Lunch Break SERIES

Why IT Security, Auditing and Compliance Matter

Security breaches can hit large and small companies alike, but when it happens to small companies, the results can be devastating. Here's a reminder of what's at stake and what you need to do to make sure your data remains safe and in compliance. Plus, stay on top of system security issues by setting up Security Compliance Manager the right way.

IT Pros, Take Charge of Your Security 1

Survive Your Own Audit 3

Microsoft Security Compliance Manager: Security Settings Simplified 7

SPONSORED BY

Redmond

Redmondmag.com

Centrify

BY DON JONES

IT Pros, Take Charge of Your Security

It's time companies erase the notion that IT security be left to a security expert. Instead, IT pros should take charge and become that expert.

In early June, Citigroup acknowledged yet another major breach of confidential customer data. It was the 251st such public notification this year, and could put us on track to exceed the 597 improper disclosures from schools, government agencies, and businesses in 2010.

According to an article in USA Today, cybercriminals are now "actively probing corporate networks for weaknesses," and businesses face particular pressure to let the public know when they've been hacked. Citigroup, in fact, was criticized by U.S. Representative Jim Langevin for taking a month to notify customers after noticing the most recent breach, which was discovered during routine monitoring. Customers' names, account numbers and e-mail addresses were all compromised.

Citigroup joins major global companies like Sony, Epsilon, Nasdaq, PBS, Google, RSA, Lockheed Martin, L-3 Communications and Northrop Grumman in being the victim of a cyberattack. Companies are more forthcoming about breaches due in part to data loss disclosure laws that are now in force in 46 U.S. states. Public companies must be especially upfront with such disclosures: Data breaches can obviously create a negative impact on business, and failure to disclose such impacts can be a violation of SEC rules and invite shareholder lawsuits.

A recent survey by Ponemon Institute and Symantec estimates that data breaches cost, on average, $7.2 million to put right—and those costs continue to climb. That's in addition to fines and fees imposed by industry groups and government legislation, making data breaches tremendously expensive.

Let's face it: We tend to give a lot of lip service to security, but you and I both know that most organizations' security, under the hood, can be pretty haphazard. Are all the permissions on your files and folders truly accurate? Are group memberships all up to date? Are you sure? Is your firewall configured properly—no unnecessary holes? Is the software up to date?

Having security flaws is almost unavoidable, simply because most products' native tools do a very poor job of letting us manage security. Go through every object in Active Directory and tell me if it has the correct permissions. Go ahead, I'll wait. You'll be a while if you're using Active Directory Users and Computers to check. Even Windows PowerShell offers fairly primitive tools for monitoring and modifying permissions, in part due to the highly distributed and extremely complex permissions structures that Windows products tend to use.

But the newspaper headlines make it clear that we'd better get on the ball. In general, you're going to need to implement three broad capabilities:

- **Protect.** You need to be able to apply the proper permissions to resources, proper configuration to security elements of their infrastruc-

tures, and maintain those settings over time.

- **Inspect.** You need the ability to continuously monitor and audit your environment to ensure that the proper permissions and configurations are in place.
- **Detect.** You need proactive monitoring and alerting to let you know when a problem does occur, so that you can take remediation steps and make the proper disclosures.

In many cases this is going to require the use of third-party tools from independent software vendors. I know, nobody likes to spend money on those things. But you're not going to be able to write a PowerShell script that does it all, much as I wish that were the case. In many cases, you'll need software that gathers distributed permissions and configuration information into a single place, analyzes that to produce reports, and uses that to generate automated alerts when necessary.

Yes, I realize that "you've never been hit." I'm sure Citigroup, Sony, and PBS felt the same way—and they got hit. Hard. Sony alone lost millions by having to take its network offline for weeks, not to mention the public relations disaster. And that was one attack. Oh, "you're not a big company, so you're not a target?" Sure, not yet. But you will be, once attackers figure out that you too have a few thousand bits of interesting information on your network and that you're a much easier target than Citigroup or Lockheed Martin.

It's probably time to give your security a quick review. Take your honest opinion to your executive team, along with a proposed plan to put things right. Have your numbers in place: This is what it's going to cost us, and this is what we stand to lose if we don't. Be able to explain why you can't fix it on your own—including, if necessary, a brief demo of why permissions and configurations are difficult to monitor and manage using the in-the-box tools. Most executives simply don't realize how difficult it is, so you'll need to educate them.

