The Staggering Cost of Law Firm Data Breaches: Protecting Your Firm

By Michael C. Maschke, Sharon D. Nelson, Esq. and John W. Simek

As we begin 2025, attorneys hope the new year brings them happiness, health, and prosperity. One situation every law firm wants to avoid this upcoming year is a cyber incident or, worse, a data breach. Not all cyber incidents are data breaches, but cybersecurity protections should be implemented to protect your firm's information and confidential files.

Keeping attackers out of your information systems has become more challenging than ever. Cyber threats have become more sophisticated, harder to detect, and much more expensive to recover from. According to Thomson Reuters, in 2024, the average cost of a data breach reached $4.88 million. That cost alone may sink some law firms, especially those which are under-insured. Understanding the actual cost of a data breach will only help firms realize the critical importance of maintaining current cyber security measures.

Data Breach Defined

A data breach is a security incident in which unauthorized individuals gain access to sensitive or confidential information, like personal data (Social Security numbers, bank details) or corporate data (customer records, intellectual property), due to a lapse in security measures, often through hacking or human error. Essentially, it's when private information is exposed to people who shouldn't have access to it.

Data breaches can occur in many ways, including phishing attacks, malware, ransomware, and insider attacks. They can result in identity theft, financial fraud, reputational damage, and possibly legal action. Class action lawsuits are proliferating with frightful speed.

Phishing attacks are more sophisticated than ever, and when combined with AI, they can get through email protection filters and steal users' credentials (these are called Business Email Compromise attacks).

Current ransomware, the data exfiltration version, continues to plague law firms by requesting two ransom payments: one to decrypt and another to return "stolen" data.

Exploiting vulnerabilities of dated, unpatched systems allows attackers to access the infected system and move laterally within the network, evading detection by common standard cybersecurity measures.

Lastly, the disgruntled former employee must not be forgotten, as sometimes they can cause far more significant damage given their intimate knowledge of the firm's technology.

The Financial Impact: It's Often Brutal

There are some obvious costs associated with data breaches. First, there is the immediate reaction and incident response. You may have expenses with information technology vendors, cybersecurity consultants, and digital forensics investigators to understand what happened, the scope of the attack, and what confidential data may have been accessed or stolen.

Business continuity costs—The expenses relating to the recovery and restoration of your systems can be expensive, depending on the number of infected endpoints and the complexity of the technical environment. Getting your business back up and operational is key to surviving a data breach. An immutable backup (backups that cannot be changed or deleted for a specified period of time) you can restore from is the #1 antidote to recovering from the venom of a cyber-attack such as ransomware.

Depending on the scope and severity, law firms are now facing regulatory fines for violating state data privacy laws, on top of the threat of a class action lawsuit. Retaining legal representation to defend against these additional actions can be astronomical and is another cost to add to the heaping pile of expenses due to a data breach.

Lastly, and the hardest to measure, is reputational damage. How many clients were lost due to the breach? How many potential clients took their business elsewhere? How many employees have left your firm, and are you finding replacing them with good talent more challenging? These are all data points that we hope you never have to measure.

You can reduce your firm's risk of experiencing data breaches in several ways. While no combination is 100% effective, every little bit helps. Mandatory cybersecurity awareness training, having a good cybersecurity posture, risk management controls, proactive monitoring for cyber incidents, and following cybersecurity best practices for small businesses such as NIST (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf) or CISA (https://www.cisa.gov/cyber-guidance-small-businesses) guidelines are great ways to start 2025 on the right path toward an incident-free year.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), a Certified Ethical Hacker (CEH), and a nationally known digital forensics expert. He is a co-author of 18 books published by the ABA. jsimek@senseient.com*