eBOOK

THE HEALTHCARE ORGANIZATION'S GUIDE TO RANSOMWARE PREVENTION

HOW TO CONFRONT RANSOMWARE IN THE HEALTHCARE INDUSTRY TODAY

Ransomware attacks targeting healthcare organizations have become an increasingly regular occurrence over the years, with 2020 seeing large-scale hospital cyberattacks that touched thousands of healthcare consumers, disrupted critical everyday activities, damaged reputations, and led to financial loss.

It's clear that this trend will continue to plague the healthcare industry. The rising adoption of EHRs, mobile devices and BYOD efforts leaves healthcare providers of all sizes more vulnerable than in years past. Prioritizing data security and establishing a clear framework for developing and revisiting protection strategies is the best path to take today to better serve healthcare organizations tomorrow.

LEARN HOW TO TACKLE RANSOMWARE TROUBLES TO PROTECT YOUR HEALTHCARE ORGANIZATION AND THE PEOPLE YOU SERVE.

CONTENTS

WHAT IS RANSOMWARE?

RANSOMWARE AND ITS IMPACT IN HEALTHCARE

DEFINING RANSOMWARE

Ransomware is any type of malicious software created with the intent to prevent access to a computer system until a specific sum, or ransom, is paid.

Experiencing hospital ransomware could mean being forced to delay patient care, being unable to deliver care using patient records or exposing private patient data and medical information. Because of the sensitive information these organizations handle daily, healthcare companies are prime targets for ransomware and other cyberattacks.

Some statistics show ransomware is on the decline, but operating off of these statistics is potentially dangerous. A false sense of security leads healthcare institutions to underestimate the destruction that ransomware and other types of cyberattacks can—and will—cause.

To become better prepared for possible ransomware attacks, organizations in the industry should act now to develop a response plan, implement tighter security and backup measures and regularly review practices and systems to improve future efforts.

The need for healthcare institutions to maintain secure access to immediately available data that fuels improved patient care means they will continue to be a prime target for ransomware and other hospital cyberattacks.

HOW DO YOU PREVENT IT?

PREVENTING RANSOMWARE

Ransomware can come in many shapes and forms, but there are several ways to prevent devastating attacks. Malware, once it breaks through the barriers of one person, can hijack contact lists to spread and cause more damage to an organization and those associated with it. Keep these best practices in mind to reduce risk at your company.

OPERATIONAL TO-DOS

- Educate and train employees to recognize malicious intent and report suspicious content
- Develop and test contingency and backup plans, reviewing and updating quarterly
- Leverage threat intelligence in an overall security management plan
- Institute segmented networks to limit attack exposure and prevent spreading
- Patch known vulnerabilities in applications and systems and update anti-malware software
- Implement targeted technical solutions for email systems

PREVENTION TIPS FOR TEAMS

- Be wary of nefarious URLs and "free" software packages that may appear legitimate
- Investigate unexpected email attachments and links by contacting the sender via phone
- If you don't know where something leads or who it came from, don't click
- Make backup copies of important business data and files
- Develop strong passwords, change them regularly and implement two-factor authentication
- Implement a Zero-Trust architecture to limit the impact
- Conduct Security Awareness Training monthly for all users

You may not be able to avoid becoming a target, but you can take steps to ensure you're not a victim. If the goal of ransomware is to make an organization pay to recover stolen data, then proactively backing up your data before it's compromised means you can recover it on your own. The rampant ransomware attacks seen today reflect healthcare organizations' inadequate backup practices.

HOW DO YOU PREVENT IT?

DEVELOPING RESPONSE PLANS

Even if your footprint in the healthcare industry is small, having a clear documented incident response plan can help you confront a ransomware attack quickly and efficiently in a time when many businesses are scrambling to save their data and their reputation.

WHY YOU NEED A PLAN

SMBs are frequent targets of ransomware attacks because unlike more established companies, they don't always have the resources for a robust security program. But for healthcare organizations especially, a data or privacy breach can lead to irreversible reputation damages and thousands or millions of dollars in remediation costs, legal fees and regulatory penalties.

If you handle personally identifiable information or protected health information, developing an incident response plan well before malicious attacks occur and implementing it quickly when the situation does arise is the smart and responsible thing to do. It may also be required by state or federal laws.

