ENJOY SAFER TECHNOLOGY®

SECURITY AUDITS: WHAT IS YOUR GAME PLAN?

Security audits: what is your game plan?

By Michael Aguilar, Business Product Technical Lead, ESET North America

There's a lot of confusion about how to perform a security audit and what it entails. Some people think that in order to have a secure infrastructure, all you need to do is install antivirus software and you're done. Others believe that limiting access to everything is the best approach.

But what is right for you? With the varying size of businesses and their staffs, this can be either a walk in the park or a long trip down a winding road. It really depends on the needs of the business, what you do, and what needs to be protected. The guidance given here is taken from my numerous interactions with clients of all sizes, so pick, choose, and use what is right for you.

What is a security audit?

A security audit (sometimes mistakenly called an assessment) is a top-down look at your business and all aspects of it. This will include technical aspects like computing systems as well as nontechnical items like policies and procedures. This is a continuous process, not something that will be completed once. Every day, new threats and problems arise, so you must stay vigilant and take a look at these items regularly:

Technical aspects

- Vulnerability scans
- Access control lists
- User permissions and rights
- Disaster recovery software/hardware analysis and testing
- Locking and badging systems and software
- Password/lockout policies

Nontechnical aspects

- Policies and procedures
- Locking systems
- Network and application design
- Checking your business against various compliance laws if in retail, finance, or medical
    - ▻ HIPAA
    - ▻ PCI-DSS
- Building security and layout

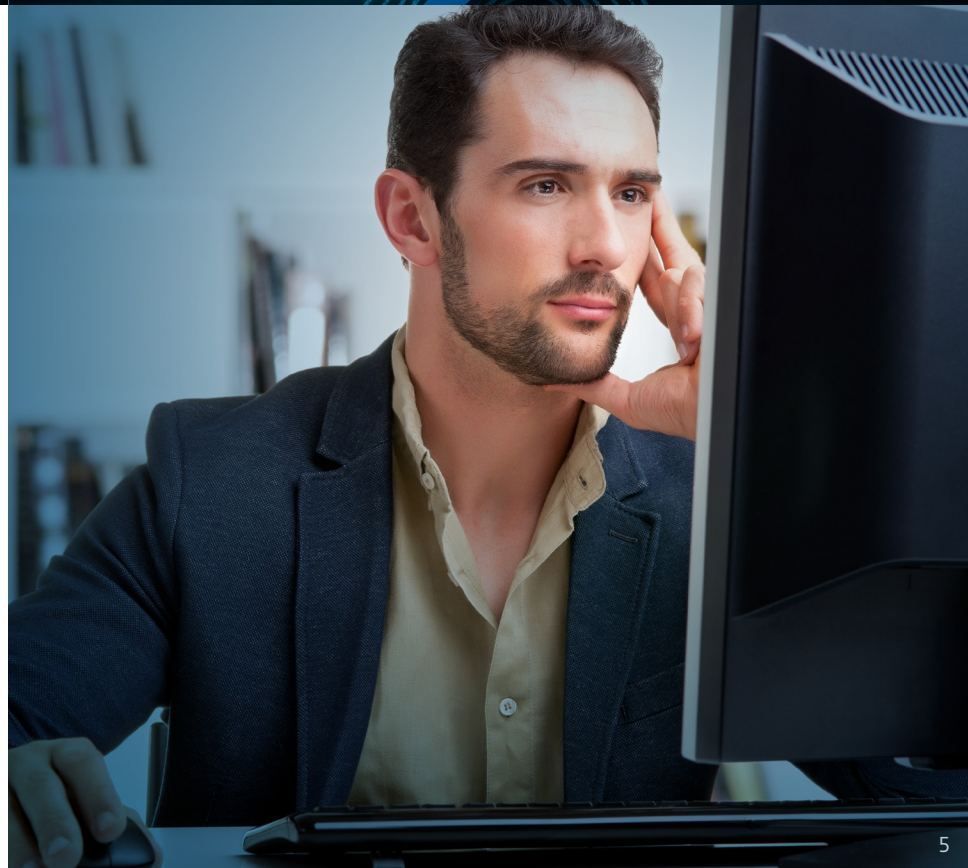
Now what? Your game plan

A security audit has many aspects and the process may seem daunting. Depending on the business and how long it has been since your last security audit, it may be. If you have never done this before, planning and assembling an initial plan of attack is going to be one of the longest aspects. However, once completed, you can use that as a framework for the next security audit.

Note: This is a framework, not a canon. You will find that on the next audit, you may be adding or subtracting items to check. This is normal and the framework is meant to be revisited often. Having a game plan and sticking to it is key; you will not want to keep adding items once you have decided on an initial framework and extending the time needed to complete tasks.

Vulnerability scans and pen testing

Depending on your staff and resources, you may be able to evaluate computing resources by yourself. Determine how you would like to test your infrastructure; however, I recommend you start with a vulnerability scan.



