

The importance of periodic security assessments

You wouldn't want to fly on a plane that hasn't had its regular safety inspection. Or take a road trip without checking your oil and tire inflation. Or miss an annual trip to the doctor — would you? Similarly, periodically assessing your IT security is an important part of your organization's preventive maintenance plan

Security is mostly an invisible attribute. We tend to set it up and then forget about it. But each of us has our blind spots, causing us to miss things. Our infrastructure changes over time, possibly opening it up to new vulnerabilities. And new methods of attack are invented daily, so what was secure yesterday may not be secure today.

Just as every car comes with a list of scheduled maintenance items, your IT organization should have a list of security features to audit on a periodic basis. You can do many of them yourself, but there's no substitute for having an independent expert occasionally check for your blind spots.

Why undertake periodic assessments?

There is a long list of reasons why you want to do periodic assessments, and an equally long list of reasons why you should. An increasing number of organizations are bound by governmental regulations that dictate what security measures you should have in place and how they should be audited. HIPAA, PCI, FISMA, Sarbanes-Oxley, and Gramm-Leach-Bliley all dictate how to secure different types of data and the systems that manage it. They also require regular security posture assessments, though they vary on specific requirements and time frames.

If you're not actually bound by any of these governmental regulations, you still might want to use them as resources to help guide your own IT security practices. ISO 27002 is a good generic security standard, and we discussed the value of FISMA to every organization in the Q4 2006 issue of *The Barking Seal*.

There are many benefits to doing periodic assessments beyond simply complying with government regulations. Undertaking regular assessments can help you to:

- *Find out whether your security has already been compromised. You might not know unless you look, and you will sleep better at night if you know.*
- *Stay on top of the latest security threats — with new attacks coming on the scene every day, you could become vulnerable even if nothing has changed since your last assessment!*
- *Make sure that your staff is being vigilant by maintaining a focus on IT security.*

- *Increase awareness and understanding of security issues throughout your company.*
- *Make smart security investments by prioritizing and focusing on the high-importance, high-payoff items.*
- *Demonstrate to your customers that security is important to you — this shows them that you care about them and their data.*

How to attain a Zen-like state of mind

What can you do to have the peace of mind that comes from diligently performing periodic security assessments? In this section, we'll briefly describe the overall categories that you need to pay attention to. Table 1 is your guide to the details: exactly what you need to look for and how often you need to do it. Change your oil every 5,000 miles. Use your password-cracking program quarterly to cut down on guessable passwords. Cut out the table and tack it to your wall. Your administrative role doesn't allow you to use scissors? Download a copy from www.atrust.com/audit-frequency-matrix.pdf and print it out.

PATHS OF ATTACK. Evaluate ways that your security can be compromised from the inside or outside, from both internal and external sources of attack. Auditing your firewall rules and watching logs is only part of the picture. Can hackers harvest information through a company directory posted on the Internet? If so, each of your employees is now a potential vector for social-engineering attacks. Internally, are you using secure tools with secure protocols, for example SSH/SFTP vs. Telnet/FTP? What services do your internal servers and workstations provide? Do they match up with your policies? And has someone snuck a wireless access point onto your network to make her life easier and give you a new security vulnerability?

SOFTWARE PATCH-LEVEL AND USE COMPLIANCE. Just how well have you been keeping up with patches? You've got a number of areas to pay attention to: operating systems on servers and workstations; infrastructure services such as email and DNS; enterprise applications including Web applications and databases; and then there are desktop productivity applications. What are your patch policies? Are you following them? And what is your lag time?

NETWORK SECURITY ARCHITECTURE.

Assess and re-assess how your network is defended at its perimeter, and how well it is segmented internally to limit the damage that can be caused by prying eyes or errant applications.