WHAT A PLAN CAN DO FOR YOU

- Outline clear steps for communicating incidents to vendors, employees and customers
- Explain how to ensure operational continuity and recover data after a breach
- Establish how to involve legal counsel and meet obligations under breach notice laws
- Minimize financial, physical and operational loss, monitor ongoing risks and regain compliance

HOW DO YOU PREVENT IT?

ADOPTING SECURITY SOLUTIONS

Many products and solutions can help healthcare organizations become better positioned to prevent ransomware attacks and overcome them quickly and responsibly when needed.

HERE ARE SOME SOLUTIONS TO CONSIDER ADOPTING WHEN YOU SEEK PROFESSIONAL EXPERTISE IN MANAGING RISKS, BOOSTING SECURITY AND PREVENTING CYBERATTACKS:

MANAGED SECURITY

SECURITY /PENETRATION TESTING

CYBERSECURITY PROGRAM STRATEGY

VIRTUAL CISO

INCIDENT PREPAREDNESS

SECURITY RISK ASSESSMENT

CLOUD SECURITY MANAGEMENT

REMEDIATION MANAGEMENT

CYBER SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

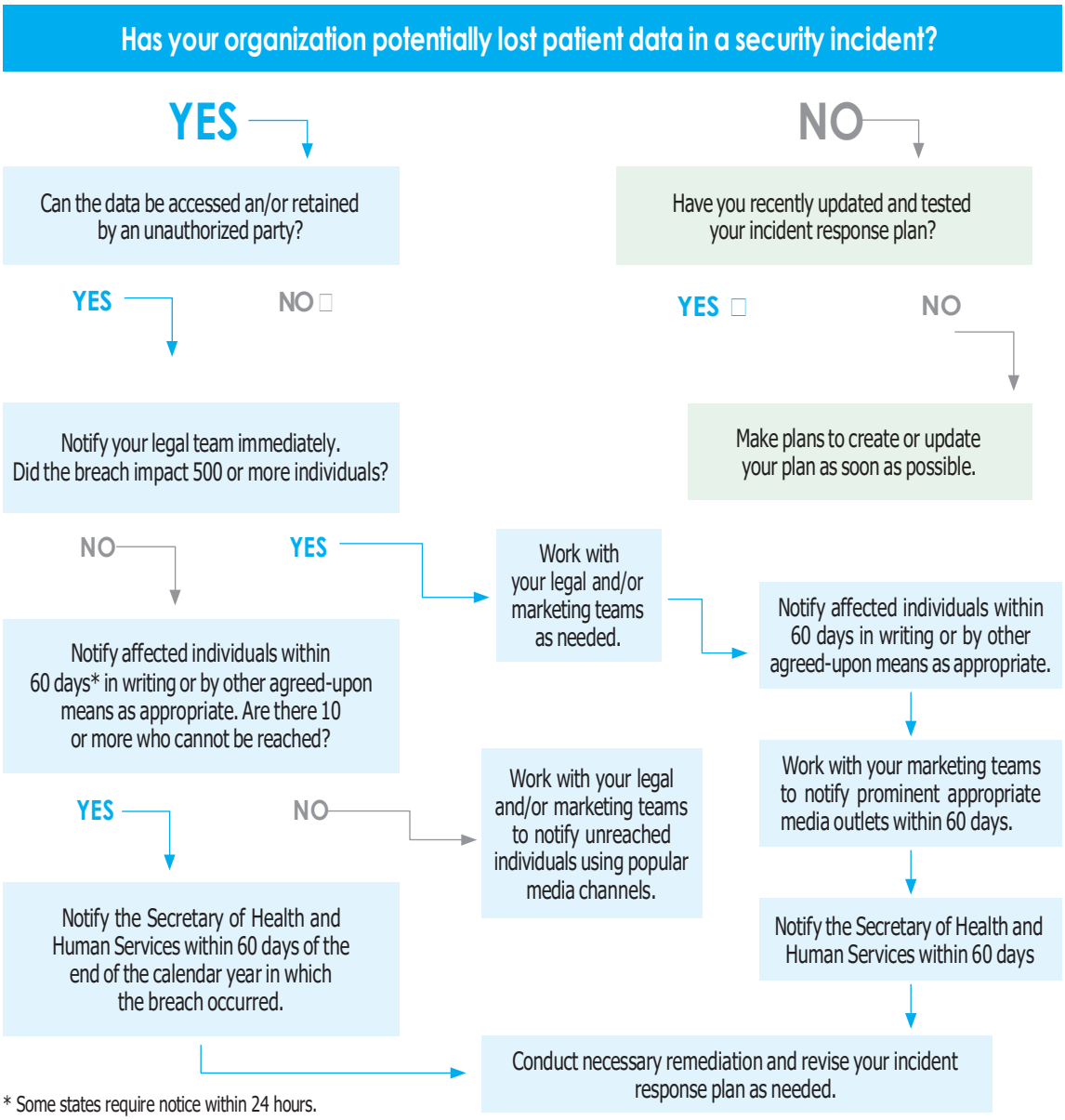
If you are not sure which services you need to improve your cybersecurity stance, talk with a HIPAA compliance specialist or an IT security provider that can assess and explain your most pressing areas of risk and available options.