Be a security leader. R

BY ROBERTA BRAGG

Survive Your Own Audit

A well-designed internal security audit can help you uncover soft spots in your system before an outsider points them out. Put on a trench coat, grab a clipboard, and start roaming the halls.

The purpose of a computer system security audit is to evaluate how well the current security policy has been implemented. Auditing lets you know if things are going according to plan.

What? You don't have a current security plan? That's an even better reason to perform an audit. Judging your systems against some commonly agreed-upon security areas can be enlightening. It can also help you develop your own security policy, since it exposes weaknesses you might not know you have, as well as reasons for incorporating security into your overall systems design.

An audit compares proposed security features against the reality of implementation. It compares current security to generally accepted security measures, given the anticipated security risks in the given situation. A good audit tests the current system with both non-invasive and invasive means.

It doesn't certify a system as secure; it merely judges the relative strength of security measures in effect against possible intrusion methods. A good audit will expose weaknesses, add a measure of accountability, and offer corrective measures. As a result, you can prevent intrusions, or at least detect them quickly and correct them.

A security audit promotes the model of allowing your users a range of access to computer systems, while still monitoring their activities.

In a small system, a formal audit may be unnecessary. It's possible to see if policy is working by simple observation and informal review. In a

Privileged User Activity Auditing

Do you know what your outsourced IT users are up to?

FREE DOWNLOAD

Centrify DirectAudit records and replays privileged user sessions on Windows servers. There's never been a better way to know if your IT contractors and outsourced staff are solving problems...or creating them.

Windows IT Pro 2011 Editors' Best GOLD

Windows IT Pro 2011 Community Choice GOLD

Winner of both the Editors' AND Community Choice Gold Award for Auditing and Compliance!

Download DirectAudit now at centrify.com/windowsaudit

Centrify

large network composed of many different OSs in many locations, a formal audit using audit tools is necessary. Every system, however, can benefit from some sort of security audit; pick the level that fits your organization.

You can conduct a computer system security audit by either external or internal personnel, or a combination of both. Many independent consulting firms offer this type of audit, as do major accounting firms. Many companies consider this function to be a part of their internal audit and control organization. You can even get certified in it, as a Certified Information System Auditor.

In this article I provide a methodology for conducting an internal audit. Such an audit isn't meant to reduce the need for possible outside intervention.

As a preliminary step, rate your computer systems by taking the audit survey (click here to view the Security Self-Audit). and strengthen your security prior to audit by external personnel. Only company management can determine if you should engage outside resources for future audits.

Where Do You Start?

An audit should consider not only your programs and hardware but also the facilities, data, and people involved. A good audit should judge each area by the level of confidentiality, integrity, availability, and reliability of information maintained. It should judge each system relative to the actual risk (not the perceived risk) of fraud, error, business interruption, and data compromise.

The size of the company as well as the confidentiality of the information will determine the need and frequency of the audit. If you've never conducted an audit, you should do it now and set a periodic time for follow-ups. Audit again after any changes to security policy and after the implementation of major changes or additions to data systems.

Types of Audits

Auditing can be a lengthy process. Listed below are different techniques you can use to audit your computer systems. A good security audit uses techniques from all areas. The proposed point system described in the Audit Survey is merely a way to judge your system's security against some typical scenarios. Your system may not fit this typical model.

Auditing by Questioning

With this method, you and staff members roam about with a standard questionnaire, asking questions relevant to security policy and implementation. Probe for details and consider attitudes, but accept answers as gospel at this point. Like a good detective, your job will be to compare these answers. By questioning numerous people who do the same thing, you'll have a better idea of reality. You'll want to try to avoid asking questions that tip off what the answer should be.

Rather than having people fill out a survey, use direct face-to-face association for the questioning process. Some of the best questions to ask are those that might come up during the normal working day. Ask whether you can use another password, or whether another user can work at a station that's already logged on. Another big question to ask: When the door to the server room should be locked. Ask about building hours and how that's enforced. Determine who has keys.

