INDIANA CEMETERY ASSOCIATION, INC.

VIEW POINT NEWSLETTER

indianacemeteryassociation.org

December 2021

Planning for the Future

A message from the president Donald R. Remenschneider

Planning is bringing the future into the present so that you can do something about it now. I remember coming home from the national cemetery conference with the book" How To Get Control of Your Time and Your Life" authored by Alan Lakein who knows a lot about the importance of planning.

He says the problem is, too many people (and businesses) spend too much time thinking and not enough time doing and then wonder why they're not making the progress they want.

For those people who understand the value in planning ahead, and then acting on those plans, the results are powerful.

As the president of the I.C.A. I am very proud to work with a board of directors under the guidance of our executive director Casey Miller and the foresight and aggressive approach that is apparent in our association. Casey is bringing the Future Into The Present, presenting the challenge and acting on these issues with the backing of the board!

The board of directors give of their own time to better the cemeteries in Indiana and issues that come about in the United States.

This past year we have been working on an issue in the Indiana State House that would affect the financial stability of every cemetery. We are being very pro active with this situation and have had numerous meetings to come up with ideas that are both good for the cemeteries and the consumer.

Yes, this comes at a cost, and therefore we need to increase our membership dues to hire the best people for the job. How and when do you start planning? A good first step is to continue your membership with the I.C.A. and encourage others to join that are not members. This helps promote education and provides networking opportunities.

Reaching my forty third year as superintendent of the Concordia Cemetery Association Inc. I have been thru more challenges and been a part of more changes in the last 10 years then in the previous 33 years. Planning for the future has kept our cemeteries in line with the new changes. I credit a lot of our success to being a member of the I.C A. and the help that previous members gave me starting on my first day. Side note, I was hired on for two weeks until a new superintendent was found. (I had my own landscaping business and had no experience working in a cemetery.) I have never regretted the opportunity to serve in the cemetery business. I credit Wilbur Purdy from Catholic Cemetery Fort Wayne who offered his help on my first day.

My prayer for everyone is to have a Blessed Christmas, good health, and a very successful New Year!

We are dedicated to maintaining cemeteries as places of sacred memories of the deceased and comfort for the living.

OFFICERS:

PRESIDENT
Don Remenschneider
260-749-9836

PRESIDENT ELECT
Ray Sabol
765-642-3714

SECRETARY/TREASURER
Amanda Klei
812-376-6375

EXECUTIVE DIRECTOR
Casey Miller
260-402-8555

BOARD of DIRECTORS:

Ted Mau
Mark Minnick
Mark McCrocklin
Aaron Seaman
Stephanie Coulter
Chris Cooke

FEATURE ARTICLE:
We're Holding Your Graves Hostage!
Ransomware in Deathcare

by Poul Lemasters, Esq.

Copyright ©2021. International Cemetery, Cremation and Funeral Association. All rights reserve.
Reprinted with permission from Memento Mori, October 2021 (Vol. 81, No. 10).

We have all seen the headlines. Ransomware attacks have risen. No wonder … the practice can be quite lucrative. Today's cyber "pirates" can amass millions of dollars just from one attack. The most recent attacks to make the headlines brought two large companies to a standstill. But small businesses also are being threatened with ransomware with demands of tens if not hundreds of thousands of dollars. Cyberattackers are sophisticated enough to know the size of the company being exploited and will ask for an amount that is just shy of insurmountable.

Hackers and scammers use ransomware to force a business to pay money or fear the loss of critical, secure data. In its simplest form, ransomware is malware that once in your system can encrypt files so they are unusable. Without the decryption key, the user cannot access the files any longer, and the hacker can potentially delete the files or sell/leak the data to others.

In May 2021, Colonial Pipeline, America's largest fuel pipeline system that originates in Houston and carries gasoline and jet fuel to parts of the southeast United States, suffered such an attack that adversely impacted computers managing the pipeline. One compromised password allowed Russian hackers to disrupt a nation's infrastructure, and many consumers experienced first-hand widespread panic that led to a major shortage in gasoline at the local pumps. One minute, it's toilet paper, the next it's gasoline. Jokes were plentiful across all the late-night television shows. But all jokes aside, this hack revealed astronomical weaknesses in U.S. cybersecurity. Colonial Pipeline's CEO buckled under the pressure and coughed up a mere $4.4 million to rescue his pipeline and save Americans from the chaos that quickly ensued as the news of the attack spread across the nation.