HOW DO YOU APPROACH AN ATTACK?

REPORTING A BREACH

Healthcare organizations are held to a high standard when it comes to remedying ransomware attacks and other security breaches. Get familiar with HIPAA's breach notification regulations and how to remain compliant using the decision tree below.

HIPAA BREACH DECISION TREE



* Some states require notice within 24 hours.

HOW DO YOU APPROACH AN ATTACK?

DECIDING WHETHER TO PAY

It is tough to make an informed decision on whether to pay the ransom associated with an attack on yourorganization. Because many ransomware attacks are not reported and attackers are always adapting and adjusting their tactics, the little information available on how to best approach a ransom might not apply to your specific situation.

Even worse is the fact that attackers often do not provide workable keys to unencrypt data after ransoms are paid. It is important to know that in order to discourage future attacks, Federal Law Enforcement advises organizations not to pay ransoms—but this means critical data will be lost.

Use this quick guide to make a more educated decision on how your organization should respond after experiencing an attack.

REASONS TO PAY THE RANSOM
PAY if the business cost of lost data is significantly higher than the ransom
PAY if the version history indicates successful access after payment
PAY if your data backups are inadequate
PAY if the ransomware is not contained
PAY if all options for restoring lost data are unsuccessful

REASONS TO NOT PAY THE RANSOM
DON'T PAY if paying will only provide a 50% chance of regaining access
DON'T PAY if clean data backups are adequate and have been verified
DON'T PAY if the ransomware has been contained
DON'T PAY if mitigation costs to clean systems will be incurred regardless
DON'T PAY if the version is reversible
DON'T PAY if paying will make you a larger future target

HOW CAN YOU GET STARTED?

FINDING A RANSOMWARE PROTECTION PROVIDER

Finding a trusted provider of ransomware protection, compliance and security services can be difficult, especially if you are looking for a partner who works closely with your team to ensure everyone has a complete understanding of the risks your healthcare organization faces today.

WHAT TO LOOK FOR IN A RANSOMWARE PROTECTION SOLUTION

- Cybersecurity program management
- HIPAA security risk assessments
- Zero Trust methodology
- Data security
- Network vulnerability and penetration testing
- Incident response planning
- Cloud and managed security
- Data backups

WHAT TO LOOK FOR IN A RANSOMWARE PROTECTION PROVIDER

- Helps confront cybersecurity risks of today and tomorrow
- Provides consulting around specific needs
- Delivers streamlined risk assessments
- Brings lessons learned from organizations like yours
- Leads a flexible, responsive, and experienced team

WORK WITH US

WORK WITH LORICCA TO EXPLORE YOUR OPTIONS FOR TACKLING RANSOMWARE IN YOUR INDUSTRY.

WHY ORGANIZATIONS TRUST US

- Streamlined security risk assessments that maximize productivity and performance
- Highly responsive service and urgent resolutions that limit disruption
- Letters of attestation demonstrating your commitment to HIPAA compliance

FOR MORE INFORMATION OR HELP GETTING STARTED, CONTACT US AT:

www.loricca.com | 855-447-2210

REFERENCES

1. Decision: Pay the Ransom?, Loricca
2. Will Healthcare Ransomware Attacks Increase?, Loricca
3. If You Can't Prevent Ransomware, You Can Outsmart It, Loricca
4. Incident Response 101: When Do You Need to Report a Breach?, Loricca
5. Ransomware Prevention and Response Policy, Loricca
6. Ransomware Guide, Loricca