Auditing by Walking

A basic method of the security auditor should be walking around. Information about the security of the physical domain, the attitude and security awareness of workers, and the effectiveness of the current policy can often be gathered by observation. Force yourself to react to what you're seeing and hearing as if you were an outsider. Look for obvious physical issues and listen to casual conversation. If people know who you are, you may want to enlist other knowledgeable people in your company to assist in this process. However, most people can't quickly respond to unexpected questions with anything other than the truth. In other words, most people are crummy actors.

During this process, be sure to check your building after hours. Who's entering and exiting? Do they have that authority? Are doors propped open during breaks? Is anyone paying attention to whether equipment comes and goes?

Auditing by Documentation

The entire configuration of your network should be documented. Do this by physical inspection (some of which can be accomplished via software), not by user survey. After examining each server and workstation, you should have:

- A list of installed software and appropriate licensing information.
- Configuration information, such as installed and enabled services, protocols, and bindings.
- Attached printers or managed network printers.
- Configuration of services, utilities, transports, and ports.
- A list of users and their permissions and rights on this system.

Document the network architecture. Where are routers, hubs, and switches, and how are they protected? Which servers and workstations are in which subnet?

Auditing By Checking

With security policy in hand, verify system components and configurations against policy directives. In this case, the results aren't subjective unless the policy is. That is, either the policy is followed or it's not. Note the exceptions and any circumstances. Also note inconsistencies, and weaknesses in policy and in implementation. (Read my October 1998 article, "Hardening NT," for a proposed configuration policy for Windows NT Server.)

Invasive Auditing

Thus far we've concentrated on non-invasive means. We've audited by observation, inspection, comparison to policy, and discussion. Security audits also include invasive tactics. What good is a perfect score after observation if a simple gesture by a hacker can penetrate your system or shut it down? A good security audit uses the same techniques available to hackers and crackers to probe for holes in the security system.

Like the heart specialist who prefers diet, exercise, and medication to open-heart surgery, I must caution you about invasive techniques. As important as they are in auditing security, there are two potential problems.

First, using these techniques without a defined policy and procedure for their use could result in your termination and even arrest. This is a policy and procedure that needs to be approved at the highest levels. Don't use these techniques without this approval, in writing, and don't use these techniques against another companies' networks.

Second, by initiating improper attacks on your company's computer information systems, you could destroy data , cripple the systems, and risk the exposure of confidential information.

That said, properly approved and used invasive attacks can assist the security professional in building appropriate defenses. The topic is far more extensive than I can cover here, so see "Hacker Tools for Auditing" for specific references to types of programs you'll need to defend against. I also list some tools you can obtain to test current defenses. The sites I mention will lead you to other sites and other tools. Educate and protect yourself thoroughly before you even begin to plan this type of system surgery.

Evaluating Results

Once you've performed your audit, what next? You're likely to find many things that need attending to. Your first job is to evaluate these newly discovered weaknesses against the actual risk of encountering attacks in the real world. If you've properly designed the audit, you may have eliminated some unreal risks already. Next, you must develop a strategy for improving security so that these newly found holes aren't exploited. Put together a checklist of items to address and assess the cost and appropriateness of each action. If you have a stated policy in place, items that violate this policy should be addressed first. If you've found new areas or areas that require a change of policy, solutions to those may have to wait.

Reporting and Recommending

Make the results of your security audit available to management, along with what it means. Share this information with an emphasis on three key items.

- **Vulnerabilities:** Where are system weaknesses? Are they relevant? What is the cost of effecting remedies? What is the potential cost of doing nothing? Are there alternatives?
- **Strengths:** How strong are current defenses? If password crackers were unable to crack passwords on the network, let's hear about it. If current policy directives are being carried out, make it be known. If server configurations match policy, sure to reward administrators by indicating this.
- **Recommendations:** As the most knowledgeable person on computer security implementation, what are your recommendations? Be sure to include a timetable, implementation costs, and appropriate media for signoffs. After all, if you've found problems, you'll want to correct them. Since your report will heighten management's security awareness, this is a good time to obtain approval to move forward with plans for improvement.