JBS USA Holdings Inc., the world's largest meat processing company, was forced to pay a ransom of $11 million after ransomware breached computer networks at the plants. Government officials warned consumers not to panic and buy up all the meat in the stores as a result of the attack.

In July 2021, Reuters reported that in one such attack on an IT firm in Florida, close to 1,500 businesses had been affected. The hackers were demanding $70 million in ransom. Organizations in a dozen countries were impacted by this breach.

Ransomware attacks are growing across the United States in all areas. You may be wondering if this could ever happen to a deathcare business. Well, it already has.

While most of America watched and felt the ransomware attacks of JBS and the Colonial Pipeline, a cemetery and funeral home combination business located in Florida went through its own ransomware attack. And while it didn't make national or even local headlines, the ransomware attack was felt by everyone at this small business.

The following is a brief overview of not only this cemetery's actual ransomware encounter, but also a guide on how to respond to a ransomware attack. More importantly, it provides the steps to take to try to prevent a ransomware attack from happening to your business.

This article in no way covers everything on ransomware, but it will help you see and understand the risks that are out there. The information provided in this article is based on guidance from Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security and the Multi-State Information Sharing & Analysis Center (MS-ISAC) which recently published a ransomware guide that outlines both preventive steps and responses to an actual ransomware attack. Download the entire guide at www.cisa.gov/stopransomware/ransomware-guide.

That Fateful Morning

It was a typical Thursday morning as the president and CEO of a cemetery and funeral home combination business got ready for work and started on his way to the office. Upon arrival, nothing seemed out of the ordinary until 9:15 am when all the printers in the office started printing. No one on staff had hit "print," yet all the printers in the building started spewing out a one-page letter. The letter was a simple one. It stated that the business had been hacked, and the "perpetrators" would be in touch.

About the same time as the letters were clogging the printers, the cemetery's IT company representative called and said, "You've been hacked. Turn everything off immediately including your server." As the president told everyone to disconnect, turn off, and unplug everything, he knew this was going to be a rough day.

The facts show that while many "threat actors"—the term for

malicious groups and individuals who are behind malicious cyber-attacks—target large public-facing companies, there is a much broader base of attacks among private businesses and individuals. The truth is that anyone with a computer connected to the internet is at risk of a ransomware attack. This cemetery and funeral home are among one of approximately 4,000 ransomware attacks that happen daily. Yes. Daily.

Who Do You Call?

Well, the Ghostbusters won't help much in a situation like this one. In any emergency, your first call should be to the people who can help you through your crisis. When it comes to ransomware attacks, most small businesses and individuals simply don't know who that should be. For this president, he knew that his insurance provider covered cyberattacks and ransomware attacks, so his first call was to his insurance broker.

The insurance broker sprang into action quickly and contacted the cybersecurity insurance carrier that would call the president directly. Within 30 minutes of the initial call reporting the incident, the cybersecurity insurance policy carrier was on the phone with the cemetery president. It is worth noting that this business had a stand-alone cybersecurity policy, which provided more thorough coverage than just a cybersecurity rider that is included in most general liability policies.

Current guidelines recommend that you contact the following people after a ransomware attack:

(1) Your IT department

(2) Your insurance company

(3) The FBI

As of the date of this article, the cemetery has not contacted the FBI, local police or any government official. However, the option exists; and as more and more ransomware attacks occur, there are local government agencies that are developing stand-alone units and departments that work entirely in the cybersecurity realm. For many businesses, it is worth investigating ahead of time what local protection and options they may have.

Rally the Troops

Once your first call is made, it is time to start resolving the ransomware attack. The cemetery's president was now working directly with the cybersecurity insurance carrier. That carrier advised the president to hire an attorney immediately and provided a list of approved attorneys from which to choose. Keep in mind that these conversations were all being held offline through telephone and secondary emails on other devices, as their entire business operation was shut down.

The chosen attorney gave the president a short list of action items, including the need to hire an intermediary cybersecurity company that could handle the repair and resolution directly.

Through the help of the insurance company, which provided another list of approved cybersecurity intermediary companies, the president contacted and hired the intermediary. Its job was to determine what was encrypted and damaged as well as work with the cemetery's IT company.

By late afternoon, the cemetery's team—which included the insurance company, attorney, IT company, and intermediary cybersecurity company—was all on a conference call developing a plan of action. In fact, by 9:15 pm that very evening, the intermediary was already onsite working to resolve issues.

