Right Networks®

eBook

Why your firm needs **“smart” security solutions right now**

Introduction

Most accounting firms aren't as secure as they think they are.

Firms are prime targets for data breaches because they manage sensitive personally identifiable information (or PII) for clients. They're a potential goldmine for ransomware attackers, and ransomware attacks are always on the rise.

Firms need threat-protection technology to prevent data breaches, but they need a lot more than that if they want to be optimally secure. They need a comprehensive security strategy that combines technical functionality with training and expertise. The fact is most firm managers don't have the time nor the expertise to manage security, but many try to, anyway. They do it at their own peril.

Fortunately, there are alternatives to firms doing everything themselves, and they're efficiently combined in a new concept called Smart Security Management (SSM), which enables firms to cover security from all angles by outsourcing it to a single security-focused team of experts. SSM goes far beyond just protecting servers. It moves security solutions into every level of computing and includes a human element often overlooked in security strategies.

Cybersecurity in the cloud is best left to **the experts**

Simply put, if you're running your own servers inside your firm, you are basically asking for a security breach. The 2022 Verizon Data Breach Investigations Report (DBIR), one of the most comprehensive studies of cybersecurity, offers a revealing perspective on how mishandling of server technology contributes to cyberattacks.

First of all, make no mistake: Cyberattacks are on the rise. The DBIR indicates that ransomware attacks rose in 2021 at a rate as fast as that of the last five years combined, a 13% increase year-over-year. But there's another number that should be of particular interest to do-it-yourselfers.

Professional error was the cause in **13% of breaches**. That doesn't mean human error as in a person clicking on a malicious link or falling for social engineering. Instead, it refers to employees misconfiguring security for their companies, and the DBIR states specifically that most of those errors involved incorrectly configured cloud storage.

The DBIR takes its data from a broad base of varying sized organizations. There are surely employees in some of those organizations dedicated to maintaining cybersecurity. Yet, in more than one in 10 breaches, the primary cause of the security breakdown was presumably well-trained employees making mistakes.

Most smaller accounting firms don't have dedicated security experts. Most don't even have IT staffs. In many cases, firm owners or other accountants are in charge of security, a task they take on as one of many responsibilities—and rarely one that takes priority over more business-specific jobs.

If your firm doesn't have a proven, dedicated professional handling security, it's at high risk for a breach. Working in the cloud is the right way to go, given all the advantages the cloud offers—including anytime, anywhere access for all employees. But trying to manage security for a server in your office or otherwise set up your own cloud security is just plain dangerous.

You need a partner that can provide the same level of security that big banks enjoy with automatic daily backups in case something unexpected happens. And you need be able to turn your cloud-security operation over to that partner safe in the knowledge that experts are preventing and mitigating cyberattacks for your firm, virtually eliminating the possibility of employee configuration error leading to a breach. Plus, when you outsource cloud security, you and your employees can focus on running your firm and better serving your clients, including giving them confidence that their data is protected to the greatest extent possible.

Individual computers are major vectors for cyberattacks

Cloud security protects the core infrastructure of your operation at the server level, but that's not where security concerns end. Each computer, or workstation, an employee uses is an "endpoint" that provides a cyberattacker a vector for access to your clients' data—or offers a platform for a virus to shut down your operation altogether for as long as it takes you to build your system back.

Anytime, anywhere access is a critical feature of the cloud, but it also introduces risks. Employees now commonly work at home, which can mean working at odd hours or working while distracted. The opportunity for one of your workers to click on a malicious email or inadvertently launch a virus is likely greater now than it has ever been.

Endpoint attacks are frequent and unpredictable. Almost **70% of IT professionals said their companies experienced at least one endpoint attack that compromised data in 2019, and the number of attacks has only increased since.** The majority are "zero-day" attacks, meaning they're virtually impossible to see coming. And they're expensive. The average cost per endpoint breach was $9 million in 2019.

As is the case with cloud security, endpoint security is both complex and critical. The sudden and unpredictable nature of attacks makes preventative endpoint security exceptionally difficult to execute. Even professionals at firms who do nothing but manage security have to focus considerable time and effort on keeping endpoints safe. Most accounting firms, particularly smaller firms, don't have anywhere near the kinds of resources needed to effectively handle endpoint security.

