Protecting Your Tax Office

Practical Steps You Can Take To Ensure
The Security Of Your Tax Office

SIGMA TAX PRO

Powering Tax Professionals

Ian Gardner, Sigma Tax Pro LLC.

Contents

Why does this matter to me?

Cyber security can seem like a daunting task, and it can also seem like something that doesn't really affect you. However, in the modern age of interconnectedness, every system is a potential target.

As you go through this eBook, continually think to yourself how this can affect your office. Think about the incredible amount of personal data that goes into creating tax returns, and how much of that is stored on your computer. How would you feel if any of that information was compromised, and what would that do to your reputation?

While some hackers target larger systems with greater payoffs, smaller networks are also a target due to the fact that they are usually not as well protected, and can yield a large amount of useful data. If a hacker can gain access to a few small systems, it can be as fruitful as gaining access to one larger network. The following pages will outline steps you can take, as well as general information about cyber security that should act as a good first step for securing your office.

Using A Layered Defense

Technical Jargon...

Employ multiple complementary approaches to security enforcement at various points in the network, therefore removing single points of security failure.

Decoding the technical jargon...

Start by putting passwords on everything. Passwords are a great first line of defense against intruders on your network. When setting it up, be sure that the password is not something easily guessed, or the default for the router.

Anti-virus software is a good additional layer of security as well, but it's important to ensure it is active and up to date. Not updating the software means you are not protected against the most recent threats, and they pop up almost daily.

You'll also want to implement firewalls on computers, to make sure that your staff are only visiting approved sights and not accidentally endangering your entire network.

These are all easy layers to implement to ensure that even if one is breached, there are still additional fail-safes in place to protect your information.

Incorporate People and Processes in Network Security Planning

This one goes a little deeper than the first step. Basically what you want to do at this point is assign roles to individuals within your organization. For example, some team members may be allowed full admin privileges, while other may be limited to only data entry. Not only do you want to be aware of who has access to your information, but equally important is how much information they can access one they are on the network.

When you are evaluating your software options for various office tasks, make sure it provides the option to assign user roles, and that you as the admin are able to edit those permissions accordingly. Sometimes the default settings will not fit your specific situations and the ability to create custom permission settings will greatly help you limit the amount of information that flows our of your office and into the hands of fraudsters.

Technical Jargon...

Employing effective processes, such as security policies, security awareness training and policy enforcement, makes your program stronger. Having the people who use the network (employees, partners and even customers) understand and adhere to these security policies is critical.

Clearly Define Security Zones and User Roles

Technical Jargon...

Use firewall, filter and access control capabilities to enforce network access policies between these zones using the least privileged concept. Require strong passwords to prevent guessing and/or machine cracking attacks, as well as other strong forms of authentication.

Basically this one entails making sure that the roles you just created for your team members are actually created within the software and enforced. It does no good to tell someone they are data entry only, but not updating their user permissions to reflect that and letting them continue having full access to your network.

This one may seem silly but it it surprising how many offices grant their entire staff full access, even seasonal employees, without knowing it. If your software has the ability to limit information, make sure you are using it. It is not just another feature mentioned by a sales person, but rather a valuable security measure.

Maintain The Integrity of Your Network, Servers, and Clients

Keep your systems updated! This one is easy to forget. Once you've put your layers of protection into place you need to make sure you are keeping them up to date, otherwise they become useless. This also includes deactivating user logins if a team member leaves the organization, because if they still have access to your systems and maybe did not leave on the best terms, they have the potential to do damage.

There are companies who's sole purpose is preventative IT maintenance. They make sure everything is up to date and backed up, so if anything were to happen, your office would be able to continue functioning. This is traditionally known as "managed services" and may seen like an unnecessary expense at first, but like car insurance, you don't need it until you really need it, and by then it's too late. It's much more of an investment in the security of your office, which can be marketed as an advantage of your practice of that of your competitor.

Technical Jargon...

The operating system of every network device and element management system should be hardened against attack by disabling unused services. Patches should be applied as soon as they become available, and system software should be regularly tested for viruses, worms and spyware.

Control Device Network Admission Through Endpoint Compliance

This one is simple, but often overlooked. With the rise of smart phones and tablets and mobile access to all programs, ensure you have control of who can access certain information remotely. Think to yourself, is there a way my employees can access my software, and thus sensitive taxpayer information, remotely? It is difficult to ensure the security of these devices at all times, especially since they are for personal use as well as business.