4 Steps Toward Resolution

In resolving a ransomware attack, there are really two main issues. The first is securing your corrupted system and data, and the second is resolving the ransomware threat itself. Under CISA guidelines, it is recommended to take the following initial steps:

(1) Document the incident.

(2) Disable all automated tasks.

(3) Find systems impacted.

(4) Secure backups.

Disable all automated tasks. The cemetery's IT company was a third-party company that oversaw the entire system. The IT company was able to handle some of the steps, including documenting the attack as well as being able to shut down all automated tasks.

Document the incident. Not all small businesses have an IT company, department, or even an IT person. If this is you, start by knowing the basics. First, take a picture of the screen to document the incident or keep a copy of the "threat actors" letter. Then, go offline. Disconnect from the internet by logging off and even unplugging any direct connections, such as Ethernet cable connections.

Some people think there may be a quick fix. Do not simply restart your system thinking you can get around the ransomware. Do not connect other devices or outside storage to the infected system. And do not start deleting files. All of these quick fixes could result in further damage as many malware viruses are programmed to do more damage upon the actions set forth above.

Find systems impacted. When it comes to finding the impacted system(s), consider an outside company that has expertise in malware issues. Even in this case when the cemetery had an outside IT company that handled all its computer needs, the president still brought in an intermediary cybersecurity company that worked with the insurance company and the IT company to identify and fix the impacted hardware.

Secure backups. This is where businesses can live or die. Without a backup, you can be crushed by a ransomware attack. The cemetery had a back-up that was as recent as 15 minutes before the hack. The cemetery was able to restore from a back-up, allowing the business to recoup all its data.

Negotiating with the Devil

There was still one more issue to deal with. The ransomware was still living within the cemetery's computer system and there was a risk that the hackers could cause further damage to the cemetery by selling or posting its data on the "dark web" or posing other threats to the data and future business. It was at this point that the cemetery—through its team of experts—entered into the stage of communicating with the threat actors.

This is when businesses, people, and insurance companies must decide if ransom should be paid. Never mind the legal issue of whether it can be paid! There are laws that prevent ransom from being paid to outside countries that are on certain sanctioned lists. But in recent times, we have seen this law violated by large public companies with no legal recourse. The truth is that there is little current legal guidance on whether you can or can't pay a ransom. In fact, there have been cases where ransom was even allowed to be written off as a tax-deductible item.

Whether you are allowed to pay, consider whether you should pay it. Many insurance companies actually choose to pay the ransom due to the potential underlying cost of rebuilding a database or the cost of data that is ultimately used for illegal purposes. As an example, in 2018, the city of Atlanta chose not to pay a ransomware demand and instead took the loss of data and destruction of its city server. Ultimately, the city rebuilt the server and system for $17 million. Oh, the ransomware that was demanded—a mere $51,000. But there is always the risk of paying the ransom and not getting the release from the malware.

In this case, the cemetery disagreed internally about whether to pay the ransom. If the cemetery paid, could it trust that the criminals would provide the decryption code? They were criminals, after all. Enter the professionals, the intermediary company, which was familiar with the threat actors in this case.

From the printed letters and method of malware, the cybersecurity intermediary recognized the actors behind the threat. It set up a line of communication to negotiate the ransom. The threat actors didn't give a ransom amount. Instead, they asked for a 'donation' to free all the files. There was a discussion on how much of a donation, where the donation would be paid, and how the donation would be paid.

The cemetery concluded, based on the intermediary's knowledge of this particular threat actor, that the attackers did in fact have control of the files and could be trusted. During the initial negotiations, the cybersecurity company asked for proof of files, which the threat actors were able to demonstrate they had copied and were in possession of. In regard to trusting the threat actors, it's ironic to call these criminals trustworthy; but in the world of ransomware, there are some groups that have built a level of trust, while others are simply criminals.

The cemetery offered an amount and the cyber "pirates" accepted it. The amount was paid in bitcoin. Upon payment, the ransomware issue was resolved. By Monday, the cemetery was up and running with all files available.

Upon Further Investigation …

It would be great to say that once the payment was made the issue was over, but that's not how this works. After a ransomware attack, there needs to be more investigation as to how and when it all happened. The cemetery discovered that the hackers had been in and out of system for up to eight months and had been corrupting files and looking at data the whole time. How did the threat actors gain access?

