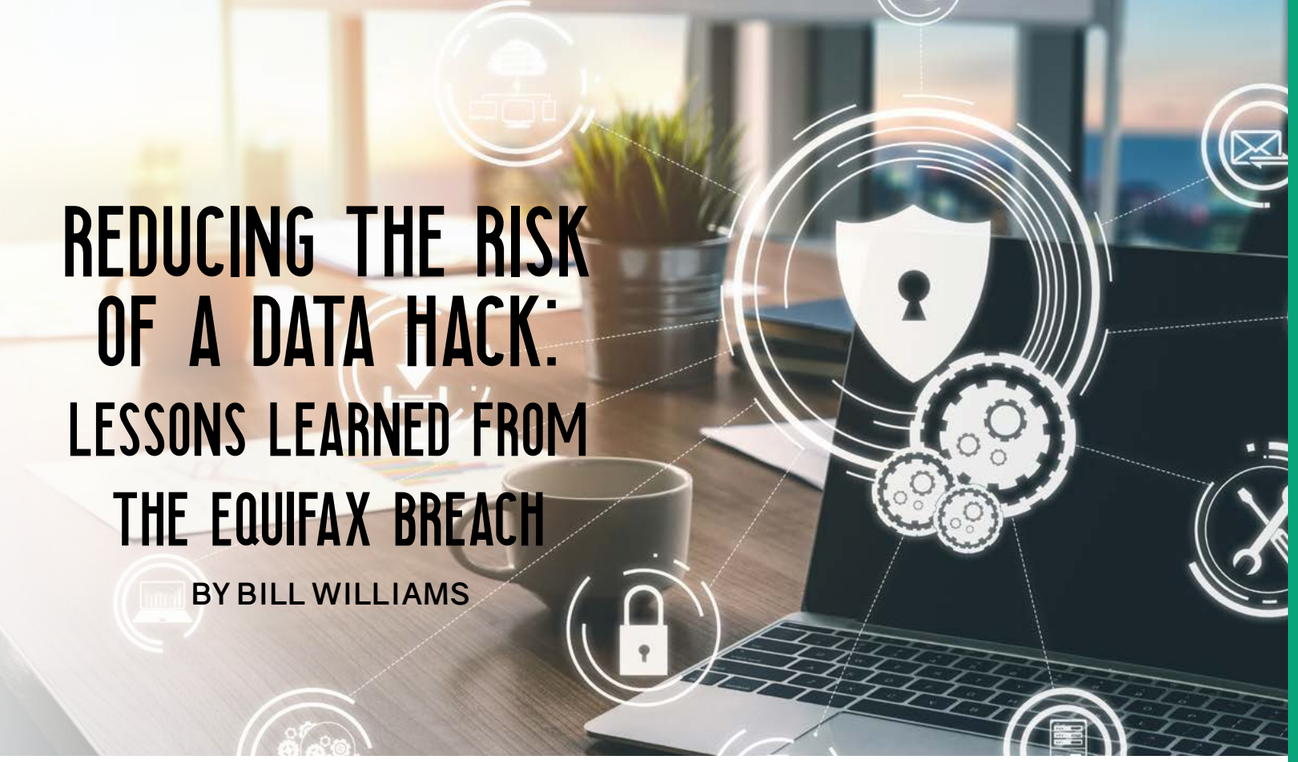

REDUCING THE RISK OF A DATA HACK: LESSONS LEARNED FROM THE EQUIFAX BREACH

BY BILL WILLIAMS

Data breaches are becoming less avoidable than ever before in today's society. Although media coverage is focused on large corporations falling victim to breaches, hackers often target smaller entities because they may have fewer measures in place to protect their data.

Deathcare firms can serve as an ideal target for hackers due to the amount of sensitive information that lies within a firm's files and the potential lack of data protection. While many believe it is a question of when, not if, you are a victim of a data hack, every deathcare professional can take steps to significantly minimize the likelihood of a breach.

One of the best ways to understand how you can protect your sensitive data is reviewing the "lessons learned" from a previous data hack. Recently, our team examined the Privacy Commissioner of Canada's report on the infamous Equifax Inc. breach, which impacted more than 143 million people. The goal was to learn how some of Equifax's security shortfalls before the breach could apply to the deathcare industry, and what practices deathcare firms could implement to avoid the same mistakes.

Before sharing the "lessons learned," I would like to emphasize that similar to Equifax, almost all deathcare firms hold extremely personal client information within their files – which is a gold mine for hackers. If a hacker obtained just one or two of your clients' records, it can be extremely harmful to you and your client's financial health, sustainability and reputation. No matter the level of your security measures, I highly recommend reviewing these findings and considering how you can apply them to your business.

Maintaining Security Certificates

Equifax initially detected the attack once it updated an expired security certificate. In short, security certificates are used to verify the identity of the individual trying to access data. For example, every website you visit must present a security certificate to your browser, which confirms the safety of the website. If the certificate is expired, you will likely receive an automatic warning from your browser.

