RANSOMWARE

SURVIVAL GUIDE

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

INDEX

1. **Before the Attack!**
   A. Endpoint Protection
   B. Backup Your Data
   C. Updates and Patch Management
   D. Training & Education
   E. Email Security

2. **During the Attack!**
   A. Call Venture Pointe!
   B. Disconnect from the Network
   C. Assess Damage
   D. Plan a Response

3. **After the Attack!**
   A. Clean up
   B. Post-mortem Review
   C. Asses User Awareness
   D. Continued Education & Training

4. **Survival Checklist**

5. **Conclusion**

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

BEFORE THE ATTACK!

The best strategy to preventing extortion from Ransomware is Security. Proper Endpoint Protection and regularly updated security definitions are critical to prevention.

ENDPOINT PROTECTION: Be sure you have up-to-date Anti-Virus, SPAM Filtering, and Anti-Malware Protection. Not sure you have this? Give us a call! Venture Pointe's Pro-Pointe Managed Services clients are covered by AVG Business by Avast's award-winning security platforms. Not a Managed Service client? Give us a call and we can help ensure you have adequate protection in place!

BACKUP YOUR DATA: Make sure you have adequate offsite data backup in place to restore your files! In the event your data is compromised by Ransomware, the ability to recover from backup is your best defense. Make sure you keep daily backups that are offsite or disconnected from your network. Don't have backup protection? Give us a call to learn about our low-cost BackupPointe offsite Cloud Backup Solutions!

UPDATES & PATCH MANAGEMENT: Ensure Operating Systems, Security Software, and Business Applications are fully up to date with the latest updates and security patches! Remember to consider all business applications and software. Programs such as Adobe Flash and Java are known to be vulnerable, make sure they are all up to date with the latest updates. Check for Windows Updates and make sure your Security software has the latest security definitions installed. Completing these task on several computers can be time consuming, difficult and cumbersome. Need Help? We can do this for you!

TRAINING & EDUCATION: Most Ransomware outbreaks begin with a well-intentioned employee opening what appears to be a valid work email. This is why training and awareness are critical to prevention. It is vital that your staff members understand what to open, what not to open, how to avoid it and how to report it. Most Ransomware attacks play off the users lack of awareness and typically require them to open malicious attachments such as PDF's or Word documents containing macros. Once the attachments are opened, the malicious macros download the ransomware and start the infection process without the user ever being aware. Proper training and education can help your staff members understand the differences between malicious and legitimate emails. Venture Pointe's Pro-Pointe Managed Service clients receive training and educational materials free of charge!

EMAIL SECURITY: Even the best user training won't stop all ransomware. Today's Phishing Emails are sophisticated and highly targeted. Attackers often carefully research their targets to create emails that look legitimate and prey on human nature to respond or open attachments. Because most ransomware is transmitted via email, Advanced Email Security plays a vital role in protection. According to our research, malicious email volume increased 66% from Q4 2015 to Q1 2016 and more than 800% from Q4 2015 to Q1 2017! Advanced Email Security solutions help protect against malicious attachments, documents and links that lead to Ransomware. Need advanced Email Security? Ask us about our MailProtector Security solutions. If you are one of Venture Pointe's CloudPointe Hosted Microsoft Exchange users, you already receive this protection included with your email subscription!

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

DURING THE ATTACK!

You've been hit with Ransomware, now what!?

CALL VENTURE POINTE: Not later, Now! We are here to respond and advise on protective measures that should be taken immediately to minimize impact. Pick up the phone and call 904-351-8101 right away!

DISCONNECT FROM THE NETWORK: The very second an employee notices somethings odd, or sees a Ransomware demand, or realizes they cannot open a file due to encryption the computer should be disconnected from the network immediately! Disconnect the network cable, unplug the computer from the wall, shut it down, whatever you have to do, you must make sure the computer is removed from the network immediately. Then, call Venture Pointe!

ASSESS THE DAMAGE: While all Ransomware is bad, some attacks are worse than others. There are important questions to be asked during or after an attack – including whether to pay the ransom or not – which can hinge on several factors. What type of attack was this? Who or what on your network has been compromised? What network resources do the compromised users or accounts have access to? What has been or can be done to prevent further damage? How quickly can the damage be repaired? These are all important questions that you should be prepared to answer during or after the attack occurs.