The short answer is we may never know. It could have been a file that was downloaded with a corrupted attachment. Or it could have been a link that was clicked, which allowed the hackers to gain access the cemetery's system. Once the door was opened, the threat actors were in and the cemetery never knew. The cemetery was told by the cybersecurity

company that a scan wouldn't have detected the hackers' presence because by downloading or clicking the corrupted link, the bad guys had permission to look around—and that's exactly what they did.

Time to Rebuild

Besides investigating, there is also the rebuild of the system. While you can use your backup to get started, it is recommended that you scan all items before opening to make sure all files aren't still encrypted. The rebuild is a timely and costly process.

Getting the Word Out

One of the most time-consuming and costly items, even more than the ransom, is the notification to the consumer of a potential data breach. All 50 states have laws that require a business to notify the consumer of a potential breach of data, under certain circumstances.

What are those circumstances? Here comes the time-consuming and costly part. Every state has its own law with different protocols. They range from access to any personal data to personal data that is likely to substantially harm an individual.

The process of notification is different from state to state and can include direct communication with the consumer to filing the breach with the state Attorney General. And don't forget, this is based on where the consumer lives—meaning that a deathcare provider may have customers in multiple states and would have to comply with all the laws in those states.

The cemetery had to scan all of its files to determine who and what contracts in the database had been affected or potentially breached. Once this was determined, the cemetery had to send a letter to the Attorney General in each state where there may have been a consumer hacked and then another letter to each person affected. The letter to the consumer must list the consumer's rights and what the hacked business will do. Fortunately for the cemetery and funeral home, the team grew by one more company that specializes specifically in reporting cybersecurity breaches.

Covering the Costs

The insurance company paid for all the costs associated with the ransomware incident, other than the initial deductible. This includes costs for the attorney, costs for the intermediary cybersecurity company, the cybersecurity breach reporting company, and the ransom itself. The fees involved in this one event were in the six figures.

Preventing the Next Ransomware Attack

CISA, as well as others, recommend implementing the following steps as minimum preventive measures to defend against ransomware attacks:

(1) Have a cybersecurity plan

(2) Perform regular backups

(3) Keep software programs up to date

(4) Maintain virus and malware software

(5) Provide training

(6) Maintain insurance

The cemetery and funeral home have made some changes and upgrades to its cybersecurity protocol. First, the cemetery has added layered security by keeping its local IT company and adding a cybersecurity program. A firewall is not enough. Businesses should consider a second layer of security behind the firewall to find corrupt activity that is happening inside the system. In this case, from the investigation, the bad guys had been knocking on the door to the system for a long time. They finally got in and did damage without anyone knowing for months.

For other businesses that do not have an IT company or an outside second layer of security, it may be time to talk to someone. If you don't have an IT person you can contact, you may want to consider finding that contact. No one wants to be on the receiving end of a ransomware attack; what's worse is not knowing who to call for support.

The cemetery had a great backup process. Make sure you have a backup system for all of your data. Many businesses now have two backup systems—local backup as well as a cloud backup. But just having the backup system is not enough. Make sure you test the backup regularly and understand how to reinstall from a backup in case the need ever arises.

Many businesses are guilty of allowing computers to run on old programs and operating systems. It is recommended that your systems always be up to date. Old, expired programs can leave patches that allow threat actors to enter your system. And make sure your anti-virus software is always current.

It truly is the simple things that can cause problems. Most cyberattacks and ransomware attacks are traced back to malware that infected the computer system through infected

email attachments and links. Train your employees recognize the threat. Don't click on attachments or links you don't know.

Lastly, make sure you have insurance in place that covers cyber and ransomware claims. Typically, there are stand-alone policies versus a rider that is under your general liability coverage. Consider talking to your insurance provider and finding out what type of coverage you have: (1) coverage of stolen data; (2) loss of access to the system that affects daily operations; (3) costs to repair and rebuild data or the system; (4) costs for notifications that are required; and, of course, (5) terms for paying ransom.

Ransomware, unfortunately, is on the rise and something everyone needs to address. If you have not thought about it, you most likely have no plan to prevent it or respond to it. A word of advice from the cemetery president who went through this: "You may think you are a small business, and they will never find or want you. That is exactly wrong. It's the small business that they actually want. Be prepared."

