Rootworks

# Security Essentials & Best Practices for The Modern Firm®

Rootworks

# Introduction

Several years ago I started writing about a concept I called "The Next Generation Accounting Firm," which today has evolved into "The Modern Firm." The original idea centered on a choice: Do you want a business that supports the life you want to live, or a business that consumes your life? The answer seems obvious when put in these terms. Yet, considering the number of accounting firm owners who feel completely devoured by their businesses, it's clearly not an easy choice to carry out.

As a firm owner for more than 30 years, I've learned that standing still is not an option. Change is inevitable. We can either build a business that is agile and effectively responsive to change, or be consumed by it. In today's competitive landscape, a modern accounting firm has to be so much more than the traditional firm of the past. A Modern Firm requires full-time leadership and a culture that attracts and retains a quality team. It's one that embraces current security standards and strives to use only the most advanced technologies to support a rich working experience for both clients and staff.

Today, the majority of owners I talk to are still overwhelmed by the firms they've created—firms built on traditional concepts...businesses that consume their lives. Of course, whether you choose to be a Modern Firm or not, chances are you will survive in the tax and accounting profession for a while longer because you are willing to struggle through. In other words, you can continue to operate a business that consumes your life, and it will still probably pay you well. But why sacrifice so much when there's an easier way?

Darren Root, CPA, Chief Executive Officer

Anyone who knows me is aware that I admire the genius of Steve Jobs. One of his most inspiring speeches was to the graduating class at Stanford University in 2005, where he said:

> "Your time is limited, so don't waste it living someone else's life. Don't be trapped by dogma, which is living with the results of other people's thinking. Don't let the noise of other's opinions drown out your own inner voice. And most important, have the courage to follow your heart and intuition. They somehow already know what you truly want to become. Everything else is secondary."
>
> — STEVE JOBS

This quote still speaks directly to me today. There is a dogma that is the accounting profession—and you know it and feel it with every deadline that passes and with every ill-fitting client you try to serve. I'm here to tell you that there is a better way and you don't have to be trapped by outdated conventions.

## Making the move to modern

The Modern Firm represents a new movement. One where firm owners ditch the dogma of the past and look to build a sustainable, profitable firm for the future. One with a sound business model, quality staff and excellent leadership. One where a positive culture is at the heart of everything and only ideal clients are onboarded. This is the transition I made in my own firm years ago—from traditional to modern—leaving the dogma of the profession far behind.

We live in a cloud-based, always-connected world where nefarious actors are only a click away from our confidential information. Being modern means being connected, but with connectivity comes significant risks. Because we are trusted with sensitive client information, we must be diligent in our efforts to protect that information.

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

I wish you all the best in building your Modern Firm!

Darren

Darren Root, CPA
CHIEF EXECUTIVE OFFICER

# The security threats are real

You've seen the headlines:

- "Deloitte hit by cyberattack, revealing clients' secret emails."
- "Equifax credit hack: The big risk and what to do now."
- "Cybercrime and hacking are even bigger worries for small accounting firms."

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% 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.

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.

# 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 or 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.

# The 8 essentials of firm security

The following are core to any security policy:

1. **Educate your staff**—As mentioned earlier, 91% 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 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.

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 cloud policy**—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?

   In relation to cloud-based applications, two-factor authentication is recommended. If cloud-based data is available for download, via such solutions as Box, Dropbox or Google Drive, do you allow employees to download at their discretion? As firms continue to adopt cloud-based solutions, it's important to consider how this affects your security culture.

## Security best practices

In conjunction with the 8 essentials for security listed above, 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 Liscio 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.

# 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.

**For more information on Rootworks and our security resources, please contact sales at andy@rootworks.com.**

rootworks.com

Right Networks®

# The leading cloud hosting provider for accounting professionals

Right Networks gets all your critical accounting and business applications into the cloud so you and your team can be more productive, collaborate more effectively, and scale with ease.

Our cloud-connected ecosystem of 250+ best-in-class accounting applications features:

- QuickBooks Desktop hosted in the cloud
- Anytime, anywhere access
- Automatic updates and backups
- Enterprise-class security
- Unparalleled support, 24/7

## Ready to get started?

866-457-9895
rightnetworks.com

**100%** Accounting Focused

**250+** Best-in-Class Applications

**50,000+** Accounting Firms & SMBs