

EBOOK

Key cybersecurity takeaways from Rightworks security leaders



 **rightworks**



Introduction

If you're not already obsessed with cybersecurity, you should be. Far from receding as a concern for accounting firms, the threat of a cyberattack is increasing all the time—literally.

Cyberattacks are becoming more frequent and more sophisticated, and your firm—along with virtually every other business—is a target. The number of phishing attempts **jumped more than 60%** in 2022 after rising almost 70% in 2021. With 80,000 malicious URLs launched every day, one of them will eventually have your firm's name on it.

Cyberattackers can strike anywhere, anytime. No one is immune to a cyberattack, not even companies that produce seemingly innocuous products or services. A major attack **crippled a large maker of jet skis and snowmobiles** in the summer of 2022. More recently, cybercriminals **took aim at the Metropolitan Opera** in New York City, severely hampering the institution's ability to sell tickets and merchandise both online and over the phone.

If cybercriminals will go after recreational vehicles and high-brow live entertainment, they'll go after just about anybody. And they'll definitely target a business such as an accounting firm whose business it is to store and manage its clients' most sensitive financial data.

Nothing will wreck your firm faster than a data breach. The cost for a typical small firm to recover from a cyberattack is **between \$170,000 and \$300,000**. Managing security cannot be an afterthought, but it's also too complex for a non-expert to try to handle. Effective cybersecurity requires round-the-clock monitoring and updates that no accountant could or should try to take on alone.

Listen to the experts who are on the front lines

That's exactly what experts at security providers do. They fight a continuous battle against cybercrime. Most people who don't work in cybersecurity don't know how complex a field it really is. Sure, we all know it's important and a major concern for accounting firms and small businesses—although many people still don't take security threats as seriously as they should.

Most of us go about our days without really appreciating the constant battle cybersecurity experts are fighting on our behalf. Brian Rae, Senior Director of Security and Compliance, and Jose Smith, Director of Cybersecurity, lead the battle against cybercriminal activity both for our customers and within Rightworks. They sat down to discuss trends in cybersecurity, the number of security threats (which is staggering), as well as what firms and businesses can do to stay safe. Spoiler: Employee training is key!

**Here are some key takeaways
from the conversation...**



Key takeaway #1

Cyberattack attempts happen far more often than most users probably realize

The successful cyberattacks that make the news, whether they hit a major retailer, a bank or the opera, represent only a fraction of total attack attempts. Right now, a bad actor is trying to steal your data. In fact, in pretty much any given second, some would-be cybercriminal is trying to break into your system.

In a given month, out of about 1 million corporate inbound emails Rightworks receives, almost 15% are categorized as phishing or malware. That averages out to about 7,500 per day being remediated. The company blocks more than 10 million potential malicious connections every 24 hours.

Granted, Rightworks, with several hundred employees, is far larger than your accounting firm or small business might be. But more than 10 million malicious hits a day is a massive number. Taken down to the scale of a much smaller business, that could still equate to thousands of attack attempts per day and hundreds or even thousands of phishing emails.

All it takes is one successful attack for a cybercriminal to steal your company's—and your clients'—data. That's why the battle behind the scenes to keep both Rightworks and its customers safe literally never ends.

**“We monitor the dark web,”
Rae says of Rightworks’
application-hosting services.
“We put people’s names in and
search them continuously.
You’d be surprised how many
hits we have.”**

With each hit, the Rightworks QuickBooks® hosting security launches a remediation effort. If a cyberattacker has stolen critical data, our experts can remediate the situation before the data thief can do any damage. But attacks remain constant—and they're becoming more sophisticated.



Key takeaway #2

Cybercrime is an industry now with vendors and tech support

You might think you can spot a phishing email before it even hits your inbox. There are misspellings, grammatical errors and other clunky mistakes that make a cyberattack attempt almost cringingly obvious. While those ham-fisted attacks still exist, the new generation of cyberattack is different. It's sophisticated, and it's literally backed by a team of professionals.

That's because cybercrime is an industry now—with merchants that offer cyberattacks as a service the way above-board vendors offer security services. "Cyberattacks are becoming more complicated," Rae says.

"Cybercriminals used to make simple mistakes, but now there's phishing as a service and malware as a service. You're at the will of a lot more bad actors."

Some malicious actors have even repurposed legitimate security tools as services for committing data theft.

The result is that cybercrime is expanding, as attackers have an easier point of entry into stealing data. In essence, many of them need only write emails. A service provider takes care of the rest.

"These cybercrime service providers offer a system that will generate a ransomware key and package it into malware," Smith explains.

"It can be distributed into a victim's system and also provides the mechanism for a cryptocurrency ransom payment. All of that is infrastructure. Cyber-attackers are paying these cybercrime vendors to run that infrastructure. The vendors are providing all the functionality."

The malicious vendors even offer professional tech support and sometimes have sales and marketing operations as well. Cybercrime is no longer the realm of klutzy amateurs.



Key takeaway #3

Phishing emails now look very much like the real thing... and sometimes better

The proliferation of cybercrime as a service has made phishing emails much more difficult to detect.

"The quality of the documentation is excellent," Rae warns. "Spot-on stuff."

There are creative new tactics in play among cybercriminals. Attacks often look like legitimate business inquiries.

Smith explains: "An accountant receives an email that says, 'I'm looking for a new accountant.' The cyberattacker sends that email under the guise of a prospective client. The firm responds.

The attacker asks for a secure place to send last year's tax documents. The firm says send to a portal. That cyberattacker then uploads malware into the portal. That is some of the most malicious malware we have seen."

