How Accountants Can Meet Tougher Cyber Insurance Coverage Requirements

March 20, 2022

As accountants and their clients evolve their businesses to support the next normal, cyber threats are close behind. Even small firms are a prime target due to the sensitive financial data they can access. The potential cost of a data breach is far-reaching, both in terms of direct costs and indirect impact to a firm's reputation.

Many companies are realizing it's a good idea to protect their business with cyber insurance coverage, but it's still not clear how to price premiums or protect against the total cost of a data breach, and there's a massive imbalance between global cyber insurance premiums and potential covered losses insurance companies might need to pay out (HBR).

What this means is cyber insurance companies are risk-averse when it comes to accepting customers. Like other forms of business insurance, they require customers to meet specific cyber insurance coverage requirements to qualify. In this post, we'll look at these security practices and explain they are beneficial for protecting sensitive client and firm data.

Multi-Factor Authentication

While the bulk of attacks (83%) against the Financial sector directly compromised personal data, 32% of data breaches were credential attacks (Verizon 2021 Data Breach Investigations Report). Once attackers possess credentials like passwords or user IDs, they can then access your systems to install ransomware, erase business-critical information, or steal sensitive data.

Multi-factor authentication (MFA) protects systems in the event of compromised credentials by requiring multiple forms of authentication, such as a password, a code sent to another device, or asking questions only the user can answer. Cyber insurance companies increasingly require MFA around email, network access, and admin access because it significantly minimizes the damage organizations incur in the event of stolen credentials.

> Cyber insurance companies increasingly require MFA around email, network access, and admin access because it significantly minimizes the damage organizations incur in the event of stolen credentials.

Some forms of MFA require you to buy technology, such as a USB authentication device, but most forms are simple, inexpensive, and only require an extra step at login.

Cloud Network Firewalls

In the early days of the internet, many organizations installed firewalls to protect their networks. These firewalls were physical devices that sat adjacent to the router and filtered malicious or unwanted traffic. These are obsolete now that businesses use cloud infrastructure to store critical data and run their applications. They've been replaced by cloud firewalls, which act like physical firewalls in how they filter traffic but are hosted in the cloud.

Cloud firewalls are available as a subscription and integrate with the cloud infrastructure you use to host data and applications. They scale to handle increased traffic, and offer network security as well as on-premise infrastructure.

End-to-End Encryption

Whenever a client sends you files or you collaborate with your colleagues online, you have to transmit that data between your system and their system. This means the data is potentially vulnerable to interception or tampering by a third-party while it's in transit.

End-to-end encryption (E2EE) protects against this by encrypting data before it leaves the sender, then decrypting it once it arrives. Prying eyes can still see the data while it's in transit, but they won't be able to read it.

Many online messaging services like WhatsApp use E2EE, which has caused controversy since it prevents authorities from monitoring these platforms. It's important to note that most email is not protected by end-to-end encryption, so it's critical to find a way to transmit critical data through methods other than email.

Train Your Staff to Be a Human Firewall

Cybersecurity brings to mind technology, firewalls, and sophisticated hacking techniques, but often the most vulnerable aspect of organizations is the human side. A single click on a single bogus email can give malicious actors access to your critical systems and data. It's key to train your staff to be aware about phishing and other ways they may inadvertently expose sensitive data to external parties.

Be sure to train your employees about the techniques most applicable to your firm. For example, if you offer outsourced CFO services, train employees on the protocol around approving transfers or payments. This can help stop attackers who have gained access to your client's systems and are attempting a fraudulent transfer.

Meeting Cyber Insurance Coverage Requirements with Managed IT Security by Swizznet

We've covered some of the most common criteria insurance companies require. Even if you

choose to self-insure rather than buy cyber insurance, these steps can help secure your organization against attackers so they'll look for an easier target.

Many accountancies lack the in-house skills and resources to develop a comprehensive security program. They're in the business of accounting, after all, which is why Swizznet is bringing its combined decades of IT and security experience together into SwizzStack.

SwizzStack is our new IT-as-a-Service offering. It can help you meet the requirements for cyber insurance and build a comprehensive IT management program for your firm, without the expense of an in-house IT department. We recently helped halt a ransomware attack on a client in the construction space, and are enthusiastic about helping protect your data and systems as well.

Contact the Swizznet sales team to start developing a Stack for your firm.