To get started, you will need to choose a vulnerability scanner. There are many choices, from trusted and widely used scanners like *Nessus* and *Nexpose* to open-source alternatives like *OpenVAS*. The results of these scans will be somewhat lengthy and will need confirmation that the threat or vulnerability actually exists. Results can be ported over to an item like *Metasploit* for a "full connect" test to validate if the threat is really there and able to be exploited. WARNING: Do not attempt a "full connect" scan unless items are backed up and staff is aware, as you may disrupt normal business operations.

After the scan, my preference is to conduct a complete pen test of a site. A good pen test (aka penetration testing) will include multiple aspects, such as items found in vulnerability scans, locking mechanisms, social engineering testing and prevention, password policies (trust me, if they are good, they will find yours out for you), and application analysis, depending on how in-depth the test is. A good test also relies on the testers' skill set. Some call a simple Nessus scan and report a "pen test." This is not correct. There are three flavors of pen testing or analysis that can occur:

- **White Box Testing**—This type of testing is normally conducted by internal staff. This test replicates an insider threat where intensive knowledge of the infrastructure is available, such as layout, passwords, and various aspects of the business. This is where having a decent IT staff helps, as staff members can assist in these kinds of tests—granted they know the technologies to use and can interpret results. Many times, an insider threat is the cause of a data breach.

- **Gray Box Testing**—This is based on limited knowledge of the infrastructure or test items. You have some idea of items running and know limited infrastructure or test subject details, but not everything. Your team will have to do some extra work in testing items, but once engaged, they should be able to help find weaknesses in systems that a white box test might have missed.

- **Red Box Testing (my favorite)**—This form of testing pretends you are a complete outsider. You are the attacker. You have no knowledge of the infrastructure or business—and you need to start from square one. This may be one of the truer tests of infrastructure and technologies, as it recreates simulated outsider attacks, the kind that you would encounter in the wild. Depending on preferences and needs, this can include items like testing against DoS (denial of service) and DDoS (distributed denial of service) attacks.

Now that you have the results from both the vulnerability assessment and a pen test, it's time to start placing controls to mitigate located risks. Controls will vary from site to site and will depend on what vulnerabilities were located, but they can include things like:

- Updating antivirus software
- Placing correct locking systems on critical infrastructure
- Changing password and system lockout policies
- Refining user permissions
- Ensuring that only authorized staff has access to sensitive areas

I also strongly recommend testing backup functionality and disaster recovery scenarios at this phase to ensure that you are prepared in case of disaster, threat, or other scenarios that can bring business to a grinding halt. (*Learn six ways for your business to back up data*.)

Nontechnical aspects

You have scanned, validated, and corrected any issues regarding your computer infrastructure. Now it is time to take a look at some exciting things … like paperwork! Before you get too excited, know that this is a critical aspect that needs to be reviewed. There are many nontechnical-based issues that can make or break your business, and having good policies and procedures is one of those aspects.

Depending on the size of your company, you may need only a quick review of existing document(s), or a thorough review of multiple documents to ensure you're free from liability in case of a data breach or other event. Having all this in order and reviewing it a few times will help you locate flaws in your business model and operations.

Your business model also needs frequent review against any compliance laws that may surround it. If you charge people using any major credit card brands, you will need to ensure that you are PCI-DSS compliant. If you handle medical records or other ePHI (electronic protected health information), make sure that you are *HIPAA compliant*. Laws vary from state to state, with some audits conducted annually, others biannually. Make sure that you are following the correct framework your state has regarding compliance.

Lastly, test your physical locking systems and floor plan layout. While these may seem obvious (of course I lock my doors!), you may be surprised. You may think that a standard door lock will keep people out of your business. Not true. If someone wants in, they can bypass that lock. If they would like

to do it quietly (not smashing the lock), simple door locks are not hard to bypass with a $13 kit of lock picks, rakes, and tension wrenches. You would be surprised how many locking systems can be picked with that small kit.

Having solid, hard-to-bypass locks on doors and critical infrastructure will reduce the threat of theft and unauthorized access by volumes. Your floor plan is also worth reviewing. You may discover just how easy it is to "tailgate" into a restricted area. Tailgating is the act of following someone who is authorized with a badge or other authentication method into an area without having those permissions yourself. Piggybacking, like tailgating, is getting access to that secured area, but with the knowledge of the person you are following. So they let you in. Both of these attacks can be prevented with the proper floor plan and locking systems, such as the addition of "man traps" in sensitive areas that need to be restricted.

A security audit can be a vast undertaking, but it serves as a crucial framework for keeping your business safe. It can be reused for recurring audits, making additions and subtractions as necessary. If the site is bound by HIPAA or PCI-DSS compliance, ensure that those portions are met when testing the whole infrastructure. You'll be glad you did.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®