs the right tools to perform his craft, understand what it is that you want to achieve. Specifically, you must understand what it is that you want to protect. Whether your goal is to have the least amount of downtime,

protect a particular document or file or protect your computer from being stolen, or all these things — understand your requirements so that you can select the proper tools to get the job done.

- **Criticality:** Not only do you need to understand what it is that you want to protect, but you also must understand how critical it is to protect it. Understanding the length to which you are willing to go in order to protect your system or data is essential in developing a security plan and selecting the right tools to meet your needs.
- **Security tolerance:** Security is often the opposite of convenience. You can do a great many things to protect your data, but too-stringent security controls can impede your ability to do certain things. In fact, Vista puts forth some security controls that will be considered by some folks as annoying. You can choose to use that security feature (put that security tool in your toolbox) or instead leave it out and opt for more convenience over security.

For more on security requirements, see Chapter 2.

Arming yourself with technical tools

Other tools you will have in your security toolbox are technical tools, which will play a large part in protecting your system and sensitive data from compromise. Vista offers a variety of security tools to assist you in appropriately protecting your hardware, software, and associated data. The majority of this book covers those Vista tools, but I also cover some additional third-party technical tools that you might need to consider when your requirements go beyond what Vista can provide. Here are some considerations when selecting the technical tools for your security toolbox:

- **Understand the tools that you have available to you.** Understanding all the tools that you have available to protect yourself is indeed important. This book provides you not with just the Vista tools that are available to you, but also with some third-party security tools that can provide some protections where Vista comes up short.
- **Understand what the tool protects.** Not all security tools are created equal. Some protect access, others assist with maximum availability, and even others might have entirely a different purpose. If you understand explicitly the protections that the tool provides, you can then make a better choice as to when and how to use it. I show you exactly what each Vista security tool can help you protect — and, just as important, what each can't protect.

- **Understand how to use the tool.** It isn't good enough just to know what tools are available and what it is that they protect: You must also know how to use them. I show you how to use each of the security tools in Vista, and provide you with some information on third-party tools if your requirements go beyond what Vista can provide.

Integrating Common Sense and Security

Not to be taken lightly or meant to be condescending in any way, but the fact is that almost every technical security control can be circumvented by some type of user behavior. At one point or another, you have likely either participated in or witnessed activity that caused security to be less effective than it otherwise could have been. My favorite is walking around the office noticing all the sticky notes on co-worker's monitors and keyboards with passwords scribbled on them for all to see.

Because security is often an inconvenience, you or people that you know will be tempted to exercise certain behavior that might not make the best use of the tools that you will find out about. Therefore, it is very important that you take the following into consideration:

- **Make security a frame of mind.** Take security seriously. Pay close attention to those things that you do that might put your system, PII, or sensitive information from work at risk. The more you make security a frame of mind, the better you will protect those things that are important to you.
- **Security is a process.** Understand that it takes more than thinking about security or technical security tools to make your system and data secure. Security is a process for which many things must come together if you are to truly achieve optimal security. This book help you bring all those things together so that you can ultimately have a security strategy that meets your requirements.

When you fill up your security toolbox with some of the new and improved-upon Vista security tools (and perhaps even a few third-party tools), don't forget to throw in a fair amount of a common-sense, security-minded approach to securing your system and data. Together, these things will provide you the ability to protect what' important to you, time and time again.