Concrete Ideas

Whatever the results of your security audit, you should have some concrete ideas of how to improve network security when you're done. You should also have a better sense of the amoebic structure of your network, the attitudes of personnel toward their equipment and software, and a better security awareness on the part of management and personnel. Don't drop the ball here. Use that information to promote and ensure security in your network. The health you save may be your own. R

About the Author Roberta Bragg, MCSE: Security, CISSP, Security+, and Microsoft MVP is a Redmond contributing editor and the owner of Have Computer Will Travel Inc., an independent firm specializing in information security and operating systems. She's series editor for Osborne/McGraw-Hill's Hardening series, books that instruct you on how to secure your networks before you are hacked, and author of the first book in the series, Hardening Windows Systems.

BY PAUL SCHNACKENBURG

Microsoft Security Compliance Manager: Security Settings Simplified

The forthcoming version of Security Compliance Manager is more accessible, flexible and capable.

The original Security Compliance Manager brought together Microsoft's best practices around security settings. It provided detailed explanations for each recommended setting and let you export customized baselines as Group Policy Objects for widespread distribution. It helped you apply the right security settings without having to plow through reams of documentation.

However, there was no way to compare your current settings with the Microsoft recommended baselines, apart from manually looking through settings. The new version of SCM closes this gap. The improvements in this new version are based on real-world customer feedback, making SCM much more accessible to the average IT professional. It also adds several new features.

"Everything we did in SCM version 2 was in response to direct customer feedback," says Jeff Sigman, senior software design engineer at Microsoft. That led to the three main areas of focus. "Customers needed to import their existing configuration knowledge into SCM to maximize the value of the tool." This need resulted in the new GPO import functionality. They needed SCM to be easier to use, which lead to the new user-experience enhancements. They also needed SCM to be more flexible in regard to the underlying SQL database.

Setting up SCM remains a simple affair. While version 1 required its own instance of SQL Server Express for installation, version two lets you point to a local SQL Server or SQL Server Express. The beta also includes 10 pre-configured baselines. When you install the beta at this point, the installation will be automatically upgraded, while preserving any previous data (see Figure 1).

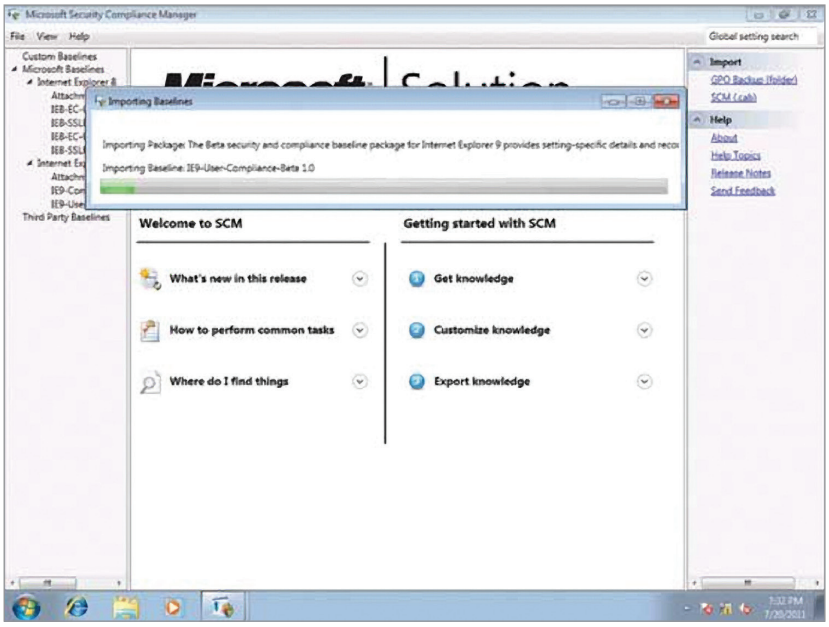

Figure 1. *When you run the SCM version 2 beta, it updates any earlier installs.*

Comprehensive Console

The welcome screen includes six informational areas you can expand for further links (see Figure 2).

The Baseline Library is on the left side of the main console. This lists all available baselines in a tree hierarchy, grouped by product. Any baselines you download are signed and you can't alter them. You have to create a copy to modify your own custom baselines. When you select a baseline, the middle pane displays information about your selection and the Actions pane on the right contains context-sensitive options for the selected object.