The Privacy Commissioner's report found that Equifax's expired certificate left it open to a breach and once the update was made, hackers were finally noticed. In fact, Equifax contained the attack the very next day. As it relates to deathcare firms, professionals must ensure security certificates for platforms that hold digital files are up-to-date, especially for their public and client websites.

CONTINUED FROM PAGE 50

Stronger Data Governance
The report also found that Equifax had "poor implementation of basic methods of protection" regarding its data maintenance. It also noted a "clear disconnect between policies and practices" that demonstrated "critical gaps."

For the internal governance of client data, every deathcare firm should have sound practices in place to understand who is saving, modifying and maintaining files – and where – and that usernames and passwords of staff and clients are stored in a secure location. In addition, your firm would benefit from investing time for a professional to train your staff on the appropriate handling of personal information.

If your firm has third parties who manage your client information, ensure that the third party is regularly maintaining the data appropriately and fulfilling its obligations to you. Whether it is your internal staff or a third party, just one mistake or breakdown in communication could lead to a massive breach.

Record Retention and Disposal
Following the breach, Equifax confirmed that while it had a record retention policy in place, it did not have a process to delete certain personal data. Equifax had not deleted any personal information in its systems since 2010. By storing outdated or duplicate files that should have been deleted, you are allowing hackers access to even more information – such as data from previous clients from several years ago.

If you have paperwork or records that are no longer relevant to your business operations, it is highly recommended to properly discard these outdated files so they are no longer vulnerable to a breach. For records that remain relevant, consolidate them into one central, secure location to avoid loose or misplaced documents that might end up in the wrong hands.

Written Agreements for Data Sharing
Within its report, the Commissioner mentioned a lack of formal written arrangements with certain third parties that managed Equifax's personal information.

Specific to deathcare firms, who may often leverage the expertise of trustees, investment advisors or record keepers, it is critical to establish clear parameters, in writing, for how personal client information should be handled. For example, as noted above, the arrangement should clearly state how long the third party can retain personal information until it must be discarded.

Best Data Security Practices for Every Deathcare Firm
In addition to the lessons learned from the Equifax breach, other simple security measures exist that will help deathcare firms reduce the risk of a data hack. Below is a list of some best practices that we encourage you to follow both at home and in the workplace.

Replace outdated software or technology systems -
Hackers often prey on weak and unprotected systems. When you replace your outdated systems and invest in high-quality technology, such as The Cloud, your records are protected at off-site data centers, which offer some of the highest levels of data encryption.

Utilize a variety of complex passwords across all accounts and change them often -
Creating long and complicated passwords for each account can often be tedious; however, this practice can make it much more difficult for hackers to access your accounts. Even if you suffered a hack to one of your accounts, another breach is far less likely if you have a variety of passwords set elsewhere. Many experts suggest changing your passwords as frequently as 30 days. At minimum, we recommend changing your passwords at least every six months. Two-factor authentication may be used as well if you have the capacity to do so.

Be wary of suspicious emails -
Hackers are becoming more sophisticated in their phishing attempts. In a world that is so heavily driven by digital communications, hackers will try to fool you and your employees with fake emails from known associates. Before you open an attachment or click on a link in an email that seems suspicious, read the email address closely to ensure the sender is legitimate. If you identify an email as a phishing attempt, notify your IT office or professional immediately – it is likely that other colleagues have or will receive similar emails.

Limit your "Bring your Own Device" (BYOD) Policy
Allowing employees to bring their own devices to work poses many risks. These risks include, but are not limited to, outside devices lacking firewall protection or anti-virus software, employees leaving your facility with sensitive data on their personal devices and employees using unsecured Wi-Fi with company information on file.

Your company might already provide employees their own computers for business operations only. If your business allows employees to use their own devices for work, then you are putting your company in a vulnerable position. While it is unnecessary to forbid all outside devices, you should consider what type of devices you permit inside your offices.

Take Action Today
It is better to be overprepared and overprotected. In our profession, we place significant emphasis on relationships with our clients and their trust in our services. To maintain and further build our clients' trust, we can take advantage of existing practices to ensure their sensitive data is as secure as possible. As we head into a new decade, which will be even more driven by technology, consider consulting an IT professional or a record keeper to learn the data security resources available to you. **FBA**

Bill Williams is president and CEO of Funeral Services Inc. and serves on the FSI Board of Directors as vice chairman. He joined FSI in 2001 as vice president. He was named president in 2003. Under his leadership, FSI has expanded to offer services in more than two dozen states across the country. Williams has experience in every aspect of the funeral service profession, including ownership and management of funeral homes and cemeteries. He began his career in the deathcare industry when he became a licensed funeral director in 1980. He is a graduate of Gupton-Jones College of Mortuary Science in Atlanta, Georgia. To connect with Bill, call him by phone at 800-749-1340 or by email at bill.williams@fsitrust.com.