[TECHNOLOGY

By Welton Hong]

Cemetery Cybersecurity

Best Practices for Protecting Sensitive Information

Cyberattacks pose a risk for just about everyone, dead or alive.

Even the deceased have been targeted by hackers. Ever heard of ghosting? No, not when someone abruptly ends communication in a friendship or romantic relationship. I'm talking about the phenomenon when cyberthieves steal the identities of people after they die – also referred to as ghost hacking.

Nothing and no one these days is immune to digital threats, not even final resting places and the people who occupy them. Not even you.

If you've ever gotten an email that your account will be deactivated or a package you weren't expecting can't be delivered unless you provide some personal information like, say, your credit card number, you've been targeted, too.

There's a target on everyone's back, and 2023 represented an all-time high for data compromises reported in the U.S. – with the majority being cyberattacks, according to the Identity Theft Resource Center's 2023 Data Breach Report.

Data breaches affect more than just the large corporations you hear about on the news; your cemetery is at risk, too.

I'll walk you through why cybersecurity is so important for cemeteries specifically, some forms of digital threats you might encounter, and a few key things you can do to safeguard your cemetery and the families you serve.

WHY IT MATTERS

Cemeteries typically aren't the first businesses to come to mind when thinking of cybersecurity – industries like health care and financial services are certainly more obvious choices. I mean, how many people think of data protection as a determining factor in choosing a final resting place for their loved ones?

In all honesty, they probably should.

From social security numbers to relatives' names to the cause of death, a lot of their personal information is in your hands.

What I'm getting at is the primary reason cybersecurity is so critical for cemeteries is to protect clients' sensitive personal information. Data breaches can lead to identity theft, fraud, and violation of privacy.

Then, there's the money to consider.

Cemeteries handle significant financial transactions related to burial plots, maintenance services, and donations. Cybersecurity measures are essential to prevent financial fraud, such as unauthorized transactions or manipulation of financial records. Protecting financial data not only safeguards the cemetery's assets but also ensures the financial security of its clients.

While the clients you serve are your top priority, protecting this data is critical for you, too. Failing to do so could have serious consequences.

Many jurisdictions have stringent regulations regarding the handling and protection of personal and financial data. If cemeteries don't comply, there could be legal repercussions, including fines – not to mention damage to your reputation.

The reputation of a cemetery is based on its perceived integrity and the respect it shows to the deceased and their families. A cyberattack that compromises personal data or disrupts operations can severely damage a cemetery's reputation, leading to a loss of trust among the community and potential clients.

From legal fines to loss of profit from reputational damage to paying a ransom to get back online (less likely, but still possible), not protecting yourself from cyberattacks could directly or indirectly hurt your bottom line.

WHEN YOU'RE UNDER A CYBERATTACK

Imagine going into the office one day and sitting down in front of your computer only to realize you have zero access to your cemetery management software. You can't pull up old records or current files; for all intents and purposes, the business side of your cemetery no longer exists.

This is just one of many scenarios that could play out if you don't protect your technology.

A cyberattack can come in many forms, and they shapeshift every year. I'll walk you through a few you might encounter.

Phishing: Check your email with caution. Phishing attacks involve deceiving individuals into revealing sensitive information or downloading malware through seemingly legitimate communication, such as emails or messages. Cemeteries might be targeted

Ghost Hacking:

The phenomenon when cyberthieves steal the identities of people after they die.

through emails pretending to be from legitimate suppliers or regulatory bodies, tricking staff into providing access credentials or financial information. This information can then be used for unauthorized access, data breaches, or financial fraud.

Hacking: Hacking isn't reserved for the movies; it's real. It encompasses unauthorized access to or manipulation of computer systems and networks. Attackers may exploit vulnerabilities in the cemetery's digital infrastructure to access sensitive data, disrupt operations, or even alter financial records.

