Catastrophic Breach of a Law Firm and a County Office

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

Another week and another data breach hit the press with thousands of victims' medical records accessed by attackers. Bassford Remele, a Minnesota-based law firm, announced that it had experienced a data breach starting last summer. According to the breach notice on its website, between July 29, 2024, and September 4, 2024, an unauthorized party may have accessed and potentially compromised sensitive personal information in its systems. It's unclear what type of information was accessed.

However, according to the notice, certain information provided by healthcare organizations to which Bassford Remele provides legal services may have been accessed, including Social Security numbers and medical record information. Notices have been sent to the affected individuals. It appears that the breach was detected when Bassford Remele discovered that unauthorized emails had been sent from a third-party application purporting to be from an employee's email account.

Also recently in the news, Scott County, Iowa, confirmed that an employee's email was accessed, exposing medical records, Social Security numbers, and other patient data for over 4,300 victims.

The ongoing alert of data breaches will indefinitely continue, keeping many partners and firm managers up at night.

This is a good time for a few recommendations on steps that firms can take immediately to improve their email security posture, with recommendations for Microsoft 365 and Google Workspace, which was likely the attacked environment for both reported incidents (and most attacks nowadays):

1. **Enable Multifactor Authentication on all email accounts and make it a requirement for access.** Even if an attacker has a user's credentials, they wouldn't have the second factor needed to access the account through the browser. While there are a few MFA methods, having users select Authenticator with push notifications is the best option moving forward. Due to security concerns, vendors are starting to eliminate the SMS/Text code option.

2. **Enable Conditional Access Policy for account logins with Microsoft 365.** This security feature is included if you have a 365 E3 or higher subscription level. If you have a lesser subscription level, you must purchase Microsoft Entra ID P1 licenses for your users to gain access to this feature. It allows fine-grained access control

measures to be set for authenticating users to grant access for resources such as mailboxes, sensitive data, and applications. Options include requiring device security compliance, the location of the originating request from an approved area and indicating whether the user is on a home or office network.

3. **Turn on event auditing in Microsoft 365 or Google Workspace.** This will enable investigators to view the activity performed or files and records accessed while an unauthorized user is logged into the mailbox or account. It takes up to 60 minutes for the changes to take effect. Administrators can search the audit log to view user and admin activity, with numerous filters available to fine-tune the searches. Audit logs help to track document access and demonstrate compliance, as well as mailbox activity.

4. **Integrate a Security Information and Event Management (SIEM) solution with your cloud-based email environment.** In short, a SIEM is a cybersecurity solution that collects, analyzes, and correlates data from various sources within an IT environment to help organizations detect, investigate, and respond to security threats. SIEM agents should be pushed out and installed on all endpoints, including desktops, laptops, and servers. A comprehensive SIEM solution will also be integrated with cloud-based email providers, such as Microsoft 365 and Google Workspace.

   A SIEM is an active security solution, rather than a reactive one, alerting admins and users in real-time to any ongoing cybersecurity threats, control changes, or alerts. Preventing business account takeover attacks or stopping them within minutes or hours, rather than weeks or months, is critical to avoiding or minimizing harm to your clients and firm.

5. **Understand your Microsoft Secure Score.** Microsoft Secure Score is a security analytics tool that provides a numerical value representing an organization's security posture, indicating how well-protected its data is. A higher score means better security. It also tracks your score over time. Microsoft provides recommendations and changes that can be made to improve the score and overall security of your firm's Microsoft environment. You can even filter recommendations for those included with your current subscription level without upgrading to a higher subscription offering.

These are just some of the steps you can take to enhance the security protections of your firm's email environment, and these recommendations only make up a part of your firm's overall security posture. A firm's cybersecurity measures to protect information systems and client data must be regularly reviewed and updated, as cyberattackers' methods and tactics are constantly evolving.

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 holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com*