Case Study

How To Survive A Ransomware Attack

Jess Howard Electric Company's Holistic Approach To Cybersecurity

Members of the Rea team recently visited Jess Howard Electric Company, a Rea client, to learn more about the business, their team culture and to tour the facility. During the visit, the company highlighted its impressive IT infrastructure and its data security efforts. Read on to find out how Jess Howard Electric was able to beat the odds and survive two Ransomware Attacks over the course of two years.

Cybercrime is not going away.

As long as there is money to be made through the infiltration and exploitation of a business's network, there will be criminals willing to find new ways to threaten the security and stability of your business's digital infrastructure.

Specifically, authorities continue to report increased instances of Ransomware. Just last year, Ransomware moved to the top spot as the number one security concern for organizations with nearly 50 percent of businesses reporting that they had suffered at least one Ransomware attack over the last 12 months. Unfortunately, of those businesses that reported being attacked, nearly 40 percent were left with no choice but to pay the ransom.

Not The Jess Howard Electric Company.

Based out of Blacklick, a suburb of Columbus, The Jess Howard Electric Company beat the odds twice – a statistic that's simply unheard of these days, particularly among small, family owned businesses.

But The Jess Howard Electric Company's approach to IT and data security is anything but ordinary.

We're In It Together

"All it takes is for one of your employees to open a single malicious email," explained Scott Stottlemire, an independent senior network/IT engineer and software engineer for Jess Howard Electric. Fortunately, the company had already made the necessary investment in its IT infrastructure. When the company was attacked, Jess Howard Electric was able to recover quickly – without paying the ransom associated with the attack.

"No matter how much you spend, how much of an investment you put into the best hardware, software and security devices, you will never be worry-free," said Scott. "The best thing you can do is to prepare for the worst. You don't want the first time you have a problem to be the first time you have ever restored your data. You have to put your infrastructure in place and you have to test your procedures regularly."

Jonathan Howard, president and CEO of Jess Howard Electric, not only agrees with Scott's logic, he has taken an active role in the company's IT and data security effort – a stance not normally seen in other businesses.

Rea & associates
a brighter way

As the president of the company, Jonathan says his primary responsibility is to protect Jess Howard Electric, its employees and its customers. Because data security is such a critical component of running a business, he maintains a close working relationship with Scott.

"I don't understand why more business owners don't have this type of relationship with IT," said Jonathan. "If something goes wrong, if your network is breached, it can cost millions to recover. Money you don't have. Your data is your business. If you lose control over that, you have nothing."

Jonathan says his relationship with Scott has been essential to protecting his company's data. This ongoing support has empowered Scott to make ongoing security recommendations and identify solutions to many of the company's IT-related challenges. The results speak for themselves.

"The cost of investing in IT and cybersecurity was a no-brainer," Jonathan explained. "We already know that if our networks are going down, we're going to lose money and strain good relationships. Our goal is to actually minimize the time our networks are down. If our IT investments help us keep downtime to a minimum, then the cost was absolutely worth it."

Take Network Configuration Seriously

Jess Howard Electric currently utilizes three physical servers, which enables the company to ensure an up-to-date backup of its data at all times. Removable hard drive media data backups are copied from the backup server every night and are taken off site as a worst case recovery option. Additionally, servers are connected via a 10GB local area network (LAN) to ensure optimized bandwidth during the copy/restore process and minimize recovery time.