Ransomware: It might seem unlikely, but someone can hold your business for ransom. Ransomware is a type of malware that encrypts files on the victim's system, demanding payment for their release. For cemeteries, a ransomware attack could mean losing access to critical operational data, such as burial records, financial documents, and maintenance schedules, potentially halting operations.

Virus: You're probably familiar with the concept of a computer virus. But what it is, is malicious software designed to replicate itself and spread to other computers, often damaging files, stealing data, or causing system malfunctions. Viruses can enter cemetery systems through email attachments, downloads, or compromised USB devices. So always think before you click!

Spyware: Spyware is a lot like it sounds. This software secretly monitors and gathers information from a target computer system. For cemeteries, spyware could be used to collect sensitive information about operations, financial data, or personal details of the deceased and their families. This information could then be exploited for identity theft, financial gain, or even competitive advantage.

Identity theft: Identity theft involves the unauthorized collection, use, or misuse of personal information to commit fraud or other crimes, often without the victim's knowledge. In the context of cemeteries, the deceased and their relatives' personal information can be particularly vulnerable. This is where ghosting, or ghost hacking, comes into play. Cybercriminals may target digital records to extract sensitive data, such as social security numbers, addresses, and birthdates, which can then be used to open fraudulent accounts, obtain credit, or commit other forms of identity fraud. This violates the privacy of the individuals involved, and can lead to significant financial and emotional distress for the families.

HOW TO PROTECT YOUR TECH

Now that I've sufficiently warned you of the dangers of a cyberattack, I should probably give you a few pointers on how to actually prevent one.

Don't worry, it's not as complex as it sounds.

But if you do feel like some of the cybersecurity strategies mentioned below are a little out of your realm, don't be afraid to consult experts. A professional can certainly help you develop a cybersecurity strategy to ensure your cemetery never makes the local news – at least not over a data breach.

Regular risk assessments: A good

first step is identifying what exactly is at risk. Cemeteries should conduct regular risk assessments to identify potential vulnerabilities in their systems. This involves evaluating your digital infrastructure, from databases to websites, and identifying where you're most vulnerable to cyberattacks.

Software installation: Invest in some reputable antivirus software to prevent virus infections, and antispyware tools to guard against spyware infiltration.

Implementing strong access controls: Access to sensitive information should be restricted to authorized personnel only. Strong access controls, including the use of multi-factor authentication and regular password updates, can significantly reduce the risk of unauthorized access. Role-based access control can further ensure individuals only have access to the information necessary for their roles. Make sure a virtual private network (VPN) is in place for any remote company network access. Establish endpoint protection on every device that has access to the company network and domain name system (DNS) security on every device connected to the company network.

Encryption of sensitive data: Encrypting sensitive data, both at rest and in transit, is a crucial measure to protect against unauthorized access. Encryption ensures that even if data is intercepted or accessed by unauthorized individuals, it remains unreadable and secure.

Regular software updates and patch management: Cyber threats are constantly evolving, and attackers can exploit software vulnerabilities to gain unauthorized access. Make sure a firewall is in place and updated regularly. Regular updates and patch management are essential to fix vulnerabilities and protect against the latest threats.

Employee training and awareness: Human error is often the weakest link in cybersecurity. Training employees on the importance of cybersecurity, recognizing phishing attempts, and following best practices can significantly reduce the risk of successful cyberattacks.

A cyberattack that compromises personal data or disrupts operations can severely damage a cemetery's reputation …

Backup and disaster recovery plans: While I hope your cemetery never comes under cyberattack, it never hurts to have a backup plan for the worst-case scenario. Cemeteries should establish robust backup and disaster-recovery plans to ensure they can recover data and restore operations in the event of a cyberattack. Regular backups, preferably stored in a secure, off-site location, can prevent data loss and facilitate the recovery process. •

Welton Hong *is the founder of Ring Ring Marketing and a leading expert in creating case generation from online to the phone line. He is the author of "Making Your Phone Ring with Internet Marketing for Funeral Homes." He can be reached at Welton@ringringmarketing.com.*