ProWriters
Professional & Management Liability Insurance

The Six-Step Guide to Becoming Your Clients' Cyber Expert

ProWriters
Professional & Management Liability Insurance

The Six-Step Guide to Becoming Your Clients' Cyber Expert

As we move further into the digital age, our lives continue to change as technology advances. With technology taking on increasingly important roles in the way we communicate, practice medicine, utilize artificial intelligence, and even vote, cyber threats are rapidly evolving to infiltrate these systems however possible. For any organization, cyber security must now be a priority in order to survive in today's high-risk climate. As brokers, it's necessary that you learn how to become a cyber security expert in order to ensure your clients are protected.

Cyber security is proving to be increasingly complex and many organizations are looking to ramp up their cyber security budgets and efforts. While cyber attacks are currently a serious threat, based on Aon's 2019 Global Risk Management Survey, cyber attacks and data breaches will climb from the sixth to the third highest risk for businesses by 2022.

As nearly every organization is now at risk of a cyber attack, it's important to consider how you can best protect your clients. Making sure your client has the right cyber policy in effect can have a consequential impact on their ability to survive a cyber attack. As the severity of these attacks increases, the damages have become so devastating that nearly 60% of small businesses fold within six months of a cyber attack.

ProWriters
Professional & Management Liability Insurance

Six Ways to Prevent Cyber Attacks and Protect Your Clients

For many of your clients, cyber security is complex and difficult to understand. As their broker, you can help them both prevent attacks before they happen and mitigate the damages should a breach occur.

Utilizing these six procedures, you can act as your clients' security consultant and help them make sure they have the best possible protection against imminent security threats.

1) Educate You & Your Client

Staying current on cyber security trends, procedures, and best practices are important for both you and your client.

Agents/Brokers:
It's imperative that agents are aware of the current threats that are affecting organizations. As these rapidly adapt, cyber policies are forced to adapt as well. Making sure you're aware of the potential risks will help you ensure that your clients have the best possible coverage to protect against threats. Check out Insurance Business Magazine for the latest news in the cyber security and insurance industries.

As ransomware attacks continue to increase and cause more substantial damages, it's necessary to understand the latest threats and how these attacks are carried out. For more information on the most current threats, take a look at Brian Krebs's blog, KrebsOnSecurity.

Not only is it now necessary to be able to quickly identify a ransomware attempt, it's also important to understand when to pay a ransom demand and when not to. It's generally important to consider the likelihood that the attacked will provide the correct decryption method, whether the network has suffered corruption as a result of the attack and whether there are any existing backups available (even if they're not current).

Clients:
Your clients, themselves, are often their first defense against threats. Your clients should be aware of the latest ransomware trends, phishing tricks, and robocalls that could potentially lead to a breach. Understanding how to identify these risks will prevent human error and potentially allowing unauthorized access.

Encourage your clients to regularly check the Cybersecurity and Infrastructure Security Agency (CISA) website for the latest in cyber threats from the Department of Homeland Security.

2) Update Software

While many attacks are due to user error, others are executed through weaknesses or glitches in software or security systems. Although this small step can feel tedious and repetitive, it's important that your clients keep all technology and software up to date with the latest and most advanced versions available. A quick, recurring reminder to your clients may be just what they need to keep their software current.

These security "patches" and updates address any known vulnerabilities. Any vulnerabilities left as is can be taken advantage of by a hacker. If you have the option to receive updates automatically, this is the most highly recommended option by CISA.

When a software program's support or updates are discontinued, this is known as end-of-life (EOL). Any EOL software product should be retired immediately.

3) Protect Passwords

With technology that can guess thousands of passwords in seconds, a complex password is a strong password. Your clients need to utilize both letters, numbers, and varying capitalization in their passwords and regularly update them to protect their private data. Utilizing a password generator or password manager can help clients select longer, more complicated passwords that will be extremely difficult to breach.

Utilizing a certain memorable phrase, song lyric, or joke can be a good way to generate a password that is both complex, but easy for you to remember. Try taking the first or last letter of each word of the phrase to build a jumble of characters you can remember, including capitalization, numbers and characters for extra protection. The longer the password, the more secure it will be. In addition, utilizing Multifactor Authentication (MFA) wherever available is another step that can help keep logins and systems more secure.

For more tips on password security, check out the KrebsOnSecurity blog post, Password Do's and Don'ts.

4) Focus on Email Security

Social engineering attacks rely on human error to gain access to sensitive data and information through email. Employees account for 90% of cyber claims which is why training and education are key in building a culture of cyber security awareness.

Here are a few steps that your clients can take to increase their email security:

1. Dual Authorization: Always have multiple people signing off on checks, ACH transactions, and wires and always call the vendor directly with a public number or number you already have on file. Never use the number or email address listed on what could be a fraudulent invoice.

2. Secure Email Gateway (SEG): This software monitors emails (both sent and received) to defend against spam, malicious attacks and fraudulent content. Popular vendors include Proofpoint, Mimecast and Barracuda. These softwares typically cost less than $5 per month.

3. Multifactor Authentication (MFA) on Email: This security measure requires more than one method of authentication to confirm who the user is and grant access. This feature is often included and free in most email software and can easily be setup.

5) Form a Data Breach Response Plan

While the prevention of cyber attacks is important, your clients will need to be realistic about the chances that they'll be affected and that a breach can likely occur. Setting up a Data Breach Response Plan in which every involved party understands their role will help your client act quickly and mitigate the potential damages. Having a team of experts on hand to guide you through the recovery process is key. This should include both a data forensics team and legal counsel.

In addition, a communications team should be in place to notify all affected parties, including employees, customers, investors, etc. Transparency is important so that consumers can protect themselves and their information.

Finally, notify law enforcement which may involve your local police, FBI, U.S. Secret Service or the U.S. Postal Inspection Service.

6) Get Protected With a Cyber Liability Policy

The most important step your client will take in protecting them from cyber attacks is purchasing a cyber liability policy. With this protection, your client will have access to the best possible vendors to help them begin the recovery process immediately, ensure they're in compliance with all rules and regulations, and protect their reputation.

As ransomware and other cyber threats won't be slowing down anytime soon, it's important to be realistic in protecting your clients. While there are many ways to protect them from these attacks, they are still very much at risk.

A cyber liability policy can provide a number of coverages:

First Party

- IT Forensics Costs
- Notification Costs
- Credit Protection Costs
- Crisis Management Costs
- Crime & Social Engineering

Third Party

- Breach of Personally Identifiable Information (PII)
- Breach of contract
- Negligent protection of data
- Network security breaches
- Transmission of software viruses denial of service attacks
- PCI fines and penalties

Additional Coverages

- Multi Media Coverage
- Cyber Extortion
- Cyber Business Interruption
- Hacker Damage or Digital Asset Damage

ProWriters Makes Cyber Simplified

With a streamlined approach, ProWriters has made the process of selling cyber insurance to your clients easier than ever. With our Cyber IQ Comparative Rate Portal, you can compare multiple quotes from multiple carriers to find flexible coverage to fit your clients' specific needs. With the best possible cyber liability coverage, your clients can rest assured that they're protected.

To keep both you and your client informed on the global cyber industry, including the latest threats, laws, regulations, and coverage options, check out any of these resources, available online:

1. Marsh JLT Specialty Cyber Newsletter (FREE)
2. ProWriters Cyber Blog (FREE)
3. Advisen Cyber FPN Newsletter (Subscription Required)

To learn more, contact a ProWriters expert today or call 484-321-2335 with any questions.

ProWriters

Professional & Management Liability Insurance