# Real Life Claims: Responding to a Ransomware Attack

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

VGM Insurance Services

800.362.3363 | info@vgminsurance.com

# The Case of the Shackled System

With cyberattacks becoming increasingly common among businesses in the healthcare industry, it's critical to take every conceivable precaution to protect your data. Yet, many businesses are still of the "it'll never happen to me" mindset.

In addition, read our real-life claims scenario, where you'll discover what it's like to experience a cyberattack as you take the point of view of a provider who suddenly loses access to her data. After you've walked in her shoes, you'll learn some tips on what to do to protect against cyberattacks and how to mitigate the damages should you experience one.

## Investigating the Case

*The day starts as any other would. There's a light morning breeze as you make your way through the entrance to one of your five locations. You spend a few minutes straightening items on shelves, sipping coffee and checking in with your staff.*

*"Oh! Maria is coming in for a fitting this afternoon. We were able to get her custom prosthesis covered," Jan says.*

*"That's great news! Let me know when she's here. I'd love to see her," you say.*

*"You got it, Karen."*

*"And great work, Jan," you say. Jan gives a small nod and starts to blush a bit as you head into your office. You sit down at your computer like you would any morning. But today, as you try to access your system, a message you haven't seen before appears.*

***All your files have been encrypted. You must pay $30,000 in Bitcoin within 72 hours to regain access to your data.***

*You reach behind your computer tower and disconnect it from your network. You hope, as you start to call your IT expert Jerry, the issue is isolated to your computer. From just outside your door, you hear Jan, "Um…Karen? There's something weird going on with the computers."*

*With that, Jerry picks up. "Hello, Karen."*

*"Hi, Jerry. We have a problem."*

*After you explain to Jerry what's just happened, he says, "Okay. Make sure you've disabled all your network connections. Have your other locations do the same. I'll see what I can find out."*

*You hang up and find Jan standing in your office doorway with sticky notes clinging to each of her fingers. "The other locations just called. They say they're getting the same message."*

*You nod and force a smile as she hands you the notes. Jan goes to leave, but turns back and asks, "Karen? Um…what should I tell the clients?"*

## The Outcome of the Case

In the end, this particular provider's business was interrupted for five days. The data on two servers, 30 computers and their proprietary software was lost. And, the most recent backup that they could use was from three days prior to the attack.

Fortunately, their patient data wasn't compromised or stolen, which could have led to extensive fines. Instead, it was simply encrypted to the point that no one could access it. However, between the disruption to business and loss of data, the provider was still left with a lofty price tag of nearly $50,000, with no cyber insurance to help with those costs.

**As attacks of this nature continue to hit providers of all sizes in all sectors of the healthcare industry, it's essential to take action today to protect your business.**

## Best Practices to Protect Your Business

### Hire third-party security experts to expose known threats and offer best practices.

There are companies that specialize in ongoing penetration tests where a security expert will attempt to breach your system. They will then provide a detailed report of vulnerabilities, which you can use to develop and implement security measures to protect data.

### Educate your staff about protecting data.

Employees should be instructed on how to identify and handle potential cyber risks. There are several easy-to-use and trackable training programs available to help educate your staff. Regular education helps build an additional line of defense. This ensures company and customer data remain secure and protected from hackers and other online threats.

### Billing software often houses valuable patient data.

However, most software allows for IP lockdown. This way it can only be accessed via the company's protected network or off-site through a secure VPN (virtual private network) connection. Remember—when using third-party hosted software, two-factor authentication should always be activated.

### Consider purchasing a Cyber Liability insurance policy.

Cyber policies can cover a business's financial liability for a cyberattack. When purchasing a cyber policy, you can expect the insurance company to also go through a list of best practices and even offer additional educational resources.

For more information about protecting your business from cyberattacks, or for a Cyber Liability insurance quote, contact your VGM Insurance Account Manager today! You can also reach out to our team at **info@vgminsurane.com**, or call us at **800-362-3363**.

VGM Insurance SERVICES