Alta Pro Insurance Services

Law Office Cybersecurity Best Practices 2021

March 23, 2021
12 Noon CST
1.0 Hour CLE Webinar

Presenters
James Davidson, O'Hagan Meyer Attorneys & Advisors
Nathan Little, Tetra Defense

Contents

1. Ethical Duty of Technical Competence

ABA Model Rule of Professional Conduct 1.1 Comment [8]: *"Maintaining Competence: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology ...."*

2. Cyber Risks Have Soared During the Pandemic

- Cyber crime has skyrocketed since February 2020.
- There has been a 75 percent increase in daily digital crimes since lockdown began. (*FBI Internet Crime Complaint Center*)
- More than 200,000 newly registered fraudulent websites and malicious domains – many designed to mimic official public websites, government portals, banks and other targets – were identified by Interpol's Global Malicious Domain Taskforce in June 2020.
- Nearly 140,000 reports of online retail fraud were made to the US Federal Trade Commission from January 1 through June 30, 2020 – almost as many as in all of 2019.
- More than 570,000 reports of identity theft were made to the FTC in that same period—also almost as many as in all of last year—as "criminals took advantage of the unfolding economic downturn and people's general anxiety about the pandemic to exploit them for their personal information, credit-card numbers and banking details." (The Economist)
- New social engineering and email phishing scams exploit fear and confusion about COVID, vaccines, economic concerns, Paycheck Protection Loans, etc.

- A remote workforce brings new risks.

3. Law Firm Data Breach Case Studies

RANSOMWARE ATTACK

Description. A mid-sized hospital network was the victim of a ransomware attack that caused an initial almost complete lock down of its data. In order to remain in operation, IT forensics had to work immediately to quarantine the virus, but also work to ensure that the unencrypted data and systems were operational. Accordingly, the Provider was required to rent extensive network and temporary equipment. Further, the Provider was required to route certain work, such as ER services and reading of x-rays and MRIs to other local providers. The Provider not only incurred restoration of data costs, but also needed privacy counsel to advise as to HIPAA and other reporting obligations. Further, the Prover experienced substantial business interruption losses.

Losses:

Privacy counsel - $30,000.00
Forensic IT and Data Restoration - $55,000.00
HIPAA Notification Expenses - $35,000.00
Business Interruption/Lost Income - $150,000.00

FRAUDULENT FUNDS TRANSFER LOSS

Description. A real estate agency was also in the business of buying properties, quickly restoring and updating the properties and "flipping" the homes for a substantial profit. An administrative assistant received an e-mail purporting to be from the CEO of the agency, asking that $275,000.00 be wired from the agency's account for a closing for a new home the agency intended to purchase and flip. The e-mail address was the actual address of the CEO. The assistant responded and had the funds wired as instructed. The wire instructions were fraudulent. This fraud was the result of an e-mail breach wherein the hacker had access to the CEO's e-mail account and was able to set up a rule so that all e-mails on this topic went to a folder that only the hacker could see.

Losses:

Fraudulent Funds Transfer Loss - $275,000.00
Forensic IT analysis of E-mail Breach - $27,500.00

OFFICE 365 DATA BREACH

Description. A small accounting firm had its e-mail system breached via a phishing e-mail that allowed the hacker to have access to an assistant's e-mail account and Office 365 account. The accounting firm handled many private client tax returns and exchanged financial information and draft returns via unencrypted messages. A review of the assistant's

Outlook account revealed that the hacker had access to the account for a period of 14 days during tax season and hundreds of clients personal and financial information was at risk.

Losses:
Privacy Counsel - $40,000.00
Data Breach Expenses - $30,000.00
Notification Cost: $10,000.00
Credit Monitoring Costs: $10,000.00

WEBSITE VIRUS

Description. A financial management firm had a virus infect its system wherein any e-mail that contained a link to the company's website was being blocked by the recipient's spam filter. This was caused by a virus infecting the firm's website seemingly only for the purpose of mayhem and chaos. The firm lost clients and had to notify all receipts of the e-mails that did not get caught by a spam filter that if they opened the e-mail, the virus could have affected their computer or system. There is the potential for resultant third-party claims if the recipients' systems were damaged.

Losses:
Data Breach Expenses - $40,000.00
Notification Costs - $5,000.00

EMPLOYEE LOST AND STOLEN LAPTOP AND MOBILE PHONE

Description. A mid-sized office supply company performed month-end financial reports which included customer information, account information, financial information and information regarding bank accounts and wire information. The information was distributed to several employees, one of which had a personal laptop and mobile phone stolen. In conjunction with IT, but without discussing with the company, the employee was given access to e-mail on his personal laptop and mobile phone. Neither of which required multi-factor identification, no encryption and ability to bypass passwords if sessions were active.