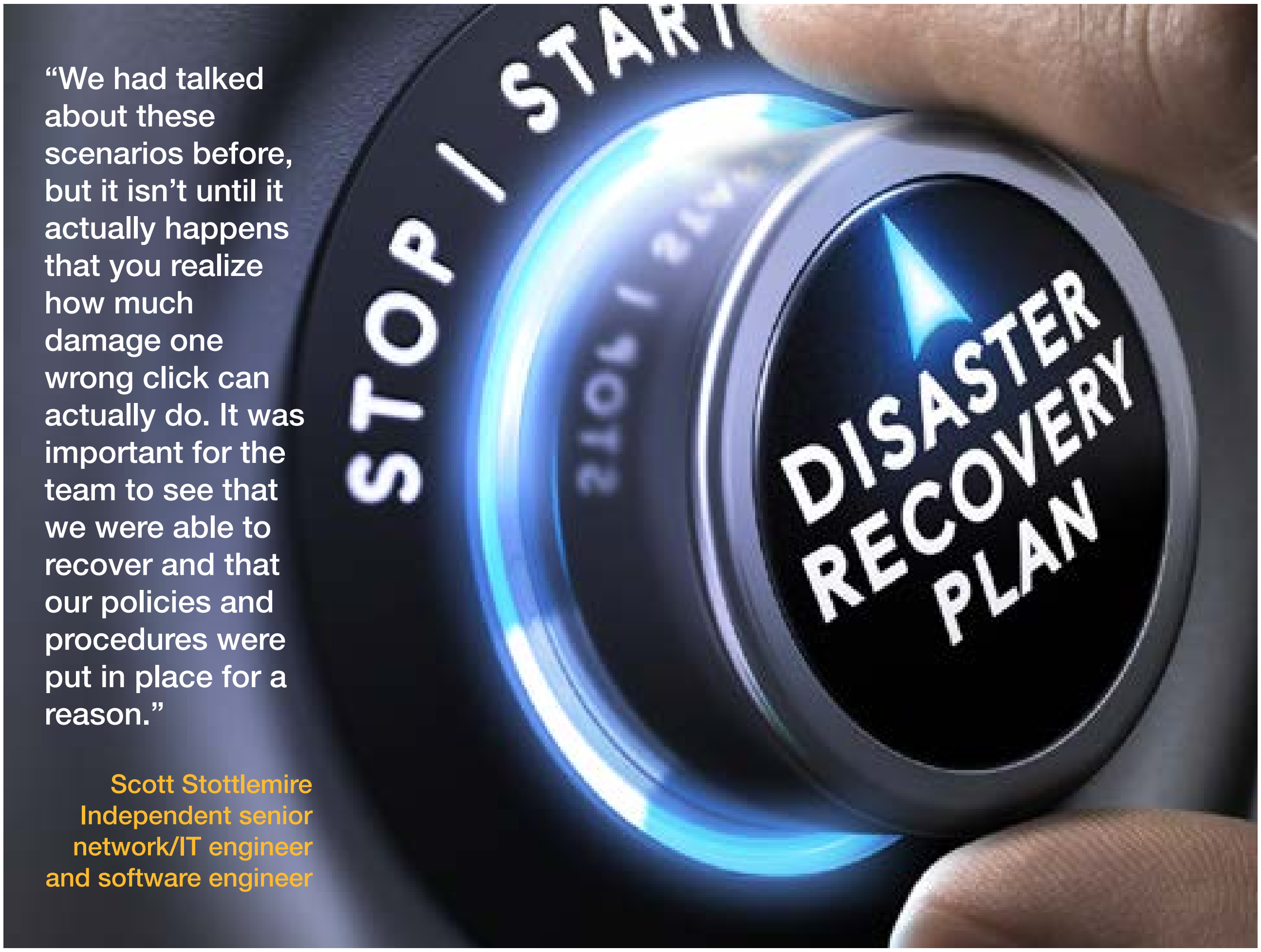
The company also runs its own external Domain Name Servers (DNS) servers which gives Jess Howard Electric full control over which Internet Protocol (IP) addresses, or unique identifier assigned to a user's computer or device, are approved for internet access, enabling seamless fail-over and fail-back processes.

Furthermore, redundant, identical routers are used to ensure constant internet connection and a mail server that is always available and primary and secondary internet providers were selected to maintain connectivity.

Protecting the company's data from Ransomware and other cyber attacks is a priority for Jess Howard Electric. From utilizing a hardware appliance for virus and malware protection related to all inbound and outbound email and attachments to installing client applications specific to preventing attacks on the team's PCs, the company continues to demonstrate its commitment to online protection.

> **The cost of investing in IT and cybersecurity was a no-brainer. We already know that if our networks are going down, we're going to lose money and strain good relationships. ... If our IT investments help us keep downtime to a minimum, then the cost was absolutely worth it.**

Jonathan Howard
President & CEO
Jess Howard Electric Company



> "We had talked about these scenarios before, but it isn't until it actually happens that you realize how much damage one wrong click can actually do. It was important for the team to see that we were able to recover and that our policies and procedures were put in place for a reason."
>
> Scott Stottlemire
> Independent senior network/IT engineer and software engineer

Finally, identical, ready-to-use Desktop PCs are used by all Jess Howard Electric staff. These computers are configured to be compatible with spare units that can be easily and immediately replaced if needed.

