Common Cybersecurity Threats for RIAs and IBDs

How to Protect Your Business and Your Clients

Your business holds incredibly valuable data about your clients and their finances. While you might think that you aren't a big enough player to be targeted by hackers, you're more at risk than you think.

Cybercrime is on the rise. According to research compiled by Varonis[i], a leading cybersecurity company, financial services are big targets for hackers looking to steal personal data and assets. Around 10% of data breaches affected the financial industry, and at an annual cost of over $18.3 million, it accounts for the highest costs across sectors.

In September 2020, the SEC issued a risk alert about credential stuffing[ii], a type of cyberattack that uses compromised log in credentials to access and steal customer assets and information. The Office of Compliance Inspections and Examinations (OCIE) reported an increase in credential stuffing attacks against RIAs. In July 2020, the SEC and OCIE released a risk alert about the increased frequency and sophistication of ransomware attacks[iii].

Prevalent cybersecurity risks for RIAs and IBDs

Phishing

Phishing and spear phishing use fraudulent emails to access your network and introduce malware or ransomware. All it takes is one unsuspecting employee to open a phishing email and click on a link to let the cyber attackers into your network where they can access all your clients' data.

Malware

Malware is an umbrella term for various types of software designed to exploit or harm a device, system, or network. It includes viruses, spyware, trojans, and ransomware. The malicious programs cause several problems ranging from crashing systems and devices to stealing data and encrypting files.

Ransomware

Ransomware is a common type of malware. When it installs on a computer, it encrypts files and demands that a ransom be paid to release and restore your data.

Data leaks

Your cybersecurity practices, or lack thereof, can increase your risk of data leaks. Many security breaches are due to human error, such as weak passwords. Despite the well-known dangers of weak passwords like qwerty12345 and using the same password for everything, people still do it, putting their business's data at risk. Additionally, if you allow your employees to use their personal devices for work, your risk of security breaches increases.

Third-party vendors can also pose a risk. As they have access to your systems, their security breaches can easily become your security breaches.

Cybersecurity solutions

Fortunately, you can take steps to protect your business and your clients.

Training

As many security breaches are due to human error, training your team to be vigilant against cybercrime risks is paramount to your security. Make sure everyone knows about the warning signs of phishing scams and password best practices.

You can also encourage the use of secure password managers to track unique passwords. This can make it easier for you and your team to manage multiple unique passwords, eliminating the temptation to use the same password for everything.

Keep your network and devices up to date

While no software is completely impenetrable, keeping your operating systems, browsers, and anti-virus software current can limit system flaws hackers use to break into your accounts. The same advice applies to mobile devices.

Log in authentication

There are several options to choose from when it comes to log in authentication. Two-factor authentication with SMS messages isn't necessarily the most effective option these days. You can also consider security keys, authenticator apps, and password managers with frequent password changes.

VPNs for remote access

Remote working has become far more common. Whether you and your team are working from home or eventually get back out to see your clients in person, a VPN (virtual private network) can protect your security. Most open Wi-Fi networks or hot spots are vulnerable to DNS (domain name server) spoofing, which redirects traffic to a fraudulent website.

Acceptable use policy

An acceptable use policy outlines exactly how your employees can use company-issued devices, software, internet, and email. In addition to ensuring that your employees are familiar with the policy and adhere to it, you can install content-filtering software and a firewall to add an extra layer of protection.

Important takeaways

Cybercrime is on the rise, and financial services companies have a high risk of attack. However, being aware of the potential vulnerabilities and taking action to lower your risk can help keep your business and your clients secure.

It's important to work with partners who are diligent about cybersecurity. Attackers can gain access to your systems through third-party vendors, so it's critical to investigate potential partners' cybersecurity practices before signing on with them.

Axos Clearing, and our affiliate Axos Bank, take cybersecurity very seriously. Our customers' and clients' security is our highest priority. Contact us today to learn how we can work together to grow your business while maintaining the highest cybersecurity standards.

---

[i] Varonis cybersecurity statistics https://www.varonis.com/blog/cybersecurity-statistics/

[ii] https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf

[iii] https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf