An IT Security Audit Offers both Insurance and Improved Productivity

Every business runs on information, which is why Pacific Crest Group includes IT support as part of our client service. System integration has become an inescapable part of back office operations. While Pacific Crest Group specializes in accounting, billing administration, and human resources support, many of the processes and procedures we build for clients have an IT component. Bookkeeping, for example, has become a computer-intensive process and software tools such as QuickBooks make our job a lot easier, and make it easier for our clients to make sense of their operational figures in order to run their businesses more efficiently.

A lot of our initial conversations with IT client prospects center on disaster recovery– what is the worst case scenario that could bring your network down? Is it a server crash? Internet failure? Multiple workstations failing at the same time? In these cases, we spend a lot of time laying out which applications and data services are critical to day-to-day operations. Then we assess the current computer environment to determine the best strategies in the event of a disaster. We find this approach is a good initial exercise since it helps the client understand the real value of their data, where their points of vulnerability are, and how to secure that data.

When we engage with a new client to provide IT support, we usually start with a security audit, which not only allows us to assess data vulnerability, but also look for potential weaknesses and points of failure within your computer network. Network security is primarily concerned with protecting your data assets, but it goes beyond simply making sure you are using anti-malware precautions and locking out cyber-intruders.

First, you have to inventory what's on your computer network. It's amazing how many times the audit process turns up surprises, like an unauthorized laptop of a forgotten printer or storage device that could pose a security problem. You also need to inventory the software running on your business machines, especially the operating systems. Then there is a review of patch management, making sure that the updates and software patches applied to those machines is up to date. Perhaps most importantly, an audit will reveal where your business-critical data resides.

Once you have created an inventory of your network, you can start thinking about taking the next steps to actually secure the network and improve performance. The most common security problems include:

· Unnecessary open ports. A network audit helps you identify all the open ports on the computer network devices, so you can close them against a potential external attack.

· Shared files and folders. Shared network devices are more prone to attack from viruses, malware, and unscrupulous users, so you may need to change permission settings to secure access.

· Unauthorized and unknown users. An audit will reveal old and unused accounts, old passwords, and other holes that could be used for an attack. If you uncover an unknown user, it may be evidence of an attack that has already happened, and you may need to do some forensic work to uncover any potential damage.

· Unnecessary running services. Any service that runs on a network device leaves that device open to attack. A security audit will determine which services are unneeded and can be turned off.

· Startup applications. Applications that automatically run when a workstation or network device starts can indicate an attack. Of course, many of these applications are necessary, but the mystery startup applications could be viruses and need to be removed.

Conducting a security audit is a solid first step to securing your computer data, and improving performance. Removing unnecessary applications and tuning your computer systems will increase response time and productivity.

Also remember that a security audit is not a one-time event. Computer networks are constantly changing, and that means new security threats are introduced all the time with changes in hardware and software. You need to be watchful that your patch management is up to date, and that you use regular security scans to detect any potential threats or infections. Regular audits will help eliminate any unpleasant surprises and keep your business-critical data safe.