CATEGORY	AUDIT ACTIVITY	RECOMMENDED AUDIT FREQUENCY
Paths of Attack	Perform external vulnerability scan	Quarterly
	Perform external application penetration test	Annually
	Conduct analog line wardialing	Annually
	Validate web content filtering	Annually
	Review DMZ service/servers	Annually
Software Patch-Level and Use Compliance	Perform software inventory and patch comparison	Quarterly
	Review installed software and software license inventory	Annually
Network Security Architecture	Conduct rogue wireless access point scan	Quarterly
	Review firewall configuration review (includes reviewing ALL firewall rules)	Quarterly
	Evaluate internal network partitioning	Quarterly
	Capture and review raw packets	Annually
Infrastructure Best Practices Comparison	Conduct industry peer comparison	Annually
	Perform global IT architectural standards comparison	Annually
User Administrative Policy and Compliance	Perform social engineering study	Annually
	Conduct user tool usage and behavior vs. policy study	Annually
Encryption Usage and Key Handling	Review encryption policy compliance	Annually
	Review key revocation procedure	Annually
	Review keystore access management and inventory emergency keystore	Annually
Trust-Level Dependencies and Management	Review vendor and trusted partner access	Annually
	Validate external party access contracts and management approval for access	Annually
Virus Protection and Management	Inventory all systems vs. systems with current, active virus protection	Quarterly
	Confirm server and workstation virus signature updates	Quarterly
	Conduct email antivirus / anti-spam effectiveness study	Quarterly
Role/Function Segmentation and Access Management	Review termination list vs. access removed, new hires vs. access granted	Annually
	Validate role separation between {production, dev, ...} environments	Quarterly
	Validate role separation for account provisioning function	Annually
	Review elevated privilege accounts	Quarterly
	Review use of shared accounts (Administrator, root, Oracle, ...)	Quarterly
Remote Access	Validate demotion/management of production data sets process	Annually
	Validate remote access is only via approved methods	Quarterly
Password Policy and Use	Review remote access accounts	Quarterly
	Conduct brute-force password cracking	Quarterly
	Evaluate password strength policy	Annually
	Review use of multi-factor authentication	Annually
	Evaluate administrative/highly privileged password freshness and storage	Annually
Organizational and Security Measures	Test lost password reset process	Annually
	Validate change and configuration management process compliance	Quarterly
	Validate critical procedures documentation	Annually
	Inventory eDiscovery support tools	Annually
	Review IT security policy	Annually
	Validate management designation of security oversight responsibility	Annually
	Validate management acknowledgement of annual comprehensive IT security audit	Annually
	Review Information Security Program components	Annually
Review integration of IT security criteria with organization's purchasing process	Annually	
Physical Network and System Infrastructure	Conduct data center walkthrough	Daily
	Perform server inventory and reconciliation	Annually
	Review data center physical access control system and users with DC access	Quarterly
	Review access control system for all IT infrastructure (IDF, MDF, etc.)	Annually
	Conduct master physical key inventory/reconciliation	Annually
	Review console access and/or KVM concentrator access	Annually
	Check/maintain environmental management and monitoring	Monthly
Review media and retired equipment disposal practices	Annually	
Telecommunication Safeguards	Verify data backup procedures and perform data recovery test	Quarterly
	Conduct telco circuit inventory/reconciliation	Annually
	Evaluate clear-text vs. encrypted data sent externally	Annually
	Review voicemail, fax/eFax security	Annually
Level and Methods of Ongoing Vigilance	Review toll ("long distance") safeguards	Annually
	Conduct incident response drill	Annually
	Review intrusion detection/prevention system effectiveness (event detection/reporting)	Quarterly
	Review new IDS/IPS and system/network monitoring events	Daily
	Validate vulnerability announcement review process	Annually
	Review emerging technology evaluation process	Annually
	Manually review server, application, and device logs	Weekly
Inventory internal accessible hosts and services	Monthly	
Regulatory Compliance	Conduct formal review of organization's compliance with applicable regulatory standards	Annually*
	Test disaster recovery and/or business continuity plan	Semi-Annually

*Some standards, such as PCI DSS, may require more frequent review

These are example best practices for a periodic audit schedule — consult an information security professional about what's best for your site.

Audit both your device configurations and your update procedures and policies.

INFRASTRUCTURE BEST PRACTICES. If hackers were wolves and you were their prey, where would you want to be? Right in the middle of the pack. Hackers, like wolves, prey upon those who lag behind. Remember that security is not absolute, but relative, so it's a game of intelligently assessing risk. Compare your security infrastructure with your peers and keep your organization in line with industry best practices.