PLAN A RESPONSE: Depending on the network configuration, it's possible the infection may have been contained to a single workstation. Best Case Scenario, a new computer is swapped out for the infected machine and a restoral of data from backup is completed. Worst case scenario, every machine on the network is infected! This may require a cost-benefit calculation that weighs support hours needed to resolve vs simply paying the ransom. While we highly advise against paying ransoms, there may be situations where this is the quickest resolution. Making this decision can be complicated and may require consulting law enforcement and/or your legal counsel. Remember, Ransomware is a crime! Not sure what to do? Let Venture Pointe help you determine the best response for your specific scenario.

P.S. Don't count on free Ransomware decryption tools! While there are free tools available, most only work for a single variation of Ransomware and quickly become outdated. As attackers continue to update and modify their ransomware these free tools quickly become inept. Research shows these tools work on less than 2% of the outbreaks reported in 2016!

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

AFTER THE ATTACK!

Regardless of the damage caused by Ransomware, the attack reveals a security failure that resulted in a device or network compromise. Now that things are back to normal, you have an opportunity to learn from the security breach and avoid future attacks.

CLEANUP: Some Ransomware contains other threats and/or backdoor Trojans that can lead to future or recurring attacks. To ensure you are fully protected it is important to wipe all compromised devices and restore all data from backups. There may be hidden threats that have been overlooked in the chaos. The best way to protect against this is to completely wipe all infected machines and rebuild.

POST MORTEM REVIEW: Now that the threat has passed, it's time to reflect on your preparedness and response. How can you improve network configurations and security to contain future attacks? Can you implement more robust security protection? Should you have a better crisis management plan? Are your current security measures capable of combating today's complex security threats? Should you consider monthly, quarterly, annual security audits or vulnerability assessments? Turn this in to a learning experience and let Venture Pointe help you create a security plan to prevent future attacks. After all, if you don't understand how the attack got through to begin with, how can you prevent the next attack from occurring?

ASSES USER AWARENESS: As mentioned previously, most strains of Ransomware rely on human interaction to deploy their payloads. Should security measures fail, your last line of defense is to ensure an "unpaid invoice" email doesn't infect your network. A well trained, well informed employee may be your best protection. Proper training and education could be the difference to avoiding another Ransomware outbreak. Make sure your employees are up to the task!

CONTINUED EDUCATION AND TRAINING: Once user awareness is analyzed, develop a curriculum to address employee vulnerability to cyber-attacks, including the lessons learned from previous attacks. Create a Crisis Plan for future attacks and ensure your employees are prepared to respond in the event of a future threat. Follow up with regular drills and testing. Consider making Cyber Attack Education and Training part of your onboarding process for new hires. Consult with Venture Pointe on additional ways to keep your employees as informed and up to date as possible on all cyber security threats.

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

SURVIVAL CHECKLIST

BEFORE THE ATTACK!

- ○ Endpoint Protection
- ○ Updates & Patch Management
- ○ Training & Education
- ○ Email Security

DURING THE ATTACK!

- ○ Call Venture Pointe!
- ○ Disconnect Devices from Network
- ○ Assess the Damage
- ○ Plan a Response

AFTER THE ATTACK!

- ○ Ransomware Cleanup
- ○ Post Mortem Review
- ○ User Awareness Assessment
- ○ Continue Education & Training

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com

CONCLUSION

Ransomware has made an impressive and lucrative comeback! The criminals behind these cyber-attacks have earned millions of dollars in ransom payments. Because of this, Ransomware is not going away any time soon. It's more important now than ever to follow these guidelines before, during, and after an attack to ensure your business is protected.

Obviously, the easiest way to combat ransomware is to prevent it right at the gates. But this requires advanced security solutions that can detect ransomware before it is delivered to your network. These robust security solutions can often be very expensive and difficult for small businesses to manage. That's where Venture Pointe can help! Venture Pointe's Pro-Pointe Managed Services include the robust cyber-security solutions required to detect and remove Ransomware before it sets foot in your environments. These solutions help reduce the human factor – the weakest link in most network environments.

To learn more about how Venture Pointe's Pro-Pointe Managed Service offerings can help keep your business protected from Ransomware, give us a call and let us show you how real-time monitoring, automated updates, advanced endpoint protection and our robust security solutions can keep your business network infrastructure safe and secure for a fraction of the cost to deploy and manage these services on your own!

Experiencing Ransomware Attack? CALL NOW!

904-351-8101

Venture Pointe, Inc.
8659 Baypine Road, Suite #106
Jacksonville, FL 32256

Phone: (904) 351-8101
Fax: (904) 301-9081
Email: info@venturepointe.com