5 Accounting Cybersecurity Tips for SMBs in the Remote Work Era

April 9, 2021

Question: What do the following scenarios have in common?

- Emailing important files to a colleague
- Using an easy-to-remember password, like "'password12345"
- Ignoring "Update Your App" messages on your smartphone
- Using coffee shop WiFi for work
- Opening a donation request email sent from UNICEF

Answer: They all are common mistakes remote staff can make that unwittingly expose your business to cyber threats.

Organizations with dedicated IT staff have robust security policies to keep sensitive information safe. However, many small or medium size businesses (SMBs) don't have dedicated security resources and systems in place. They rely on staff to safeguard critical data, but — let's face it — most people are too busy with their regular work to stay up-to-date on the latest accounting cybersecurity threats.

The rise of remote work has only accentuated the complexities around cybersecurity for SMBs. At the beginning of COVID-19, businesses were forced to adapt to a remote work model, some more successfully than others. This meant finding ways to access critical accounting software, like Sage, and other business applications from anywhere. Some chose VPN. Some subscribed to SaaS solutions. Others chose to host Sage Desktop software in the cloud. After seeing the benefits of managing workflows and accessing data from anywhere through cloud-based tools, the remote model is becoming a permanent way to conduct business.

A remote style of work allows for flexibility and collaboration unimaginable using legacy systems, but it introduces new challenges as well, particularly around accounting software security. So what are the key considerations when developing a cybersecurity plan for your business?

1. It's critical to consider accounting cybersecurity and compliance

The atmosphere around sensitive information is "hot," with a variety of threats that are continually evolving. Over the past year we've seen a rash of ransomware attacks, where bad actors collect confidential data and threaten to release it unless a ransom is paid.

These attacks often gain access to an organization's servers or networks through phishing, a type of cyberattack where an email links you to fake websites or attachments that download malware or ransomware on your computer.

It's critical to evaluate every possible access point to your business's servers and files. While the overall number of malware attacks on businesses dropped by 24% over 2020, the threat detections for a type of malware called HackTools increased by 147%. It's clear that bad actors are becoming more sophisticated in their approach, and since financial motives are behind 83% of attacks on SMBs under 1,000 employees, accounting cybersecurity plays a special role in counteracting the threat.

2. Mobile devices and BYOD are a particular area of concern

Work from home is something that's not going away. In the era of remote work, mobile devices are becoming a default choice for getting work done. And why not? The idea of being able to use that device — say, your phone — for email or communication, or to grab a file quickly and send it off to a client, is extremely appealing.

Still, businesses must stay in compliance with regulatory guidelines on technology and cybersecurity management. So we can't simply ignore the increased security issues that come with mobile devices.

They are broken into more easily than legacy, on-premise computers, which increases a company's susceptibility of being hacked. And the trend of bring-your-own-device (BYOD) further increases that susceptibility, since team members are using the same device for work and for their personal activities.

3. Develop and enforce policies around employee devices

If you haven't done so already, do a quick audit of how your accounting cybersecurity policies are being implemented. Make sure your team members really are enforcing that policy. At a

minimum your policy should include:

First, don't click on suspicious links or download unusual files, even from reputable-looking senders like the IRS or a bank.

Second, hackers try to gain access to networks and data using password-guessing software. They typically screen weak passwords like "password12345" first. So use strong passwords, or consider a password manager like LastPass.

Third, use Two-Factor or Multi-Factor Authentication, which requires users to go through multiple steps of authentication, such as entering a password then receiving a code through SMS. This ensures that if hackers defeat one layer of your company's safeguards, they can't gain access to the account.

Finally, outdated technology, such as older versions of Windows or Microsoft Office, aren't secure against newer forms of attack. As cyber criminals develop new ways to exploit systems, Microsoft and other vendors update their software with patches targeting specific vulnerabilities. So be sure team members install updates regularly.

To learn more specific accounting cybersecurity tips for remote work, check out our blog post, "Cyber Security In Accounting: Secure Your Work From Home Setup."

4. Use applications that have built-in partitioning from the rest of the device

Since employees often use the same device to perform work-related activities and access personal sites such as social media or banking apps, it's critical to partition any sensitive data from the rest of the device.

Enterprise-grade application providers like Microsoft make this straightforward to do. The key part is they partition the applications and data associated with the business from other apps and files.

By using these partitioned applications, employees can conduct business on their personal devices while ensuring that if one part of their device is compromised, their business-critical files will remain secure. They'll also rest assured that they can conduct personal activities without feeling their boss or Big Brother is violating their privacy.

5. The number one trend in the next year: FinTech integration with the rest of the technology stack

In the coming year, we can expect to see more integration between new FinTech apps and the broader technology stack. Part of this includes combining all your company's financial information into a single point of truth, then doing deep integration from that single point of

truth. This will simplify workflows and enable you to expand your business without expanding your staff.

A key part of this is identity management, or being able to identify end users and integrate that identification throughout all the FinTech apps. Another part is new tools that allow you to easily move between apps. So, for example, if you want to move from one CRM to another, we'll see tools coming on the market that enable doing that more easily.

Plan Ahead by Budgeting for Security and Tech Upgrades

To truly meet and sustain the new demands of the remote work environment, make plans for a 10% increase in spending on the tech stack. This is for spending on PCs, laptops, internet and technology, basically anything you need to make your remote work environment work. Part of this spending likely includes some form of remote desktop for Sage or other accounting applications.

Remote desktop interfaces come with their own vulnerabilities, so when you need to move your Sage workflows into a cloud-based, remote work-friendly model, it's important to work with a provider that can provide the security you need. Swizznet makes it easy to access the same Sage software you're used to, on any device, from anywhere on the planet. Our services come with heavy-duty, enterprise-grade Sage accounting cybersecurity. If you are interested in learning more about our cloud-hosting solutions, visit us at www.swizznet.com/why-swizznet. We would be happy to discuss how our cloud-hosting services can help make remote work easier and more secure for your business.

> **Wes Stillman, Chief Executive Officer, RightSize Solutions**
>
> "Really understanding the industry you serve is the only way to fully leverage technology."
>
> After 30+ years of managing technology in high-level positions, Wes began RightSize Solutions in 2002 because wealth management firms needed a technology partner who really understood their needs. More than 13 years later, he remains committed to understanding every nuance of his clients' businesses.
>
> Prior to founding RightSize Solutions, Wes' clients included major airlines, broker dealers, trust companies, health care providers, community banks and other financial institutions. He has held high-level positions at National Advisors Trust Company, FSB, Comdisco, Midwest Consulting Group (Senior Consultant and Yellow Technology Services (Director of Technology).
>
> A technology pioneer in every sense, Wes is regularly quoted as a subject matter

expert in industry publications and also speaks to small and large groups on topics such as cybersecurity, cloud-based environments and leveraging technology.

About RightSize Solution

A sister company in the Swizznet family, RightSize Solutions is headquartered in Lenexa, KS. Our company roots date back to 2002 and our focus is exclusively in the wealth management community. As a leading provider of IT Management and Cybersecurity, RightSize Solutions helps firms navigate the promise of technology to gain greater flexibility, lower costs and increase productivity. A hybrid of customized technology, proactive management and unrivaled service, we keep your systems securely running and your business soaring.