—Reprinted with permission from PIA Management Services Inc.—

MARC S. VOSES, ESQ.
Partner, Kaufman Dolowich & Voluck LLP

Shields up: Prepare your cyberdefenses

If Target, Home Depot, Sony and Equifax are unable to defend against a cyberattack with their resources, what chance do insurance agents and brokers have against a similar attack? Well, given the right preparation and corporate culture, you stand a fair chance, but only if you can learn from others' mistakes and take action quickly to shore up your defenses.

A treasure trove of information

When it comes to insurance producers, we must consider the nature of the information that is shared during the application process. Names, addresses, financials, contracts, blueprints, descriptions of internal controls, ownership structures, proprietary information and other highly confidential and nonpublic information is voluntarily shared by prospective insureds with insurance agents and brokers, which is then shared with third parties.

What are your security protocols for protecting this nonpublic information? What security protocols do your third parties have in place? For those who do know the answers, it is most likely, "We don't have any security protocols that I'm aware of, and I've never asked the third parties that we send client information about their security protocols."

Your company's computer system also holds additional valuable information (i.e., your employee records, which includes names, addresses, Social Security numbers, health-care information, bank routing numbers and W-2 forms). They deserve as much protection as the information that belongs to your clients.

Payment card pitfalls

Does your agency accept credit cards for premium payments? If so, this adds another layer of vulnerability to your operations. Do you retain your clients' payment information (e.g., credit card or bank wire information) in your computer system? That information is valuable to cyberthieves. What kind of processing software do you have to accept credit card payments? If cyberthieves can introduce malware into the payment processing software, information collected in the payment process is vulnerable to theft.

Social-engineering fraud

If your company accepts or makes wire transfers, those transactions are susceptible to manipulation. If cybercriminals gain access to your computer system, they could redirect wire payments from your clients to another bank account and the money would be gone before anyone noticed. They also could transfer a company's money or trick an employee into transferring money into their own account.

Social-engineering fraud, which is getting someone to do something that they otherwise would not do if they knew the result, is accomplished in a number of ways. For example, your accounts payable clerk receives an email from the CFO directing the payment of a long-standing vendor's invoice by bank wire to a new bank account. The email appears authentic and was sent from a person with the authority to direct such a wire payment, and is even written in the CFO's writing style, and the vendor invoice checks out against the company's records. Thinking the request was valid, the accounts payable clerk initiates the wire.

In actuality, cybercriminals stole the CFO's login credentials by tricking the CFO into giving up that information in a series of emails and website links. With unauthorized and unlimited access to the CFO's email account, they identify similar emails from the CFO to the accounts payable clerk directing payment of vendor invoices. Mimicking the CFO's prior emails, the cybercriminals used a valid invoice received by the company and directed the accounts payable clerk to make

a wire transfer to a bank account they set up. When the real vendor asks about the status of payment of the still outstanding invoice weeks later, the company discovers the scheme and the cybercriminals have closed out their bank account.

Watering-hole attack

Every industry has go-to websites that allow professionals to get the latest industry news; share thoughts on major issues; and network with prospects. Chances are you have visited these sites and clicked on links; downloaded files; and signed up for emails. In a "watering-hole" attack, cybercriminals stalk these websites and manipulate them to insert malicious links and files, and use email registration information to send "phishing" emails that look like they are coming from the trusted website.

Maintaining cyberdefenses

The apparent ease with which cybercriminals are able to infiltrate and capitalize on a company's treasure trove of information and electronic assets is stunning. The fact that it is happening with increasing frequency is reason for concern. However, each event provides cyberexperts with greater insight into how to develop more robust cybersecurity measures to prevent repeat attacks. While there always will be new cyberthreats to address, implementing security protocols that block the path of known cyberthreats is a good start. Here are a few basic protocols to consider:

Passwords. In addition to requiring passwords to gain access to any computer system, a strong password is necessary. Change your password immediately if you think it may have been compromised, but do not reuse a password from another account. If your company can support two-factor authentication, use it.

Encryption. Encrypting data while it is resting on your network and while in transit to third parties is an effective strategy in combating unauthorized access to that information and may serve as a safe harbor in the event that you lose control over the data in your possession.

Limit access to information. Chances are your company's human resources records are off limits to most employees because of the sensitive nature of the information contained in those records. Similarly, you should limit who has access to all sensitive information.

Monitor the flow of information. While there may be a legitimate reason for a significant uptick in the amount of data leaving the company, it also can serve as an indication of a cybertheft. Comparing the ordinary usage of employees over time will allow spikes in data transfers to stick out and trigger an investigation.

Payment card information. While maintaining customer payment information on your computer network is a convenient way to speed up payments, it presents a risk that needs to be managed. If you can do so, avoid saving payment information on your computer system. However, if you do save this information, it needs to be encrypted and restricted to those employees who handle payments.

Payments to third parties. Given the risks presented by social-engineering fraud, it is imperative to verify wire-transfer payment requests verbally with the third party receiving the money. Blindly issuing payment to a third party by way of a new bank account is not prudent.

Software patches. Software can be expensive. However, using pirated software that cannot receive security patches can be more expensive than buying it in the first place. Just ask those companies affected by the WannaCry attack. Even companies that have legitimate versions of software, but do not regularly update their systems, are vulnerable to attack, so activate automatic software updates.

Business vs. personal internet use. Internet shopping, social media and personal email accounts all present a path that cybercriminals can take to access your network. Encourage employees to segregate their internet usage and only use personal devices to conduct personal business to prevent infected, nonwork-related attachments from becoming the next attack on your network.

Takeaway

Having a plan to protect data and to respond to the loss of data will help your agency weather the next cyberstorm. For the plan to succeed, there needs to be a corporate culture of cybersecurity, education and regular reassessments of whether the plan needs to change to address new threats.

Voses is a partner in the New York City office of Kaufman Dolowich & Voluck LLP. He serves as the chair of the firm's Data Privacy Liability and Technology Services Practice Group. Reach him at (212) 485-9962.