Separate from the company's network configuration, which is specifically designed to limit user access to the company's entire network while providing for a fail-safe in the event an attack does occur, Jess Howard Electric takes specific steps to protect the network from viruses and Ransomware. From utilizing a hardware appliance for virus and malware protection related to all inbound and outbound email and attachments, to installing client applications specific to preventing attacks on the team's PCs, the company continues to demonstrate its commitment to online protection.

"We are currently implementing a messaging gateway solution that will disassemble all emails and disarm and remove any malicious scripts or attachments, reassemble the email with the threat removed and then deliver the email as intended with a user notification indicating that an attachment or malicious items were automatically removed from the email," said Scott. "We believe this will help optimize real-time protection against cyber threats, which will also maximize our uptime."

Additional Precautions

Per the recommendations made by Scott Stottlemire, an independent senior network/IT engineer and software engineer who works with Jess Howard Electric, the company has taken additional measures to protect the company's data, including:

- The utilization of Cisco Umbrella for protection against possible infections stemming from internet traffic in conjunction with the establishment of a customized internet policy designed to limit access to unproductive, non-work related websites.
- Segregating Wi-Fi device connections from the company's LAN subnet, forcing them to connect to a different subnet. This action basically puts an impenetrable wall between the company's LAN and the user's wireless device, helping protect against malicious file transfer, virus attacks or recursive file encryption scripts from cross infecting the company's network.
- Constant maintenance and timely installation of all necessary updates.

Beyond Tech

The hardware and software solutions implemented by Jess Howard Electric demonstrate the company's commitment to data security. But perhaps the most important investment the company has made has been in the continued education of the Jess Howard Electric team.

"We recognized long ago that you can't solve a user or management problem with technology. After all, your systems aren't going to infect themselves. Your team, your users, are your first line of defense and educating the end-user is just as critical as all the other planning we've done," said Scott. "You can't keep them in the dark. They need to be aware of what is going on."

Jess Howard Electric began hosting regular IT Open Lunch Roundtable events designed to maintain open lines of communication with employees. During the events, Scott reports important news and information related to IT, cybersecurity and the software company employees use daily. Additionally, the event features a Q&A session and open discussion.

Education and regular communication throughout the company about these topics is critical, a fact that Scott said was reiterated after the second Ransomware attack.

"When we recovered from that attack, I actually saw the relief on their faces," said Scott. "We had talked about these scenarios before, but it isn't until it actually happens that you realize how much damage one wrong click can actually do. It was important for the team to see that we were able to recover and that our policies and procedures were put in place for a reason."

"We put a lot of trust in the user not to click on a bad link or open an infected attachment," he continued. "But they have to have trust in us, the company, too. They have to have confidence that if something does go wrong that the company can recover. Regular communication reinforces the fact that we are a team and that we are all responsible for the safety and security of the business and the data we have access to."

As your first line of defense, employees are absolutely critical in the fight against Ransomware – and that includes the employees responsible for managing your IT infrastructure. Jonathan reiterates the importance of this relationship and why business owners should carefully consider who they put in charge of this essential business function.

"There really has to be real trust between management and your IT department," he said. "Not only do you need to trust that they know what they are doing, you need to know that they are physically managing your servers, monitoring your computer equipment and checking your backups."

The management of Jess Howard's IT systems is ongoing and Scott and Jonathan stress that the worst mistake a company can make is to blindly trust that everything is working as it should be.

About The Company

JESS HOWARD JH ELECTRIC CO.

Founded in 1945, the Jess Howard Electric Company is a family-owned business based out of Blacklick, a suburb of Columbus, Ohio. For more than 65 years, the company has provided electrical contracting work for residential, commercial and industrial customers throughout Central Ohio. To learn more about Jess Howard Electric Co., Inc., visit www.jesshoward.com.

Find out if your IT infrastructure is up to par. Contact the Rea & Associates IT audit team to learn more about current cyber threats facing businesses and how you can help protect your company's data from dangers like Ransomware.

Brian Garland, CPA | 614.923.6584
Dublin office | 614.889.8725
New Philadelphia office | 330.339.6651
www.reacpa.com

Rea & associates
a brighter way

Written & Designed by Abbey Kanellakis
Content Development Specialist
614.923.6551
abbey.kanellakis@reacpa.com