

Six Tips to Help Safeguard Data During the Work-from-Home Era

By Bill Williams, president and CEO, Funeral Services Inc.

The coronavirus pandemic and the subsequent work-from-home mandates have brought many changes to the way death-care professionals serve the needs of families. Improvements in technology have made it easier to manage our firms remotely, but it has left us more vulnerable to cyber criminals eager to steal confidential data or, even worse, hold your data for ransom.

It is common knowledge that the death-care industry has been slow to adopt new technology. Our profession's primary focus has been, and will always be, supporting families during a time of great loss.

These days, however, data security needs to move up your "to-do" list as quickly as possible because cyber-criminal activity has skyrocketed during the pandemic. The number of COVID-specific malware attacks increased 475% from February to March, according to research by cybersecurity firm Bitdefender. In July, a study completed by VMware Carbon Black found that 91% of businesses reported an increase in cyberattacks since the pandemic began.

Remote work creates new risks for our industry. Fortunately, by putting in place certain security protocols and software, funeral directors and cemeterians can protect families' sensitive information that is shared daily during the course of business. Here's how you do it:

1. Make sure employees secure personal devices

Most likely, your funeral home or cemetery has more employees working from home these days because of local or statewide mandates put in place to protect their health and reduce the spread of the coronavirus. Unless they have been provided computers, that means they are conducting company business and accessing files on their personal desktop computers, laptops, tablets and cellphones. To safeguard company files from computer viruses and malware, make sure all employees working from home have firewall protection and anti-virus software installed on each device they use for company business – and that the software is automatically updated. All it takes is one employee to accidentally click a phishing email and your firm's data could be open to cyber criminals.

2. Use a dedicated system for remote work

To further protect your business from data breaches, require employees to use a virtual private network (VPN) when conducting business from home. VPNs, which encrypt data being transmitted between devices, are among the most secure methods for allowing employees to access company resources when working remotely. Do your homework before selecting a VPN vendor. The best providers will have policies that clearly explain how you manage confidential data. The relatively low cost (around \$10 per user per month) is well worth the investment – and the peace of mind knowing your data is secure.



Bill Williams

3. Make sure credit card payment technology is PCI compliant

Face-to-face communication and personalized service are at the heart of our industry, yet the pandemic has made that challenging. Our industry professionals are now interacting via phone and email with families more frequently than ever before, and that includes accepting credit card payments. Data security should be a top priority when accepting all forms of electronic payments. Make sure your credit card processor ensures Payment Card Industry (PCI) compliance, which is the gold standard in protecting data theft and fraud.

4. Update your firm's business continuity and data backup plan

Every funeral home and cemetery should back up their data in the event of an emergency. Even though it's an accepted best practice, 14% of businesses still do not back up their data, according to a 2019 survey by Acronis. Backing up digital files, such as preneed contracts, ensures business continuity in the event of a data breach, theft or natural disaster. Companies will be well-served by following the time-tested 3-2-1 rule for backup: three copies of data saved on two different storage devices, with one copy stored offsite (preferably in the cloud). We recommend having a clearly defined process that details how backed-up data is accessed and restored if your system is breached.

5. Educate and train staff on cybersecurity prevention

Your employees are the first line of defense in protecting your firm from hackers. To help your staff shield your funeral home or cemetery from cyber criminals, employees should be well informed about the types of cyber threats, how to prevent them and, if needed, how to respond to a data breach. Conduct regularly scheduled training sessions or have employees participate in online cybersecurity classes. Knowledge is power in the fight against cyber criminals.

6. Implement a secure process for sharing contracts and sensitive files digitally

Over the past several months, you have likely interacted with families digitally in a variety of ways and more than ever before – whether that be by email, Zoom or another virtual platform. While sending and signing preneed contracts and other documents digitally can help you serve families better, especially those uncomfortable visiting a facility, it comes with a significant security risk if you do not implement the proper safeguards. After all, preneed contracts include very sensitive information of an individual. Ensure you are sending these contracts securely, such as through an encrypted link. Your trustee or recordkeeper should have tools and resources in place that help you achieve this with confidence.

Most likely, many employees will continue working from home well into the latter part of the year. And, moving forward, more consumers will continue to seek ways to conduct their end-of-line planning online or through virtual means. By establishing these data security policies and procedures, you will be better armed in the fight against cybercriminals so you can spend more time doing what's important: taking care of your families when they need you most.

Get more guidance from Bill Williams when he joins Wendy Russell Wiener, managing member of WRW Legal, in a presentation on due diligence at the Funeral Service Business Plan Conference, Dec. 3-4, in Nashville, Tennessee. Learn more at <https://events.kates-boylston.com/event/bizplan>.