What You Need to Know About Ransomware

Protect yourself from this growing threat.

BY JAMES D. KRICKETT

Ransomware has long been thought of as an economic nuisance but the recent proliferation of well-publicized cyberattacks has revealedransomware to be a serious national security threat. Still largely hidden from public view, rarely making the headlines, are the attacks on small businesses and professional practices, including many podiatry professionals.

A ransomware attack on Colonial Pipeline led to gas shortages and resulted in a 75-bitcoin ransom payment of about $4.5 million. An attack on JBS SA, the world's largest meat processor, was resolved with a ransomware payment close to $11 million. Surprisingly, however, while ransomware has become a multibillion-dollar threat, the average payment demanded was only $310,000 in 2020, with many payments in the $25,000 to $30,000 range.

The increase in ransomware attacks in recent years has proven to be an extremely lucrative criminal enterprise. Targeted victims believe that paying the ransom is the most cost-effective way to get their data back—something that may also be the reality.

Unfortunately, every single business, practice, or organization that pays to recover their files is directly funding the development of the next generation of cyber threats. As a result, ransomware attacks continue to evolve, with more sophisticated variants. So, too, do the costs for victims continue to increase.

What can a podiatry professional or practice manager do to reduce the risk of becoming a ransomware victim? The ethics and morality of making these payments aside, the question of how to make a ransomware payment and how to use the cybercurrency market require planning. Fortunately, there are steps that can be taken via taxes and insurance to reduce the pain of many ransom payments.

The increase in ransomware attacks in recent years has proven to be an extremely lucrative criminal enterprise.

What Is Ransomware?

Ransomware is a type of malicious software or malware that prevents a practice or business from accessing its computer files, systems, or networks and demands payment of a

Continued on page 98

Ransomware (from page 97)

ransom for their return. Ransomware can unknowingly be downloaded onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Ransomware attacks were first seen in Russia between 2005 and 2006, according to several experts. Among the early reports was a case that involved a variant that zipped certain file types before overwriting the original files, leaving only the password-protected zip files in the victim's system. The ransom demanded: $300.

Once the code is loaded onto a computer, it will lock access to the computer itself or to data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers. Obviously, ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

In many situations, users are unaware their computers have been infected. It is usually discovered only when data can no longer be accessed or a computer message pops up alerting users to the attack and demanding ransom payments.

Paying the Piper—Or Not

Top U.S. law enforcement officials have long attempted to discourage meeting ransomware demands. The FBI is currently doubling down on its guidance to affected businesses and professional practices and their message remains: don't pay the cybercriminals.

Ransom payments vary depending on the ransomware variant and the price or exchange rates of digital currencies. However, paying ransom in a ransomware attack is not as easy as wiring money from a bank or filling a suitcase with hundred-dollar bills.

Today, ransomware attacks usually call for cryptocurrency payment to unlock kidnapped data with amounts ranging from a few hundred to even millions of dollars. On the lower end of the scale, alternative payment options are frequently employed using iTunes and Amazon gift cards. Surprisingly, small scale ransomware attackers often demand payment to be wired through Western Union or paid through a specialized text message. But it is the anonymity offered by cryptocurrencies that makes this the ideal payment vehicle.

Payment Mechanics

Bitcoin is the most popular currency demanded by ransomware attackers, but other cryptocurrencies such as Ethereum, Zcash, and Monero are also frequently demanded. Although traditional financial institutions reportedly have their hands tied when it comes to ransomware payments under the money-laundering and know-your-customer regulations, the first step in any ransomware attack should be to contact the podiatry practice's bank to determine if they transfer funds to a cryptocurrency exchange and if there are any limits. Most ransomware victims will buy cryptocurrency through an exchange. Buying cryptocurrencies from exchanges is a simple process and can be done using normal banking methods such as a credit card or bank transfer.

