IT’S TIME TO GET SERIOUS ABOUT CYBERCRIME

By Tom Wetzel

How well is your agency protected for cybercrime – and what is your comfort level in guiding your clients to protect themselves from cyber hacks and scams? The fact is most agencies fall short on both counts even though cybercrime is growing in frequency and severity while the cyber insurance market hardens.

It’s no secret that agents and clients alike are bombarded everyday with news of the latest data breaches, including some in the insurance industry such as Geico, CNA and Vertafore. With each new breach, consumers grow more concerned about where the personal data they hand over for goods and services ends up. Agents need to take serious note of this consumer angst. Legally, agents are liable for the data they collect from prospects and clients, no matter how or where that data gets shared.

Regulators are also responding to cybercrime by creating new rules for agents to better protect the data they collect and share. These regulations go beyond the NAIC Insurance Data Security Model Law to new laws governing data privacy and the latest law in Michigan that requires agencies with twenty-five employees or more to file a cyber plan with the state.

Insurers are weighing in as well with many rewriting agency agreements to require agents to make stronger efforts to mitigate cyber risk. Not only that, but most insurers also now require prospective insureds to show proof they have already taken specific steps to protect its data before issuing a quote, let alone bind a policy.

Cyber criminals use many strategies and techniques to wreak their havoc, however ransomware garners the most attention. The emphasis on ransomware is not misplaced, as it represents the largest cybercrime segment. Cyber insurer Coalition reports, however, that 59% of its cyber insurance claims were not due to ransomware, but cyber events including funds transfer fraud and email compromise. Hackers are also finding new ways to break into your data through agency vendors, such as quoting software and through policyholder groups, particularly contractors.

Now more than ever, every agency must step up its efforts to address its own cybersecurity vulnerabilities and those of its clients. Cybersecurity experts agree the best defense involves using a layered approach by combining multiple authentication methods with more secure systems and protocols. Some insurers offer security audit services to agents and others are revising agency agreements to require greater attention to cybersecurity.

A critical starting point is a cyber risk assessment, to identify the agency’s cyber weaknesses, where they reside, and how to fix them**. Contact PIA about its new cyber assessment program**. Insurer Beazley’s “Steps to Protect Against Ransomware,” advises the following:

- Start with a risk assessment. Addressing risks starts with identifying what they are, where they are, and how severe the consequences are.
- Secure email content and delivery. Enforce strict Sender Policy Framework (SPF) checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro-documents, and links to malicious sites.

- Manage access effectively. Ransomware does not have to go viral in an organization. Put in place appropriate measures for general user and system access across the organization: privileged access for critical assets (servers, endpoints, applications, databases, etc.) and enforce multi-factor authentication (MFA) where appropriate (for example remote access/VPN, externally facing applications).
- Back-up key systems and databases. Ensure regular back-ups that are verified and stored safely offline. Use strong, unique back-up credentials, and secure them separately. Test backups to ensure restoration from them.
- Educate users. Most attacks rely on users making mistakes. Train users to identify phishing emails with malicious links or attachments. Regular phishing exercises are a terrific way to do this.
- Patch systems and applications. Conduct regular vulnerability scans and rapidly patch critical vulnerabilities across endpoints and servers – especially externally facing systems.
- Secure remote access. Do not expose Remote Desktop Protocol (RDP) directly to the Internet. Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled virtual private network (VPN).

Cybercrime poses an existential threat to your agency as well as your clients -- one cyber hack could well cripple your agency or a client – and you owe it to them to provide the counsel they expect and need. This is not an issue that can be put on the back burner.

Tom Wetzel is CEO of Thomas H. Wetzel & Associates, an insurance marketing firm for independent agencies which has partnered with PIA to deliver its cyber risk assessment designed just for agents. Th firm also offers, HI-TRUST-certified messaging, website design, content creation, and the Wetzel Digital Roadmap©. For more information, the firm's website is www.wetzelandassociates.com. Contact him at twetzel@wetzelandassoc.com