USER ADMINISTRATIVE POLICY AND COMPLIANCE. Writing down your security policies gives your employees guidance and you a benchmark with which to compare your performance. Do you have policies for what administrators, end users, and software developers can do? Measure your performance against your own standards.

ENCRYPTION USAGE AND KEY HANDLING. Use encryption to secure internal and external communication, including between layers of software. Make sure you're using it, and you're exercising proper control over encryption keys.

TRUST-LEVEL DEPENDENCIES AND MANAGEMENT. How well do you understand your business relationships and the trust you place in them? Do you trust your business partners, for example, so much that their security vulnerabilities can become yours? Or do you give them controlled, role-based access only to the applications they need?

VIRUS PROTECTION AND MANAGEMENT. Viruses can come from practically anywhere: from an employee's home laptop, from visiting a malicious Web site, from an infected USB drive. How well is your antivirus software working, and how prepared are you to stop viruses if your countermeasures fail?

ROLE/FUNCTION SEGMENTATION AND ACCESS MANAGEMENT. Segmenting user and administrator privileges by roles increases security by limiting the extent of damage that they can cause — either intentionally or by accident. Make sure that you implement role-based access and that privileges overlap only where you intend them to.

REMOTE ACCESS. By what means do you allow remote employees, partners, and contractors to access your internal resources? Are they segmented by role? Are the communication channels secure? Can security problems on their remote workstations become yours? Brush up on the topic by reading 'Safe and secure remote access' in the Q4 2007 issue of *The Barking Seal*.

PASSWORD POLICY AND USE. Have a policy that dictates how complex user passwords must be and when users are forced to change them. Do you have such a policy in place? Is it automatically enforced? And are you auditing it periodically by running password-cracking software?

ORGANIZATIONAL AND SECURITY MEASURES. A well-organized security staff is more efficient and more effective

at everything from patching systems in a timely manner to responding appropriately to suspected incidents. Assess how well your organization works, how well your procedures are documented, and how well your staff members keep up to date with their field.

PHYSICAL NETWORK AND SYSTEM INFRASTRUCTURE SECURITY. All of your security measures are for naught if someone can walk into your datacenter and walk off with a disk drive, or enter a closet and watch your network. Are your physical security devices adequate? (Hint, most card-key access systems installed before 2005 are not.) Are they in place and working? Be sure nobody is propping open a switching closet with a brick or with tape over the striker plate. Backups are also part of your security strategy; verify that they work by actually restoring your data.

TELECOMMUNICATIONS SAFEGUARDS. Your telecommunications infrastructure offers routes of attack from network snooping to social engineering. If you have a dedicated network connecting multiple sites, is its traffic encrypted and secure from prying eyes along its route? Can a casual passer-by press a 'voice mail' button on an employee phone and gain access to company secrets?

LEVEL AND METHODS OF ONGOING VIGILANCE. You can boost security and minimize risk not only by following the recommendations in this article. You can also educate non-security staff members with lunch-and-learn sessions that communicate the importance of good passwords, not falling prey to social-engineering attacks, and not opening attachments from people they don't know.

REGULATORY COMPLIANCE. Back to the beginning. You may be bound by governmental regulations dictating how you secure and manage your business data and your customer information. These regulations sometimes dictate how you respond to an incident; California, for example, regulates how and when you must inform your customers if a breach may have compromised the security of their personal information. If you have, or are required to have, a disaster recovery plan, test it to make sure that it performs in the event of a real disaster. Finally, be sure of which regulations affect you and make sure that you're in compliance.

Checking checks & balances

We've introduced a comprehensive list of areas that should be part of your regular security assessment schedule. Table 1 condenses this information and gives recommendations for how often to address each of them.

Think about security like your finance department thinks about money. Just as your accounting system has checks and balances to help prevent fraud and embezzlement, your IT security policies need to have checks and balances to help prevent intentional and unintentional security compromises. You can handle periodic security assessments internally so long as you have a good checklist and a good set of checks and balances. Having an independent

third party do some of your security assessments is your check and balance that your checks and balances themselves are in place and are, in fact, working. ■

This article was reprinted from the Q4 2008 issue of The Barking Seal, a publication of Applied Trust. You can subscribe to The Barking Seal online at <http://www.appliedtrust.com/barkingseal>. “Applied Trust” and the “Seal on a Rock” Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.