Fiat-to-crypto exchanges like Coinbase, where you trade real money for cryptocurrencies, are the best place to buy Bitcoins. If you already own cryptocurrency but need to exchange it for another type, for example swapping Bitcoin to Ethereum, a crypto-to-crypto exchange such as Binance may be more suitable.

Regulated exchanges will require you to register to help avoid issues around money laundering regulations. Naturally, there will likely be fees for buying, trading, and moving cryptocurrencies on exchanges and cryptocurrency value will vary among exchanges as no single source dictates the exchange rates. It should be noted that funds held in custodial accounts are usually FDIC-insured for up to $250,000.

Unfortunately, paying the ransom does not guarantee that users will get the decryption key or unlock code needed to regain access to the infected computer system or files being held hostage. Successful or not, however, there may be insurance to cover both the disruption expenses and the ransomware payment itself. Most importantly, the government offers a little-noticed incentive for those who do pay: the ransom may be tax deductible.

Unfortunately, paying the ransom does not guarantee that users will get the decryption key or unlock code needed to regain access to the infected computer system or files being held hostage.

Taxes to the Rescue

Tax deductibility is part of a bigger quandary stemming from the rise in ransomware attacks. The government does warn payments that fund criminal gangs could encourage even more attacks. But failing to pay a ransomware demand can have devastating consequences for any podiatry professional—or his or her practice.

Fortunately, any practice that pays ransomware may be entitled to claim a tax deduction on their federal tax returns. After all, in order to be deductible, business expenses should be considered "ordinary and necessary." Losses from more traditional crimes such as robberies or embezzlement have long been deductible so, in all likelihood, are today's ransomware payments.

Naturally, there are limits to the deduction. If, for example, the practice's loss is covered by insurance, especially the increasingly popular cyber coverages, the practice can't claim a deduction for any payments made by an insurer.

Insurance

The question of whether traditional insurance policies provide cov-

Continued on page 99

Ransomware (from page 98)

erage for losses due to cyberattacks and cybersecurity breaches is, at least temporarily, yes. A federal court in Maryland recently ruled that an insurance company must cover the costs of software, data, computers, and servers that were lost or damaged by ransomware under the property insurance coverage of one business owner's insurance policy.

Business interruption insurance can help the podiatry practice regain some of the financial loss that results from a security breach.

Since ransomware attacks are becoming easier for cybercriminals to execute, it makes sense for every podiatry professional to think about fortifying the operation's digital assets and making sure they have business interruption coverage in the event of an attack.

Business interruption insurance can help the podiatry practice regain some of the financial loss that results from a security breach. Without business interruption insurance the podiatry practice could not make up any income lost due to the disaster—the ransomware attack.

To protect against cyber risks, a number of practices are beginning to add cyber or cyber liability coverage to their business insurance policies. So-called "data breach insurance" helps a podiatrist respond to breaches and usually offers sufficient protection for most professional practices and small businesses. Cyber liability insurance, on the other hand, is typically used by larger businesses and offers more coverage to help prepare for, respond, and recover from cyberattacks. Cyber extortion is a coverage option under many cyber liability policies. It protects a practice against losses caused by ransomware as well as other types of cyber extortion.

What's Covered

Many cyber liability policies cover three types of expenses that commonly result from an attack:

- Ransom Money. This is money paid to a cybercriminal in response to a threat. Some policies also cover property (other than money) relinquished by a victim to an extortionist.
- Extortion-Related Expenses. These are expenses incurred as a result of the extortion threat. Examples are travel expenses incured when making a ransom payment and the cost of hiring a security expert to provide advice on how to respond to a threat.
- Most Repair Costs. Payment of a ransom does not guarantee the practice's computers and data will be undamaged after their release, or that they'll be released at all.
- Most cyber liability policies cover losses sustained

Continued on page 100

Ransomware (from page 99)

by the practice as a result of damage, disruption, theft, or misuse of its data. Policies cover the cost to restore, replace, or reconstruct programs, software, or data.