The current beta release contains new baselines as part of the package. If you need to download others, go to Tools | Check for Baselines, then select the ones you'd like and click Download. There's also an option to create copies of each baseline you're importing so you can start modifying

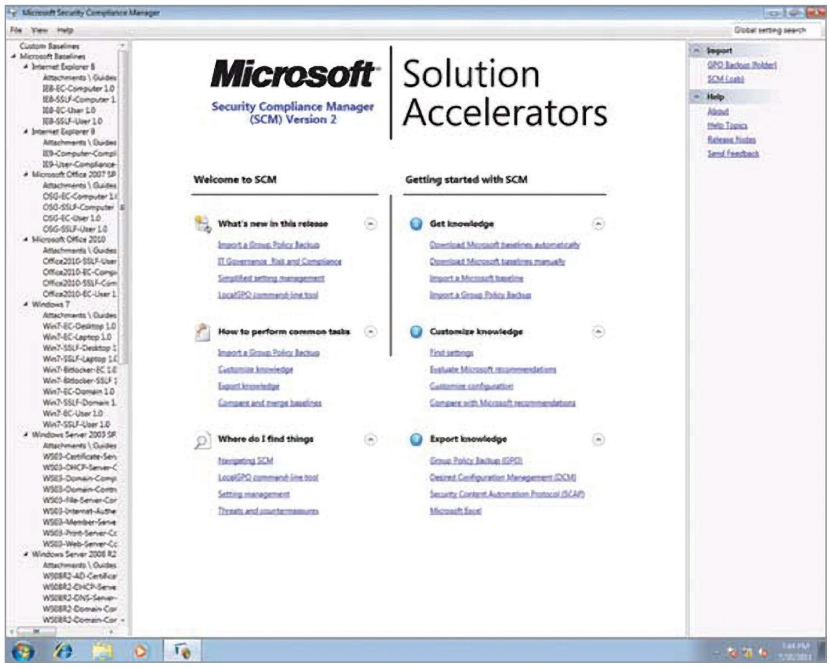

Figure 2. *The guides and additional information provided will help you get started in short order.*

them right away.

The main difference in using SCM version 2 compared to its predecessor is the new "settings grid." Each section is grouped by a horizontal bar you can expand or collapse. This makes it much easier to work with long lists of settings. Sigman points out that the settings grid layout was inspired by the look and feel of Windows Intune and is designed to minimize the amount of clicks necessary to modify settings.

Another new feature that will make the confusing world of security settings easier to navigate is the "breadcrumb bar." This works similar to Windows Explorer. You can navigate up and down the GPO hierarchy, as well as filter out unneeded information. To enable this, simply click Advanced View. Use the small buttons to navigate to the right level; click the red X to jump back to the top of the hierarchy (see Figure 3).

SCM is also a brilliant educational tool. Each best practice setting includes a comprehensive description that not only describes what the setting does, but also why you should use it, details about the threat and how this setting mitigates the risk.

Import Your GPOs

You can import current settings from your GPOs and compare these to the Microsoft recommended best practices. Start with a GPO backup that you would commonly create in the Group Policy Management Console. Take note of the folder to which the backup is saved. In SCM, select GPO Backup, browse to the GPO folder's Globally Unique Identifier and select a name for the GPO when it's imported.

SCM will preserve any ADM files and GP Preference files (those with non-security settings that SCM doesn't parse) you're storing with your GPO backups. It saves them in a subfolder within the user's public folder. When you export the baseline as a GPO again, it also restores all the associated files.

Birth of a Baseline

Sigman outlines the multiple steps involved in developing a baseline. It all starts with a group of subject-matter experts creating draft