And it's hard to stop, Smith continues, because no business can reject what looks like a genuine inquiry from a new customer. "If you say to an accountant, 'You need to be careful of people looking for new business,' that doesn't sell very well. But they can be tricked through email pretty easily. The phishing emails are almost constant."

There are other new theft techniques, too, such as an attacker who searches LinkedIn for people who have just taken new jobs. The attacker spoofs an email from the new hire's boss or CEO and sends the new hire a message that will ultimately launch malware once the new employee clicks on a link or document in the email.

"The obvious cyberattacks of the past are fading away in favor of more nuanced stuff," Smith confirms. "That's why training employees is more important than ever."

Key takeaway #4

Multifactor authentication is necessary but not perfect

Some of the methods firms and businesses use to protect themselves are rooted in technology—for instance, every employee should use a password manager. But even the most sophisticated technology must work in tandem with security-savvy employees. One essential security measure our experts mentioned was multifactor authentication (MFA), which involves logging into an application or device with two or more elements of authentication.

In other words, if you're using MFA, you might log in with a password on your computer and then receive a confirmation on your phone that you'll need to accept before you can access your app or device. MFA itself is evolving with biometrics such as facial and fingerprint recognition becoming more common as forms of authenticating identity.

MFA is effective in preventing data theft because even if a cybercriminal steals a user's data, the bad actor won't be able to simply log into the user's accounts through a single source. The second level of authentication stops a lot of would-be data theft.

"If you accidentally give your credentials away, there's a backstop there," Rae says.

But while it's a security technology all businesses must absolutely have, it's not perfect. One element that is chipping away at the effectiveness of MFA has more to do with users than it does with the



technology itself. MFA fatigue sets in when users accept a second form of authentication even when they never entered a first one.

For instance, say a bad actor steals someone's username and password. The attacker tries to log into the user's account but can't because the user has to give permission using a second identifier. So, while the attacker tries to access the user's computer, the user's phone prompts for permission for account access.

In too many cases, MFA fatigue sets in, and a user will allow access to the account just to stop the phone from prompting even though the user isn't trying to access the account in question. At that point, the attacker is in, and data theft begins.

"It's unfortunate behavior by the users," Rae says.

Key takeaway #5

Training employees in security should be a top priority

Both Rae and Smith insist that the number one thing any business can do to protect itself from cybersecurity threats is to train employees to recognize and avoid security risks. **The greatest security risk to accounting firms and small businesses is user behavior.**

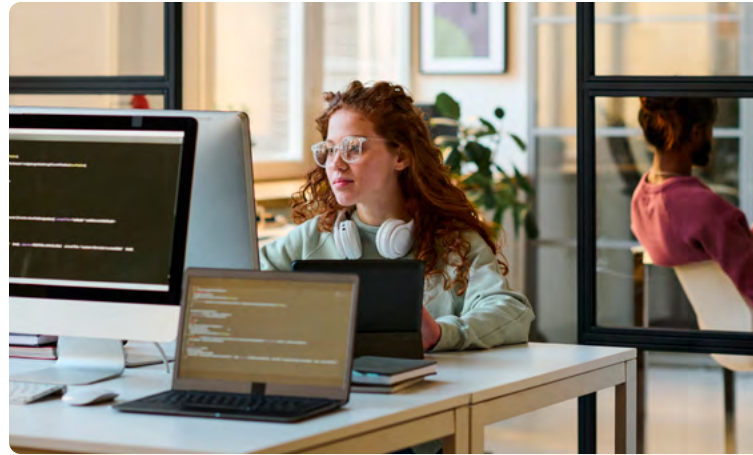
■ **“It’s always the users,” Rae says.
“That’s our biggest threat factor.”**

Clicking a phishing email or answering a call and giving out information that allows a malicious attacker to use that info for social engineering. It’s the everyday stuff that the malicious actors are looking for.

To be fair, it’s hard for employees to be on guard all the time—both at work and at home. As always, the cybersecurity battle never ends.

“You’re getting inundated with this stuff on a business level and a personal level,” Rae confirms.

“If there is a way for the user to work, there is a way for the user to do something that they shouldn’t,” Smith adds.



Small firms and businesses are hardly immune to attacks, either. In fact, they’re frequent targets. Accounting firms are especially in the crosshairs because they have access to their clients’ most critical information, but every type of business is at risk.

“IT security is not top of mind for small businesses,” Rae says. “It only becomes top of mind when things happen. They become victims more often than some of the bigger businesses.”

Every business, regardless of size, needs to train employees, owners and everyone else involved with the operation on how to recognize and avoid security threats. Ultimately, most attacks that result in data loss occur because a user in an organization opens the door to let them happen. Technology can help avoid attacks and can remediate damage caused by one, but the first line in preventing attacks is always people.

■ **As Smith says, “Your people are
a critical part of your security.”**

Rightworks is your security partner

The cloud remains the most reliable and safest way for your firm to access its applications, secure your IT infrastructure or outsource your IT processes—including security—altogether. Whether you're looking for secure QuickBooks® Desktop that's available anytime, anywhere, or you want to have experts run a managed IT service so you don't have to worry about cybersecurity, Rightworks has a service for your firm.

And remember, Rightworks also offers enterprise-level security for your devices, as well as training for employees that will enable them to detect and avoid cyberattacks. And it's all backed by experts who fight the battle against cybercrime for you every minute of every day.

Want to learn more?

Contact us today at **888.210.0237**



rightworks
rightworks.com