An easy way to get a handle on this is to create a complete list of everyone on your network, and then begin to list their individual permissions to pinpoint weaknesses in your defense, and allow you to be proactive against threats.

Technical Jargon...

Account for all user device types -- wired and wireless. Don't forget devices such as smart phones and handhelds, which can store significant intellectual property and are easier for employees to misplace or have stolen.

Protect The Network Management Information

Somewhere along the way, as your system was being built, a map was created that showed exactly how your office is setup. This is something that you, as the business owner, need to be aware of and protect. This is basically a roadmap for how to get into your system and how to break down your defenses. Only admin users and network engineers should have access to this information. If you hired an IT professional and they did not create or provide you with this map, you may want to consider having another IT professional or Managed Services company come in to look everything over and recreate the structure with more security.

Often, IT duties are handled by a friend or relative, since it's a one time process and doesn't seem hard to compete. However, this is not good enough in the age of cyber security, and without having a real map, plans, and redundancy systems in place, you're leaving yourself wide open to attack.

Technical Jargon...

Ensure that virtual LANs (VLAN) and other security mechanisms (IPsec, SNMPv3, SSH, TLS) are used to protect network devices and element management systems so only authorized personnel have access. Establish a backup process for device configurations, and implement a change management process for tracking.

Protect User Information

Technical Jargon...

WLAN/Wi-Fi or Wireless Mesh communications should use VPNs or 802.11i with Temporal Key Integrity Protocol for security purposes. VLANs should separate traffic between departments within the same network and separate regular users from guests.

Do not give your Wi-Fi password out to everyone that asks for it. When you do this, you are handing that individual access to your network. Optimally, you can create different access points for each department, so you can continue to compartmentalize and block access to certain sites. For example, your marketing department may need access to social media sites like Facebook, while your data entry team does not.

At a minimum, you can create two distinct Wi-Fi networks, one for your team members, and another separate access point for guests in the office.

Both of these passwords should be updated occasionally, since that will allow you to have a fresh start on the individuals with access to each network.

Gain Awareness of Your Network Traffic

Technical Jargon...

Gain awareness of your network traffic, threats and vulnerabilities for each security zone, presuming both internal and external threats. Use anti spoofing, bogon blocking and denial-of-service prevention capabilities at security zone perimeters to block invalid traffic.

Who is managing your firewalls, or your network? Setting up this infrastructure is just step one. Continuing to manage and monitor your network is an ongoing process that must be functioning constantly. Any IT professional should be generating monthly reports for their clients to show them exactly where the threats are coming from, who is using their network, and how team members are spending their time.

This also falls under the umbrella of keeping yourself up to date on new security threats and proactively blocking possible intruders or fraudsters.

Log, Correlate, and Manage Security and Audit Event Information

Make sure you're keeping a log of events that occur throughout the year. This will allow you to look back and attempt to correlate when attacks are occurring and ensure that you are able to increase security around those times. For example, if you are noticing a majority of threats are occurring during November and December, then limit the number of users who are able to access your system during that time. This is just one more layer of security you can add to protect your network.

This information is also valuable because you can see what type of attacks are happening and take steps to protect from those specific events.

It is standard practice for an IT professional or Managed Services company to provide these reports, as well as help you understand what they mean and begin to formulate a defensive strategy.

Technical Jargon...

Aggregate and standardize security event information to provide a high-level consolidated view of security events on your network. This allows correlation of distributed attacks and a network wide awareness of security status and threat activity.

Sigma Tax Pro has developed the first Managed Service program designed specifically for Tax Professionals!

Why Managed Services?

Most modern businesses are using managed service plans to solve their IT needs. It is far more cost effective to pay a fixed monthly or annual fee and feel secure that your business is running smoothly. Managed service plans include line of business software, email, backup/cloud storage, Microsoft Office and virtual servers among other items. Most importantly, businesses can eliminate the need for an in-house IT department by contracting with a managed services provider.

Imagine being able to access your tax office from any device anywhere in the world!

Sigma's virtual server solutions allow your tax office to host its professional tax software on a secure server with 99.9% uptime. You and your team can login from your laptop, tablet or smartphone and enjoy full access to your tax software any time of day. You'll never have to worry about your desktop crashing, power outages or your IT guy calling out sick again!

Our managed service plans include virtual servers and other essential IT solutions that will save you time, money and effort so that next tax season will be your most successful one yet. Whether your office takes advantage of bank products or prefers collecting prep fees up front, we offer a plan to fit your business.