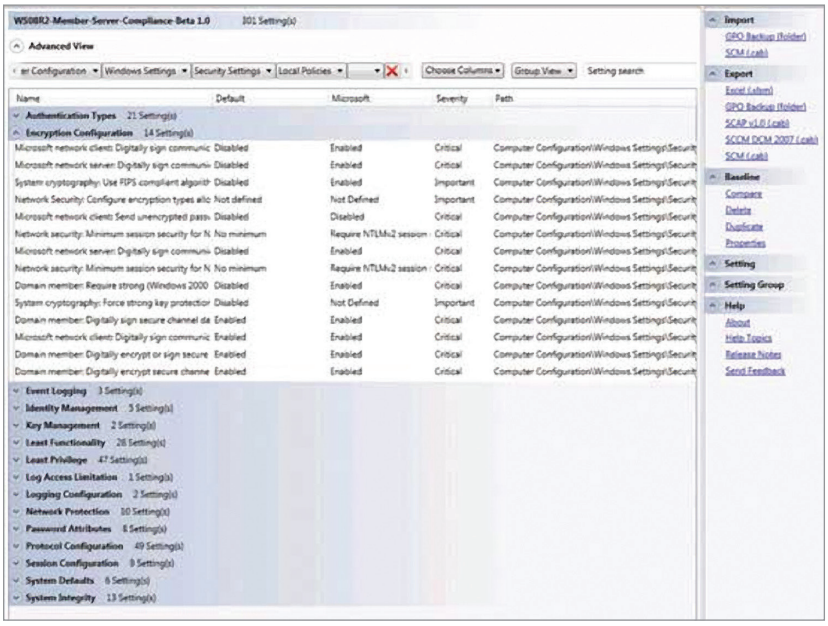

Figure 3. *Navigating your way through a multitude of settings is much easier with the breadcrumb bar.*

guidance. The product group within Microsoft then pores over this document. Then it releases a beta to the community.

In the case of SCM, the community includes agencies within the U.S. Department of Defense, Microsoft Consulting Services, NATO and governments around the world. After further testing, Microsoft creates the baseline. Then this baseline is maintained and updated with every new service pack, as well as changes in the threat landscape.

Add Settings

One common problem in the first version of SCM was extending a baseline with your own settings. There were "Setting Packs" that had all the settings for a product, instead of the ones for which Microsoft has best practices. Then you had to merge these into a baseline and remove any superfluous settings.

SCM version 2 makes this scenario much easier. There's a new Add Settings in the right side action pane. This brings up a dialog box that lets you select the product, indicate the group to which the new setting should be added, and choose from a list of available settings you can filter with the same breadcrumb buttons (see Figure 4).

These settings are displayed in the new Setting library that contains every setting SCM knows about and every product it understands (including Windows XP SP3 to Windows 7; Windows Server 2003 SP2 to Windows Server 2008 R2; Office 2007 to Office 2010; and Internet Explorer 7 to Internet Explorer 9). This library is maintained in the same manner as baselines. There are new settings added with each SP release--you can check your library version in the About dialog.

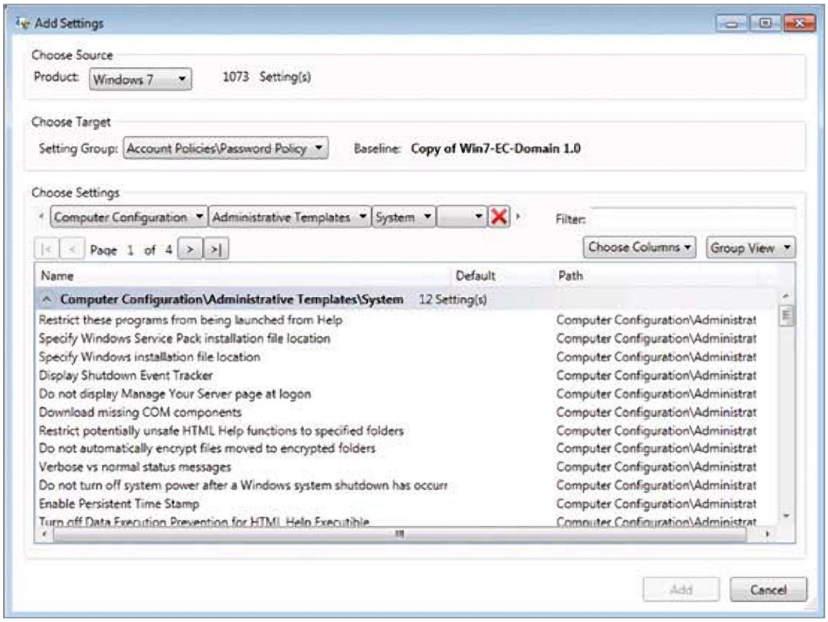

Figure 4. *It's easy to add settings to a baseline in SCM version 2.*

LocalGPO

There's a command-line tool called LocalGPO that lets you import and export GPOs directly from a computer's configuration. The installer is included in SCM, but it's installed separately. It runs on Windows XP and later.

