DON'T BITE – RESIST THE LURE OF PHISHING EMAILS

As law firms continue to go "paperless" and email communication becomes the norm, there is an increased risk for fraud and malicious activity. Although we all appreciate the efficiency of email, there are significant risks that a law firm faces in the digital age. One of those risks is the ability of bad actors to gain access to the firm's network and client records through phishing emails. Phishing emails by nature are designed to cast a wide net and "trick" the user to click on a malicious link. Such links might then provide access to the firm's network, enabling the hacker to search for potential administrative passwords and/or to gain access to other networks. Other phishing links might trick the user into providing administrative passwords directly to the bad actor.

"Spear fishing" is a more sophisticated, targeted attack directed towards individuals involved in specific activities within the organization. For example, the bad actor may target employees in payroll, human resources, IT or finance. These employees typically have greater access to the firm's network or administrative capabilities and may also be in possession of Personally Identifiable Information ("PII") or Protected Health Information ("PHI"). The intent is to access and monetize the data.

EXAMPLE

A law firm employee receives a phishing email from a source who appears to be their court reporter vendor. That employee clicks on the link to download their recent invoice for payment. The employee receives a pop-up indicating they must update their Office365 in order to access the vendor invoice. The employee follows the prompts and enters their username and password. Unbeknownst to the employee, the bad actor now has access to their credentials and their Office365 account. Further, the employee may have inadvertently downloaded malware allowing the bad actor access to the firm network.

THE IMPACT OF PHISHING

The repercussions of just one employee clicking on a phishing email can be devastating. In addition to monetary loss, such activities can negatively impact client relationships due to a loss of confidence in the firm. The employee may or may not realize what has just transpired and the firm may not recognize the breach until they see unusual activity on their network. This could come in the form of ransomware, social engineering fraud where they pose as a vendor or other business partner, or notice from clients of unusual communications from the firm.

The bad actor, now having access to a firm's entire email directory, may decide to initiate a secondary phishing scheme directed to all clients utilizing the firm's trusted email domain to infiltrate client networks. If client networks are impacted, this may expose the firm to third-party claims from those clients. Further, if the bad actor was able to transmit malware through the link, the firm may lose access to their entire network and receive a monetary demand/ransom in order to regain access. With the threat of missed deadlines and statutes of limitation, this network shutdown could be a catastrophic event for a law firm – and one that creates an E&O exposure for future malpractice claims.

NEXT STEPS AND LESSONS LEARNED

Should the bad actor gain access to client files there are a multitude of regulatory and ethical rules which need to be evaluated. Further, depending on the breach and type of data viewed or exfiltrated, each client may need to be directly notified of the incident in conjunction with state, local, and even international regulatory authorities.

The regulatory landscape for privacy law is dynamic and constantly evolving. In this heightened environment, and considering the high risk associated with a breach to a law firm, it is important for a firm to evaluate their network security and risk management associated with a potential breach. A cyber/privacy insurance policy is an effective way to help reduce and effectively manage this risk. Most privacy/cyber policies provide both first-party (breach consultation/breach response coverages) and third-party claim coverage which help control costs and impact to the law firm should a privacy breach or network security attack occur.

Some insurance carriers also provide proactive risk management services that help firms enhance their cyber security readiness and incident response capabilities. Some offer access to customized phishing exercises with assessment, reporting, behavior trends and user metrics that help educate staff and train them to be more diligent and less apt to fall for phishing schemes.

AUTHOR

Erika Nelson
Assistant Vice President, Cyber Claims Response Team
North American Claims Group

QUESTIONS? Contact your local Allied World Underwriter. **alliedworldinsurance.com**