Losses:
Privacy Counsel - $45,000.00
Notification Costs - $20,000.00
Credit Monitoring - $30,000.00

(Source: O'Hagan Meyer)

4. Best Practices for Law Firms

- **Develop a Cyber Policy and Educate Employees.** Do not just make this a bullet point in an employee handbook handed out to new employees. Regularly train employees on cyber and data security issues.
- **Have a Specific Policy for Wiring Funds or Sending Money.** For law firms and any business that routinely wires funds, a policy of verifying the instructions via a phone call should be mandatory for anything over a small amount (i.e. $1,000.00). Further, an instruction on an e-mail to clients that they should call and verify any change in payment/wire instructions they receive should be made. Further, if you're depositing a large check in a Trust Account with the funds to then be wired out, require that the funds actually clear before they leave the Trust Account.
- **Have a Specific Policy about Opening Links from Unknown Sources.** Employees simply should not click on a link in an e-mail from a third-party source without first either verifying the e-mail is legitimate or showing it to IT. No employee should ever provide credentials such as a password or username in such an instance.
- **Consider a Personal Use Internet Policy (or Enforcing the Policy you Have).** Besides being a drain on productivity, employee internet surfing can lead to cyber attacks. Some law firms have prohibited personal internet use other than Westlaw or Lexis and have dedicated computers that are not on the Firm's system for employees to use on their breaks.
- **Have a Cell Phone and Personal Computer Policy.** Performing work functions on cell phones and a personal computer that has not been vetted and approved by the company's IT can be dangerous. For example, a stolen mobile phone could contain significant client confidential information if the individual uses that mobile phone for work e-mail. Multi-factor identification discussed below can be helpful.
- **Enact a Combination of Firewalls and Data Encryption.** Understanding your IT protection and options is key. For many of the next several points, understanding what your in-house or third-party IT and data host provider is doing to protect your data and network is essential.
- **Have your IT Explain its Back-Up Procedures.** Too often in catastrophic ransomware attacks specifically, a business learns that its data has not been properly backed-up, or that the back-up is so closely tied to the server that it is too encrypted. Putting your IT company to the test *before* an event can make life much easier when an event occurs.

- **Make Sure all Virus and Anti-Malware Software is up to Date.** Do not be afraid to spend on the front end to prevent an attack.
- **Have a Password Policy.** Over 60 percent of data breaches are a result of weak or stolen passwords. Many employees never change the dummy password they are given at the start of employment (i.e. "1234"). Further, employees often save or write passwords in public places, such as putting them on a sticky note on their computer screen or desk. Require frequent password change, make sure the original dummy password is changed and make this a topic of conversation.
- **Establish a Laptop and Mobile Device Policy.** This is especially important for non-company issues devices ("BYOD"). Require password protection, multi-factor identification and current software and antivirus protection.
- **Multi-Factor Identification for Remote Access.** Hacker intrusion through remote access portal is high. Any employee that is working in a system remotely should be required to go through a multifactor identification process.
- **Understand Policies of Companies Who Store Data or Who You Share With.** It does no good to have strict data and cyber policies if you use a third-party host that is not careful, or if you share sensitive information with unsafe recipients.
- **Consider Spending on Annual Penetration Testing.** Many forensic IT companies offer services where the company network and e-mail are tested to highlight vulnerabilities and then offer solutions to "close the holes."

(Source: O'Hagan Meyer)

5. What We're Seeing: Cyber Incidents

Ransomware. This form of malware allows a threat actor to encrypt data, then demand payment for said data in the form of cryptocurrency. It poses a threat to organizations of all shapes and sizes. This cyberattack has significantly increased the scope and impact of cybercrime for previously unaffected organizations.

The threat landscape. Ransomware groups have managed the reputational fallout of their activities by referring to themselves as benevolent security crusaders. Their victims are referred to as "clients" who are now in business with creators of the "best" decryptors available. These groups operate with the structure of a proper business.

Misuse of legitimate tools. Both ransomware and BEC threat actors are continuing to use legitimate Remote Access tools and Security tools in their attacks.

- Remote Management Tools (RMM)
- Cobalt Strike / Cloudflare
- Remote Desktop Protocol (RDP) connections available on the public Internet

To protect against these attacks, safe remote access, safe authentication measures, and proper backup practices should be in place.

Business email compromise. Under the guise of false pretenses, Business email fraud can lead to major damage. BEC is comprised of several deception methods, and often for several different motivations from a threat actor's perspective (to perform wire transfer fraud, collect classified information, etc.)

(Source: Tetra Defense)

6. How to Strengthen Defenses

There are often inexpensive, preventative measures that can thwart some of the most prolific cyber attacks. We recommend the following to start strengthening your defenses today:

ENSURE SECURITY OF REMOTE ACCESS AND WORK FROM HOME TOOLS. Windows RDP should not be used as a main source of remote access without a Virtual Private Network (VPN) or multi-factor authentication (MFA).
LIMIT SERVICES FACING THE PUBLIC INTERNET. There must be a schema/rationale for determining what services can access the public internet. Leverage firewalls and other tools to determine external exposure to the public internet.

ENABLE MULTI-FACTOR AUTHENTICATION. MFA should be utilized to protect all user accounts, but especially accounts with administrative privileges.
DEPLOY ANTI-MALWARE. Endpoint protection should be installed on all workstations and servers, as well as be continuously monitored.
VERIFY BACKUP FREQUENCY, SECURITY, & RELIABILITY. Cloud backups should be secured with MFA and regularly tested at a rate of more than once per day.