A special thank you to Kennan Knopke, CCFE, of Curlew Hills Memory Gardens, a 30-acre cemetery located in Palm Harbor, FL, that does approximately 450 events a year at the cemetery and serves approximately 600 families at its onsite funeral home. By sharing his story about how they handled this ransomware attack, it allows the entire profession to better understand the risk as well as how to prepare.

Poul Lemasters, Esq., poul@iccfa.com, serves as ICCFA general counsel and cremation programs coordinator. He also serves on the Government and Legal Affairs Committee. Poul is an attorney and a funeral director/embalmer with degrees from the Cincinnati College of Mortuary Science and the Northern Kentucky University Chase College of Law. He is a licensed funeral director/embalmer in Ohio and West Virginia and is admitted to practice law in Ohio, Kentucky, and Virginia. As principal of Lemasters Consulting, a deathcare consulting company, Poul offers ICCFA members in good standing a free one-hour consultation relating to cremation; in addition, members are entitled to a free GPL review to check for Funeral Rule compliance.Eps, con simus, ta Senduce psestim usquiumum spiciam am et, que faudeestra, fur, P. Obsediis cula tam tebuntem, nos, conduci pimilia quem inatum adduciem talica L. Grat vidiondac ompos, quos, cae pata, pubi imandit L. Issimis; hostore a conon Etriuro et L. Am. Eris comnestant.

We wish you and your family a holy and prayerful Christmas Season

FEATURE CEMETERY:

GRANT MEMORIAL PARK
NEEDHAM • STOREY • WAMPNER
FUNERAL SERVICE

History of Grant Memorial Park

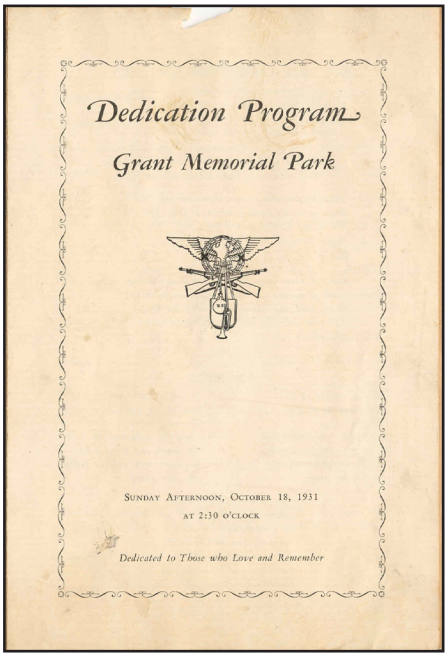
In 1930 Edward Stewart, Josiah Winters, and Judge Robert M. VanAtta began Grant Memorial Park on an 80 acre tract of land west of Western Avenue between 16th and 26th streets in Marion, Indiana. Their initial offices were in the Hotel Spencer in Marion – now the Grant County Office Building. Through the years, Grant Memorial Park has always been a for-profit cemetery.

John M. Storey and Benjamin R. Needham jointly purchased the cemetery from the Brandon family in 1985. In 1995, Grant Memorial Park became a subsidiary of Needham-Storey Funeral Service, Inc. In December 2000 ownership became Needham-Storey-Wampner Funeral Service, Inc. To date, Mark Story (Owner and President) continues to carry on the tradition of "Dedicated to those who love and remember".

Grant Memorial Park offers disposition options for ground burial, mausoleum and multiple cremation niche options in the mausoleum and The Gardens. The new entrance sign was erected in 2021, where the original driveway entrance was located.