It should be noted that most cyber-related policies require the insurer's permission before any ransom amounts are paid. The same requirement also applies to extortion-related expenses. And, although most cyber-related insurance policies reimburse ransom payments and related expenses, they don't pay these costs upfront.

Extortion-related expenses, including the cost of hiring a security expert for advice on responding to these threats—and ensuring they don't happen again—obviously deserve attention. Since payment of a ransom does not guarantee the podiatry practice's computers or data will be unchanged after their release, expenditures to restore, replace, or reconstruct programs, software, and data may also be necessary.

Avoiding the Inevitable

While it is frightening to think that nothing can be done when faced with a cyberattack, being prepared for the potential lost revenue/income during downtime due to an attack is as important as preemptively assessing what cybersecurity measures are already in place.

Whether just one computer or device in the practice falls victim to a ransomware attack, or hundreds of computers or devices get locked up, advanced planning is strongly advised by security experts. Without prior planning, it can take anywhere from four- to five hours from the time a ransom attack is launched to when a payment is made.

Ransomware attackers, indeed all malware distributors, have grown increasingly savvy requiring extreme caution about what is downloaded or clicked on. Obviously, the best way to avoid being exposed to ransomware, or any type of malware, requires caution whenever the podiatry practice's computers are used—by everyone. However, even simple steps taken by a podiatry professional or the practice manager can help ease the bite of a ransomware attack, including these basic cybersecurity hygiene and best practices:

- Keeping operating systems, software and applications up-to-date
- Ensuring anti-virus and anti-malware programs update regularly and scans run on a regular basis
- Backing-up data regularly, double-checking that those back-ups were completed
- Securing those back-ups and ensuring they are kept separate from the networks and computers that were backed up, and

Continued on page 101

Ransomware (from page 100)

• Most importantly, creating a plan in case the practice is the victim of a ransomware attack.

The End Game

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) recently warned against making ransomware payments at the risk of violating economic sanctions imposed by the government against cybercriminal groups or state-sponsored hackers.

Still, when pushed into a difficult situation, some podiatry professionals may feel as though they have no option other than paying the criminals the ransom demand. The fact is, these attacks are costly and disruptive—whether or not the criminals are paid to return access to locked systems.

The rise of ransomware attacks over the last few years has created an extremely profitable criminal enterprise. Targeted businesses, organizations, and even governments often feel paying the ransom is the most cost-effective way to get their data back. However, it is an unfortunate fact that payment may be the best option.

Hearings held by the Senate Judiciary Committee revealed that it is small businesses that are bearing the brunt of ransomware attacks. According to the committee's chair, Dick Durbin (D-IL), small businesses make up over half the victims, with the committee's ranking minority member, Chuck Grassley (R-IA), putting the number at three out of every four.

More than half (56%) of ransomware victims paid the ransom to restore access to their data last year, according to a global study of 15,000 consumers conducted by global security company Kaspersky. Yet for 17% of those, paying the ransom did not guarantee the return of stolen data. It is virtually impossible to completely eliminate the risk of a ransomware attack.

Preparedness only goes so far in protecting against these increasingly more sophisticated attacks.

Were ransomware to change in a few years, it would not be surprising. In terms of potential, it can evolve into malware that disables entire infrastructures until a ransom is paid. Online extortion is bound to develop from taking computers and servers hostage to eventually doing the same to any type of insufficiently protected connected device, including smart devices and critical infrastructures. The return on investment (ROI) and opportunities for development that the targeted approach has opened will ensure that it continues in the future.

Obviously, podiatry professionals need to be prepared for the possibility of more threat actors or groups shifting to and joining the ransomware bandwagon. The theme of double extortion seems to indicate how ransomware operators will continue to find new ways of increasing the stakes for their victims and cornering them into meeting their demands instead of just walking away. **PM**

James D. Krickett is a well-known tax and financial adviser whose columns are syndicated to more than 65 publications each week. His features routinely appear in the pages of leading trade magazines and professional journals.