Published in: JOURNAL OF ACCOUNTANCY

AICPA® Professional Liability SPOTLIGHT

March 2017

The armor of awareness

By Sarah Beckett Ference, CPA

Trojan horses, spoofing, spear-phishing ... these terms seem better suited to medieval warfare than the everyday cybersecurity lexicon of a CPA firm. While the jargon may sound similar, two contrasts can be found between medieval times and today's cybersecurity threats. The victor of medieval warfare was generally decided after a key battle, the winner taking all. In modern times, cyberattackers adjust their approach after defeat and return with successive attacks, each with a greater level of sophistication than the last. In medieval warfare, fighting was left to the soldiers while the citizenry remained safe behind castle walls. Defense against today's rapidly evolving cyberattacks on a CPA firm's fortress requires more than the IT cavalry. It requires every citizen to don armor and carry a shield to help keep attackers at bay and the CPA firm's confidential data safe.

Fortunately, every citizen has his or her own armor to help defend the firm against a cyberattack. This armor is not expensive and does not require a degree in IT to wear. In fact, most CPAs probably have this armor readily available and are well-trained in using it. It is the armor of awareness.

To help strengthen your armor of awareness and create a contemporary fortress unlike anything known in medieval times, we describe three types of typical data security battles confronted by CPA firms in the AICPA Professional Liability Insurance Program (the Program).

HAST THOU SEEN MY LAPTOP?

Or thumb drive? Or smartphone? Or tablet? Or [insert name of small, transportable media storage device]? While cyberattacks perpetrated by overseas crime syndicates make for attention-grabbing headlines, a significant number of data security incidents are due to lost or stolen media devices. When these devices are stolen from cars or from airport security lines, the thief is generally after the device itself, not the information contained therein. Nevertheless, notification to clients of the potential exposure of their confidential information may be required. Depending on the type and amount of data maintained on the device, this can be very costly.

The tale

Consider this example: A sole practitioner's office was burglarized, and the thief made off with the practitioner's unencrypted laptop. The CPA employed several controls over the firm's data, including regular backup of data to a separate server and using a portal to allow for secure transmission of client information. Unfortunately, a fraction of the CPA's clients had sent sensitive tax data for themselves and their employees to the CPA via email, and this information was stored on the laptop in email folders. In the end, the CPA was required by state law to notify 1,800 individuals that their confidential personal information was exposed.

The lessons

Be mindful of the physical security of mobile devices. A car's back seat is not a good place to keep a laptop. Lock up or otherwise secure and store devices when they are left unattended, even if you are just leaving the office for lunch. Mobile devices are attractive targets for thieves because they are, well, mobile. In addition, encrypt your devices. While encryption is not a "get out of the dungeon free" card, some state laws include a safe harbor that waives breach notification requirements if data are encrypted. Consultation with an attorney is suggested to understand applicable requirements. Finally, limit the type and amount of data stored on a digital media device to only those that are necessary to deliver services. Before a client gives you his or her confidential data, pause and ask yourself, "Do I really need this level of data?" If not, ask the client to redact sensitive information.

GO PHISH

Phishing, whaling, and spear-phishing are all forms of social engineering in which a message, typically an email, with a malicious attachment or link is sent to a victim with the intent of tricking the recipient to either open the attachment or click on the link. If the victim takes the bait, malware is downloaded; the attacker gains a foothold into the firm's systems and can pursue various nefarious activities. According to the 2016 Data Security Incident Response Report published by BakerHostetler, a law firm, phishing/hacking/malware attacks represented 31% of 2015 incidents managed by the law firm and were the leading cause of data security incidents. Data security incidents for CPA firms in the Program reflect a similar trend. This increase is not surprising. Phishing is one of the easiest ways to gain access into an organization as unsuspecting individuals continue to fall prey to this scheme.

The tale

A CPA's computer was infected by malware downloaded to the employee's computer after the employee clicked on an infected internet link included in a benign-looking email. The malware was designed to capture keystrokes and mouse clicks entered by the

continued...

CPA into the internet browser. The CPA processed payroll for clients using an internet-based payroll service. Using the malware, the hacker obtained the CPA's login credentials for the payroll provider's website and added fictitious independent contractors and payment amounts to a client's payroll. When the CPA processed payroll for the client, he unknowingly made fraudulent payments to the hacker. Several hundred thousand dollars was diverted from the client to the hacker before the scheme was detected. The client brought a claim against the firm for its loss.

The lessons

The sophistication of phishing emails is rapidly increasing, so hypervigilance is critical. Approach any email from an unknown source with suspicion. Red flags may include:

- A mismatched URL whereby the actual hyperlinked web address does not match how it appears in the email (hover over the link to see this, but do not click on it);
- Use of poor spelling or grammar;
- Use of urgent or threatening language;
- Suspicious domain names in email headers;
- Requests for personal information; or
- Offers that seem too good to be true.

Even if the email is from someone known to the CPA, be alert if the communication style, information requested, or mannerisms differ from expectations. The person's email could have been hacked. CPA firms should regularly train employees (and then train them some more) regarding the existence of phishing scams and potential red flags. In addition, firms should consider an email filtering system to identify and segregate suspicious emails before they even reach an employee's inbox.

TO ERR IS HUMAN

In the throes of busy season, mistakes can easily be made. Many data security incidents can be attributed to misdirected emails or documents lost in the mail.

A final tale

A midsize CPA firm prepared several partnership returns for a client. Client copies of the returns were mistakenly sent to the wrong email recipient, who viewed the names and Social Security numbers of the partners included on the forms. The firm told the affected individuals of the mistake and offered credit-monitoring insurance. One of the individuals was very upset and threatened litigation.

The lessons

Handle all sensitive information with care. Double-check, or even triple-check, the accuracy of the intended recipient when sensitive information is transmitted. Better yet, help prevent errors by requiring all sensitive data to be transmitted to and from the client via a secure portal. Help prevent items from being lost in the mail by using a traceable delivery method. Encrypt or password-protect files and devices that are sent.

Sarah Beckett Ference (sarah.ference@cna.com) *is a risk control director at CNA.*

To learn more about the AICPA Professional Liability Insurance Program, please visit cpai.com or call 800.221.3023

CNA AON