GRANT MEMORIAL PARK PRIOR TO ANY DEVELOPMENT, JANUARY, 1930

THE FIRST DAY ON THE FIELD TO START THE WORK AFTER CLEARING THE SURFACE, MAY, 1930

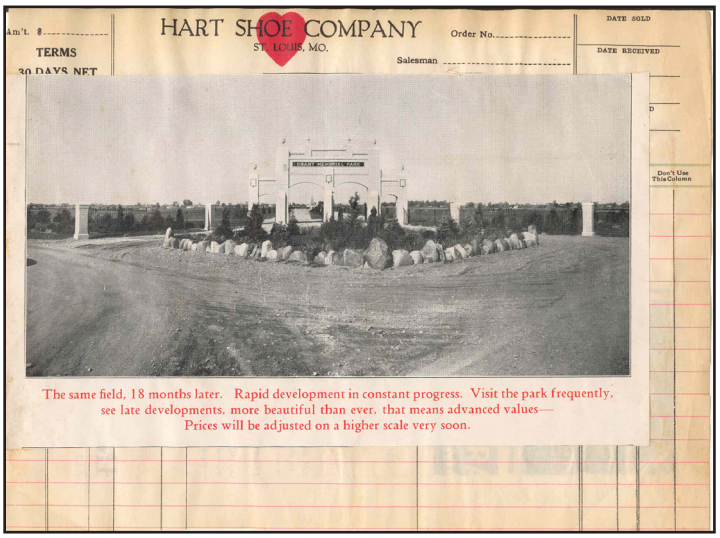


Dedication Program

Grant Memorial Park

Sunday Afternoon, October 18, 1931
at 2:30 o'clock

Dedicated to Those who Love and Remember



HART SHOE COMPANY
ST. LOUIS, MO.

TERMS

Order No.

Salesman

DATE SOLD

DATE RECEIVED

The same field, 18 months later. Rapid development in constant progress. Visit the park frequently, see late developments, more beautiful than ever, that means advanced values—
Prices will be adjusted on a higher scale very soon.

FEATURE CEMETERY: (continued from page seven)

GRANT MEMORIAL PARK
NEEDHAM • STOREY • WAMPNER
FUNERAL SERVICE

New Entrance Sign

Grant Memorial Park Mausoleum and Chapel

To ICA Members

A message from the Executive Director, Casey Miller

To say that I have personally missed all of you because the Annual Convention and Trade Show has been cancelled due to Covid for the past two years would be a huge understatement! The sharing of ideas and catching up with the lives of good friends is something that I really miss. So, with that said, let's all hope that 2022 will be different and bring us together again.

Covid certainly has not hindered progress within the Indiana Cemetery Association. The Board of Directors has met in person more this year than in any other year that I can remember. The reason for that is because a very fundamental aspect of our business is being challenged in the Indiana legislature. The ICA is in the midst of defending our ability to preserve our grounds and present our families a beautiful and peaceful cemetery experience while they visit a friend or family member. As you well know, an effort is under way to prohibit our ability to perform exclusive work in our cemeteries. The ICA is well aware that this effort would have severe consequences for the families that rely on us to provide them with professional cemetery services. Only cemetery personnel has the intimate knowledge and training to perform critical work in your cemetery such as the performance of memorial/monument installations and providing an interment, entombment or inurnment service. The ICA will be vigilant in defending this issue during the 2022 short legislative session.

On behalf of the ICA Board of Directors, let me wish you a Merry Christmas and a very happy New Year!

Executive Director

CASEY MILLER • EXECUTIVE DIRECTOR
13219 Drayton Parkway • Fort Wayne, Indiana 46845
260.402.8555 • cmillerica@gmail.com

INDIANA CEMETERY ASSOCIATION, INC.

E & L CEMETERY SERVICES ™

We offer a full range of services, from initial conceptual design, to final installation of cemetery and civic memorials. We specialize in field installation and remedial site work. Field work includes, but not limited to memorial installation, restoration, cleaning, raise–align–reset of cemetery memorials, estate mausoleums and columbarium construction.

We can also source granite, marble and limestone for any architectural building applications.

Our Mission

Provide exceptional service through memorialization and cemetery care activities, to preserve, restore and protect the memories of the departed.

About Us

E & L Cemetery Services LLC., was founded in 2014 by Edward "Eddie" Curtis and to fill a need for installation of small scale family memorials up to large private estate and civic projects.

Eddie started in the memorial industry at the age of nineteen with one of the most progressive monument firms in Elberton, Georgia. That humble start and a lifelong career in the memorial trade brings experience to assist with your every need.

2856 Banwick Road • Columbus, Ohio 43232
Tel: 866.451.7052 • Fax: 866.531.5572

www.EandLcemeteryservices.com

E & L Cemetery Services LLC

Are you a funeral home that would like to sell memorials, but lacks the expertise and equipment to install?

We will install it for you!

You can make more money!

Cemetery Installations

Mausoleum & Columbarium Installations

Mausoleum & Columbarium Installations

- Over 40 years experience
- Members of Ohio Cemetery Assoc. (OCA)
- Member of the Indiana Cemetery Association
- Members of Monument Builders of North America (MBNA)
- DryTreat Accredited Applicator
- Nationwide Service Capabilities

www.EandLcemeteryservices.com

INDIANA CEMETERY ASSOCIATION, INC.