The best defense for endpoints comes from a combination of tools and expertise. Antivirus protection for endpoints is key for keeping a firm's entire system up and running.

Viruses that enter though endpoints can still bring firms to a halt. New machine-learning technology adds another layer to antivirus defense, giving security providers the ability to better predict and thwart threats.

Another critical function is the ability to mitigate damage when attacks do happen. That means always having a current backup on hand to restore data from a compromised computer so that it's both safe and not lost. Data encryption is a further important function of endpoint security. Encrypted data is much more difficult to compromise since it requires a "key" to access in a readable format.

It's highly unlikely that any small or midsized accounting firm can effectively purchase and maintain all those technologies in-house, and applications on their own don't offer expertise on damage mitigation during the panic of an actual attack. Again, the only real choice for your firm is to seek a partner that can provide workstation security while you take care of the business of accounting. Doing anything else is just too risky and time-consuming, and ultimately not cost effective. Your firm is a target for attack. You need the best protection you can get.

Employee behavior is the most common cause of cyberattacks

The Verizon DBIR established that the cause of more than one in 10 data breaches is professional error—an IT pro getting something wrong, often involving misconfiguration of cloud storage. That's bad. But what's really bad is the much more common and damaging form of user error—your employees clicking on links or installing applications that launch ransomware, malware, viruses and other damaging applications on your network.

It happens all the time. The "human element"—for instance, somebody in your firm clicking on a malware link—was present in a whopping 82% of breaches in the DBIR. It's far and away the most common factor in data breaches. Employees get tired and careless—everybody does—and perpetrators of phishing and other attacks become more clever, and their attempts to steal data more frequent, all the time.

Not all attacks are external, either. Although attacks from internal sources seem unlikely and represent a minority of breaches overall, they're generally the most financially damaging when they happen. In any case, your employees need to know how to avoid attacks and to recognize when one is happening, no matter the source.

Technology alone will never be enough to keep a firm safe. Yes, it helps a lot, especially when experts who do nothing but provide security are running it. But the "human element" will never disappear from security threats. If anything, the rise in ransomware attacks is making the importance of training employees more evident all the time. (Otherwise stated, the continued rise of ransomware demonstrates that the security training most businesses think is working probably isn't.)

Firms need to know that their employees are as unsusceptible to attack as they can possibly be. Clients need to know that as well, and the IRS has even tightened its security requirements for firms in recent years. There is no effective security without effective security training, and the most effective security training comes from experts who understand both the topic of security itself and how to teach employees what they need to know.

Security training shouldn't be generic. It should be as focused on an individual employee's role as much as possible, and it should absolutely be focused on the specific industry or profession in which a company operates. Accountants and people who work at accounting firms need security training specific to accounting. And you need the confidence of knowing that your firm's employees won't easily be tricked into falling into security traps, even in their most vulnerable moments.

This is Smart Security Management (SSM)

SSM is where the three critical functions of security management—cloud security, endpoint security and end-user training—come together. What makes SSM so "smart" is that it leaves little to chance, and it's available from a single source.

There's no need for your firm to take the risk of handling security internally. There's also no reason to seek out different partners for cloud security, endpoint security and security training. Right Networks has a solution for this three-pronged approach to SSM.

Secure Cloud offers secure and reliable cloud hosting that safeguards your data with end-to-end redundancy across all systems, real-time data replication and enterprise-class multi-layer security systems—24/7/365.

Secure Workstation is a comprehensive, secure endpoint solution to safeguard your business-critical data. You can have peace of mind with added security for all your employees with one enterprise-level solution.

Security Awareness Training offers an employee education program that provides best practices for staying safe online using an expert-developed gamified training program.

Right Networks offers SSM technology, expertise and training from one organization that has been at the forefront of securing accounting firms for more than two decades. The core fundamentals of SSM in all three critical areas of security are designed and built specifically for accounting firms and based on expertise recognized throughout the accounting profession.

Accountants shouldn't try to be security experts. Instead, they should be focused on serving their clients. Outsourcing the three pillars of security is safer and ultimately more cost-effective than trying to handle security internally with employees who are better off undertaking other tasks. Smart Security Management is the smart move for accounting firms and one they should make now—before it's too late.