Security Considerations for Accounting Firms: Is Your Client Data Safe?

Right Networks®

By law, we have a duty to protect our client data. It's important that we understand our physical security risks and know what risk points exist for exposure of client data. It's our responsibility to create and enforce a plan to keep key systems properly updated and staff current on security best practices.

The truth is a hacker can find out everything they need to know about your domain, spam service, website and mail server just through passive and publicly-available information lookups. And, if you happen to be hosting both your website and mail server from your office, this tells a hacker exactly what IP range to attack.

So, how do you keep your firm protected? Consider the following:

Server Security

If your servers are located in your office, legislation, like the *Massachusetts 201 CMR 17*, requires that they be behind a secure locked door with restricted access and that the server cases, cabinets, drive chassis and server console screen be locked. If your servers are hosted off site at a data center, it's best to ensure that all the physical security requirements are being met based on your needs.

Confidential Data

In theory, accounting firms securely shred everything. In practice, someone could likely find a wealth of information they shouldn't be able to access just by digging into a dumpster. Does your firm actively enforce a confidential data policy that addresses paper copies of confidential data?

Password Security

It is important to educate your firm on the importance of using secure passwords and keeping them secure by not writing them down, telling them to anyone or using the "remember my password" checkbox at the login prompt. Did you know that adding just one capital letter and one asterisk can change the processing time to crack a 9-character password from a matter of hours to about a year?

We recommend enforcing a password policy that includes forced password changes every 90 days with specific complexity requirements (a minimum of 8 characters with a combination of lowercase, uppercase, numbers and symbols). Also, here's a helpful site to find out how many days (or seconds) it would take to crack a given password.

Microsoft Patches

Staying up-to-date with Microsoft patches is a critical step to ensuring your firm's security. We recommend using automated patch management like GFI LANguard or Windows Server Update Services (WSUS), which is free. All of the Microsoft server vulnerabilities and their related patches (sometimes called "fixes") are published on its Security Advisories Archive site. This serves as a great inventory of information on how to protect your firm while providing hackers a roadmap for exactly how to break into your unpatched servers. Server security is only as good as its latest application of patches.

Website

Another thing to consider is what information you post on your website. Accounting firms love to publish everyone's name, phone number and e-mail address, which is helpful for the general public, but makes it one step easier for someone to get into your network. If you find this concerning, consider including a contact number and generic e-mail address for each department to add one more layer of protection for your firm.

Voicemail System

Secure passwords are important here too. You don't want someone calling your office after hours, figuring out how to get a password prompt and then gaining access to someone's voicemail because the employee used something like 1111, 1234 or 0000 as his or her password. This is another reason not to post everyone's number online.

ISP Router

The Internet Service Provider's (ISP) "managed router" is one of the most overlooked pieces of the network. It's a nondescript box in the closet with blinking lights that few people understand. Most firms assume that because the ISP set it up, it must be configured correctly. Not true. We've seen default passwords used on ISP routers many times. MANY times. Some of these routers have built-in sniffing tools to allow you to watch all traffic going in and out. This information is very helpful to a hacker. Request that your ISP change the default login password on your router.

Firewall

When is the last time your firewall was updated? Firewalls are found both in the server room and as a piece of software on your PC. We recommend using Fortinet or Cisco for network hardware-based firewalls. Just as any other component of technology needs management, hardware firewalls also need to be kept up-to-date. Your PC-based firewalls found on desktops, laptops and home PCs are generally updated whenever the Windows Updates are installed.

We also recommend using Intrusion Detection/Prevention (IDS/IPS) in addition to firewalls to protect your firm. Where firewalls passively block known attacks, IDS/IPS solutions are proactive in nature and will provide reporting on the number and types of attacks that are attempted. This service is included with Fortinet firewalls and is another reason why we like this manufacturer. There are numerous options out there, including free services like Symantec DeepSight and Snort. Other options include McAfee, VeriSign, and IBM ISS. This provides an extra layer of protection, as a hacker would have to get through your firewall and IDS/IPS system before getting to your client data.

Wireless Access

WPA2 (Wi-Fi Protected Access) is mandatory for all new devices considered "Wi-Fi certified" by the Wi-Fi Alliance. Using Wired Equivalent Privacy (WEP) is unsecure and opens up the risk of key loggers and Wi-Fi piggybacking. If a hacker were able to get onto your wireless network, they would be able to dig deeper by scanning and mapping your network from the inside.

