Security Essentials & Best Practices in The Modern Firm®

Rootworks

The security threats are real

You've seen the headlines:

Deloitte hit by cyberattack, revealing clients' secret emails

IRS warns of 2021 tax scammers: Very active and very creative

FBI warns: 300 percent increase in cybercrimes since COVID-19

Cybercrimes are happening all around us, but it seems the severity of this epidemic has yet to hit home in the accounting profession. Nonetheless, with the constant rise in security breach cases, every firm should have a plan in place for mitigating risk and protecting their clients' sensitive information.

According to a recent report from PhishMe, 91 percent of data breaches start with a simple email. With this in mind, it seems obvious that the best way to reduce risk is to transition away from email as much as possible. Yet, in most firms, email is the central communication tool. This means that clients are sending all types of personal information via email, including bank account information, social security numbers and tax documents.

According to a recent report from PhishMe, 91 percent of data breaches start with a simple email.

Today, a key concern for all firms should be securing the data our clients have entrusted us to maintain. Without a proper security plan in place, it puts your clients and your firm in jeopardy—placing you front and center for cybercriminals who prey on the unprepared. This is today's reality...the danger of living in a connected world.

To help you build your modern firm, this eBook is dedicated to the topic of firm security—what this means to firm owners and staff and how to mitigate risk and protect your clients.

The modern security culture

Being intentional about developing a sound culture around security is the key to mitigating data breaches in your firm. Your security culture is made up of the collective beliefs and behaviors you and your staff have about security. A strong, intentional security culture, for example, is one where email is not the main mode of communication and clients are not delivering sensitive information from inbox to inbox. It's one where staff are properly educated on cybersecurity protocols, such as not clicking links within emails and not trusting unknown email addresses.

Creating an intentional security culture starts by acknowledging that you must make security a priority. To begin building a strong culture, two initial actions are required:

1 Appoint a security officer

This person is responsible for developing your security culture. Your security officer does not have to be a security expert, but will be responsible for working with any expert(s) hired. This person should be properly trained on what to do in case of a security incident, such as a ransomware attack or server hack.

2 Develop a cybersecurity policy

Recorded policy is critical to cementing an intentional security culture. Creating a policy from scratch is not necessary; there are several models available online that offer a sound starting point. Rootworks offers its members a templated security policy created specifically for the tax and accounting space.

Your security policy should be a living, breathing document that is used to educate staff and keep everyone apprised of updated security protocol. Everyone in your firm should understand the policy and make it a part of the daily routine.

Creating an intentional security culture starts by acknowledging that you must make security a priority.

The 8 essentials of firm security

The following are core to any security policy:

1 Educate your staff

As mentioned earlier, 91 percent of cyberattacks begin with an email. Of course, an email alone is not enough to foster an attack; it's the action of the recipient. Cybercriminals are engineering emails that convince recipients to take immediate action. This means that your security culture will only be effective if your staff is educated on proper security protocol. Conduct regular security training throughout the year to ensure your staff is your best line of defense against hackers.

Training each quarter is recommended on the following topics:

- Email 101: Detecting phishing attacks and other nefarious intent
- Password policy updates
- How to report incidents and strange activity
- The role of the security officer

Regular quarterly meetings and training sets the tone that security is important in your firm.

2 Test network security

Firms should have network security tested at least annually. This is usually done by a security company to identify vulnerabilities. In the security world, this is usually called a "pen test" (penetration test). Keep in mind the difference between an information technology (IT) provider and a security firm. It's important that your IT is tested by a security professional.

3 Create visibility

Your network should be actively monitored by a security professional, which can be accomplished remotely. The goal is to understand potential threats via unusual activity before it's too late. Visibility into vulnerabilities is essential to a strong security culture.

4 Ensure endpoint protection

An endpoint is any device that's connected to your network, using either a network cable or Wi-Fi. This can include copiers, laptops, tablets, mobile phones, wireless access points and more. Each time a device connects to your network, you are creating an endpoint—increasing your security risk profile. Your security policy should include expectations of protection for any device allowed to connect to your network. Endpoint protection is typically accomplished with software, and that software should be regularly updated.

5 Adopt removable media controls

Removable media is any data device that is inserted into an endpoint, such as a laptop or desktop computer, with the intent to transfer information. With any external data transfer, there is the possibility of viruses. For example, clients often provide QuickBooks® Desktop files via USB devices. To avoid having to use removable media, many firms use Right Networks to host QuickBooks Desktop, eliminating the need to transfer data back and forth via removable devices. Firms need to have a strict policy on the use of removable media.

6 Limit user access and ensure authentication

This has to do with user rights and password access on your network. Years ago, common practice was to give admin rights to every user for ease of access to the tools required to perform daily work. This is a dangerous practice today. All it takes to open up your network to cybercriminals is one employee with admin rights clicking an email that launches a key logger (a malicious program for recording computer user keystrokes to steal passwords and other sensitive information). Today, limiting user rights is key to a strong security culture.

Firms should also be using multi-factor authentication for user accounts with access to sensitive data, as well as require passwords of at least 16 characters in length. To prevent use of the same password in multiple locations, password managers are encouraged.

To prevent use of the same password in multiple locations, password managers are encouraged.

7 Implement an incident response policy

This offers detailed procedure in the event of a cyber incident. Consider procedural items such as notifying the security officer and how to shut down the network. This could also include unplugging devices and contacting your security firm and legal counsel. In cases of client data breach, there are state-by-state and federal notification requirements that must be met. Communicating breaches with clients should be outlined in detail according to these requirements.

8 Implement mobile and remote work policies

This details policy regarding use of mobile devices. Your policy should address who owns the devices and what data is available on those devices (e.g., firm technologies, apps, email and more). It should also address what happens when an employee leaves. Do they take private correspondence with them? Additionally, in an era where we've experienced a global pandemic, is your staff prepared and equipped to work from home as securely and as productively as at the office?

Security best practices

In conjunction with the 8 essentials for firm security previously listed, also consider the following best practices:

- Perform routine security training for staff. Your staff is your best line of defense, so empower them to protect your clients and your firm.
- Move out of email as much as possible and into highly secure communication tools such as Slack for internal staff communications and a leading system for client communications.
- Verify the authenticity of any communication before acting on it.
- Enable multi-factor authentication on all systems that contain sensitive data and communications.
- Encrypt all data in transit.
- Do not use the same password for more than one login.
- Ensure passwords are at least 16 characters long.
- Educate clients on how to protect their online identity.
- Maintain a strong relationship with your IT and security professionals so they understand your unique situation.

Building a strong, intentional security culture is more about mindset than it is about skill set. You and your staff do not need to be technology experts to help mitigate cybersecurity risks if you follow the essentials and best practices presented in this eBook.

Move out of email as much as possible and into highly secure communication tools.

Final words...

We live in an era where security breaches are happening at record pace. Modern firms are developing security cultures that are intentional and mitigate cybersecurity risk via staff education, advanced tools and platforms, and implementation of security policy and procedure. Ensuring the safety of client data is job one, so developing a security culture made up of smart, informed behaviors is key.

Want to learn more about security for The Modern Firm?

At Rootworks, our team is committed to helping our members build intentional, strong security cultures via ongoing education. And we are continually developing tools and resources that our members require to support education in the area of security.

If you want to learn more, please contact sales at membership@rootworks.com

Rootworks
rootworks.com