SPONSORED

7 Ways to Prepare for a Cybersecurity Audit

Start by counting your devices, then move onto these other key steps.

shutterstock

Data breaches, phishing attacks, information disclosure – the Internet can be a scary place. Conducting a cybersecurity audit (or getting a third-party assessment) is a great way to understand your organization's cybersecurity posture. But, like preparing any exam or review, getting ready for a cybersecurity audit can be intimidating. While every security assessment will be a bit different, here are seven ways you can prepare for your next cybersecurity audit.

#1: Count your devices

How can you protect something if you aren't aware it's out there? The first step for any good security plan is to count every device that's connected to your network. Be sure to include not just desktops and laptops, but also cell phones, printers, or security systems which are integrated into your network layout. Creating a device inventory can be challenging at first, but once you're done, you'll have a real picture of what you're responsible for securing. Be sure to maintain your inventory by updating it when new devices are added or removed, so there are no surprises during your review.

#2: Check what's running

Once you've completed a device inventory, it's time to do the same for software and firmware applications. Find out what exactly is running on each machine in your network, and what actually *needs*to run to complete business functions. You can use your device inventory to create a limited, approved list of software that's well, approved to run (this is called "application whitelisting"). Application whitelisting can prevent users from downloading and using software outside of what's necessary for business applications.

#3: Apply the principle of least privilege

The "Principle of Least Privilege" is a valuable computer security concept. Essentially, it promotes minimal user profile privileges (as opposed to root or admin-level access), based on the user's role or job functions. Adjusting user privileges may feel limiting at first, but it goes a long way toward preventing the downloading and installation of unwanted applications. It also comes into play when a machine has been compromised. If a cyber criminal gains unauthorized access to a machine with limited privileges, they'll be able to do much less damage than if the compromised system had admin-level abilities.

#4: Implement secure configurations

Operating systems, browsers, and even printers all come with various settings which should be configured with security in mind. In fact, a single operating system can have hundreds of settings to choose from, covering things like password length requirements, which ports are open, and when users are allowed to log on. The CIS Benchmarks, consensus-based secure configuration standards for over 150 different technologies, are available as free PDF downloads.

#5: Patch, patch, patch!

As new vulnerabilities are discovered, vendors release updates (or "patches") to close security gaps and make applications more secure. Cyber criminals look for easy wins and low-hanging fruit, so it's essential to apply patches as they are released in order to keep your systems secure. A fully-patched network will impress any auditor. When an application reaches end-of-support (sometimes called end-of-life), the vendor stops releasing patches. That's when you know it's time to upgrade to newer version or find alternative, supported software.

#6: Develop an incident response plan

What happens if there is a data breach in your organization? Do employees know what to do if they spot (or worse, fall prey to) a phishing email? Surprise your auditor by showing you are prepared for the eventual attack on your systems. Components of incident response planning include conducting a risk assessment, penetration testing, and training employees. You may need to draft written policies to instruct employees on what to do in various situations, for example, if they receive a suspicious email, accidentally download a malicious file, or spot an insider threat.

 # 7: Utilize available resources

Don't let the idea of a cybersecurity audit overwhelm you. Take advantage of tools that can help make this process easier from beginning to end. Memberships like CIS SecureSuite provide an array of resources that can help you scan systems and produce a report on a system's compliance, quickly implement secure configurations, and connect with other cybersecurity experts.

Learn more about CIS SecureSuite Membership

Taking these seven steps before your next audit will not just improve your network security, but demonstrate preparedness for future cyber threats. While some of these steps may take time to implement, the security payoff is worth it – not to mention passing your assessment with flying colors!