Additionally, many firms are now creating an additional DMZ wireless network that has absolutely no access to internal servers and only connects to the internet. This adds another layer of protection for portable electronics, guest access, and vendors that need access to the internet without the ability to see your internal infrastructure.

Bring Your Own Device (BYOD)

With the rise of Bring Your Own Device (BYOD) in the workplace, portable handheld computers are everywhere, and they can enter your network by both employees and non-employees. It is important that you only allow "non-hacked" devices onto your network and enforce a password on your wireless access, as mentioned above.

Hacked devices mean the devices have changed from the manufacturer's settings and can be as vulnerable as an unpatched server. These devices can be used to launch attacks onto your network. These devices also can connect to company email and store files and attachments on these devices.

We recommend mandating that all phones that connect to company information require a screen-locking password. The implications of company owned data on users' personal devices must be considered. If an employee leaves the organization or loses their device, steps must be taken to neutralize the company data located on the personal device. In situations like this, it's useful to have access to BYOD services that allow firm administrative staff to selectively remove company data from personally owned user devices. Alternatively, prior to accessing company data or email, users need to give consent to have their entire personal device wiped, should they leave the company or lose the device.

Remote Access

Currently, the convenience of anytime, anywhere access to data poses new security threats that firms need to consider and address. Our duty to keep client data secure now extends far beyond the walls of the office and staff in the field to our employees' homes and cell phones as well. It's a good idea to develop a written policy for remote access and transit with things like remote wipe, mobile phone lock, Wi-Fi protocol and password complexity enforcement. Centralized management of anti-virus and personal firewalls is also key to making sure your firm is adequately protected on all fronts.

Encryption

Most states have breach notification laws and nearly all of them waive the requirement for notification where data has been encrypted. Whole disk and USB-stick encryption are the two most common places where encryption can be used. Imagine all the free press you could get just by having an auditor lose their USB-memory stick.

Another way to avoid data loss without using device or PC encryption is by using remote access technologies such as Citrix/Terminal Services. In the remote computing environments, data is rarely stored on the device, rather it is left on the server where it can be controlled and is generally less likely to be left on a train or stolen from your backseat.

We also recommend using remote laptop security tools like Xtool MobileSecurity and Absolute Software Computrace LoJack, which come with a laptop tracker and recovery guarantee to help protect your firm. Xtool MobileSecurity also includes features like encrypted disk and remote delete, which are helpful in such situations as well. We recommend using IronKey or PGP to encrypt your USB sticks and PGP or Windows Vista BitLocker for whole disk encryption.

Advanced Email Security Tools

Whether you use an on-premise device, or a third-party smart host, the need for a successful and efficient email spam filter has only increased. While users may get less spam in their inbox than in previous years, the threat of an email induced networks attack is still great. Unfortunately, phishing and spear phishing via email still have proven to be effective ways for hackers to compromise networks. Smart email hosts, like Mimecast, can scan incoming links and attachments to secure your users from malicious email messages.

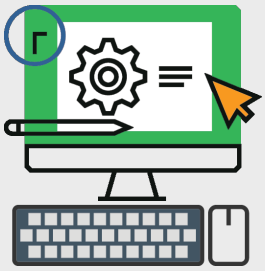
Encrypted Messaging and File Transfer

State legislation, like *Massachusetts 201 CMR 17*, also requires client data to be encrypted before it travels across the public internet. While not all states currently have similar legislation in place, the principles and regulations outlined are part of every firm that takes data security seriously. Transferring unencrypted data to and from clients on the public internet is dangerous. Secure file sharing services and encrypted portals, like Sharefile, when used correctly, make it very difficult for hackers to steal data in transit.

Dual Factor Authentication

Dual factor authentication from providers, like DUO, give firms an additional layer of protection from the risk of having unauthorized users log in to their network. Dual factor authentication operates on the principle of requiring users to both “know something and have something” to verify their identity upon login. Instead of simply providing the correct password, users will also need access to their mobile device or physical security key to authorize their login. This prevents hackers from gaining access to your network even if they are successful in stealing one of your user’s passwords.

In conclusion, we encourage you to consider this list, as well as additional policies like third-party connection, acceptable use and incident reporting, and more, to ensure your firm is adequately protected on all fronts. Above all, make sure your firm actively enforces the policies and standards you establish, because no matter what kind of security you have in place, your firm is only as safe as your weakest line of defense.



Learn more at

www.rightnetworks.com