SCM isn't dependent on Local GPO and Local GPO isn't dependent on SCM. Where LocalGPO shines is for non-domain joined systems and in conjunction with the Microsoft Deployment Toolkit.

You have to run the LocalGPO command line as an administrator. To export local settings from a reference computer simply enter:

```
1.LocalGPO.wsf /Path:c:\GPOBackup /
Export
```

And then to apply settings, type (The GUID in red text is the identification of the GPO you want to apply.):

```
1.LocalGPO.wsf /Path:c:\GPOBackup\
{12345678-9ABC-DEFG-1234-
56789ABCDEFG}
```

This process makes it relatively easy to enforce company policy on separate or workgroup computers where you can't rely on centralized Group Policy.

There's a new GPOPack option in LocalGPO that packs everything you need to apply a security baseline into one self-extracting file. You can apply this without installing LocalGPO first. The beauty of that is if you're using the MDT to set up client machines, you can simply add one line to a setup script to apply a GPO backup directly after installing an OS.

Naming a GPOPack is optional. It stops you from being able to import the GPO in the GPMC, but it makes it a lot easier to type in scripts because you don't have to type the long GUID. To use GPOPack, simply point your script to the GPOPack.wsf file generated by the GPOPack option like so:

```
1.C:\GPObackup\{12345678-9ABC-
DEFG-1234-56789ABCDEFG}\GPO-
Pack.wsf /path:C:\GPOBackups\
{12345678-9ABC-DEFG-1234-
56789ABCDEFG} /silent
```

You can also use LocalGPO to audit configuration drift on computers out of your domain, export their current settings, import those into SCM and compare them against your baseline.

EC and SSLF?

The baselines with the first SCM came in two flavors: EC for Enterprise Client and SSLF for Specialized Security, Limited Functionality. The new baselines for SCM version 2 adopt a four-level severity system. Each item is ranked so you can filter a baseline to select which settings you need:

- Critical settings have a high impact on system security. You should apply these settings to almost any system. Most settings in the former EC baselines will be included here.
- Important settings have significant impact on systems and data. Most settings with this rating match the older SSLF baselines.
- Optional settings have little or no security impact. You can ignore these when defining security baselines.
- None is the default security level for items that haven't been included in previous baselines. You can ignore these as well.

Sigman points out that the change in baselines is a natural progression. Businesses have become increasingly focused on IT governance, risk and compliance (GRC) initiatives. This has also lead to reorganizing baseline settings into GRC groupings for improved reporting.

Compare and Merge

You can use the Compare feature to view the difference between two baselines. The summary tab displays how many settings differ between baselines, and if there are any unique settings in either baseline. The Values tab tells you exactly which settings are different and how they're set in each baseline.

You can use the Merge feature to combine baselines as well. Start with the source baseline and select Merge in the actions pane. Then pick the target baseline. It shows you which items will change. You can deselect settings you don't want to change. It also shows you items only present in the source, items only present in the target and items in both baselines with identical settings. You can delete multiple settings from a baseline in one operation, which is a definitive improvement over the first version of SCM.

SCM can also create baselines in the Security Content Automation Protocol XML-based format, managed by the National Institute of Standards and Technology. For those working in U.S. government organizations, this is a much more robust version of United States Government Configuration Baselines.

You can't deny the thoroughness of Microsoft's security guidance. It has never been so easy to compare current settings with new recommendations and create new GPOs for locking down your systems. The new import GPO functionality, Local GPO enhancements and easier-to-use interface should move this tool out from relative obscurity. R

Paul Schnackenburg has been working in IT since the days of 286 computers. He works part time as an IT teacher as well as running his own business, Expert IT Solutions, on the Sunshine Coast of Australia. He has MCSE, MCT, MCTS and MCITP certifications and specializes in Windows Server, Hyper-V and Exchange solutions for businesses. Reach him at paul@expertitsolutions.com.au and follow his blog at TellITasITis.com.au.