Reducing your funeral home or cemetery's risk of a data breach

By: Bill Williams, President and CEO, FSI

Data breaches are becoming less avoidable in today's society. They have the potential to affect every individual and company, even those that seem invulnerable. Although large corporations often experience these incidents - Equifax and Capital One were the latest - doesn't mean you are not a target.

Specific to the deathcare industry, several funeral homes and cemeteries are vulnerable to these types of breaches, especially if they are behind in leveraging the latest technology, trends and safeguards being implemented in other industries.

As data hacks are continuing to increase, FSI has made security a core focus in its day-to-day operations of administration and recordkeeping for deathcare trusts and preneed programs. While our team puts extensive measures in place to protect client data, you can also take steps at your funeral home or cemetery to minimize the likelihood of a data hack. Below is a list of our best practices we encourage our clients to follow at home or in the workplace.

Replace outdated software or technology systems

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 When you replace your outdated systems and invest in high-quality technology, such as The Cloud, your records are protected at off-site data centers, which offer some of the highest levels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

Yes, 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 also recommend changing your passwords as frequently as 30 days. While that may be too often to maintain, FSI still recommends changing your passwords at least every six months. Two-factor authentication may be used as well if you have the capacity to do so.

FSI
TRUST SOLUTIONS

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 other colleagues have or will receive similar emails.

Delete old, irrelevant records and consolidate remaining assets
You may have paperwork or records that are no longer relevant to your business operations but include sensitive information about your business or clients. These records may not be maintained well or are currently saved or sorted in various locations. In this situation, it is recommended to delete or shred these old files so they are no longer vulnerable to hackers.

If you uncover old records that remain relevant to your business, consolidate those files into one central, secure location to avoid loose or misplaced documents that might end up in the wrong hands.

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 with access to business data.

Educate Your Employees
"You are only as strong as your weakest link." While cliché, this phrase carries a lot of truth when it comes to keeping your company's data safe. Once you understand how to implement these measures, you should educate the rest of your team to ensure your data is as secure as possible at all levels of your business.

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 resources and practices to ensure their sensitive data is as secure as possible.

Bill Williams is president and CEO of Funeral Services, Inc. (FSI) and serves on the FSI board of directors as vice chairman. He can be reached at Bill.Williams@FSItrust.com.