JumpStart

**Are you prepared for a cyberattack?  
How to keep your data and patient files safe**

*By Terra Shastri - Ontario Veterinary Medical Association’s Director of Business Development and Strategic Initiatives*

A regular day at the clinic turned into a potential nightmare when Dr. Matt Croskery, practice owner at Oakpark Pet Hospital in Oakville, Ont., couldn’t access a digital X-ray.

“We tried to access another X-ray, but again, we couldn’t access it, so we called Idexx and it confirmed it wasn’t an issue on their end,” he says. Eventually, the problem was identified as ransomware.

Ransomware is malicious software designed to block access to a computer system until a sum of money is paid. Paying the ransom doesn’t guarantee your data will be restored (for more information on ransomware and cyber crime, see page xx).

After unplugging all 24 of their computer stations, Martin Brassard, an IT professional from Progressive Thinking, advised the clinic not to use any of their computers due to the risk of the virus regenerating and freezing Oakpark’s files and data.

“If you believe your computer or server is infected by a virus, malware or ransomware, the first thing you should do is unplug the network cable, turn off all wireless connections and don’t connect any of the connected USB memory devices to another computer until they’ve been scanned for the virus,” Brassard explains.

**Why it could happen to you**

Nancy Dewitz, a veterinary technology consultant with Beyond Indigo Pets, says veterinary practices are often easy targets. “The programmers behind ransomware see veterinary clinics as easy targets because they know how valuable the patient files are to a veterinarian, and they also know most veterinarians don’t think anyone would be interested in their data,” she says.

Most veterinary teams might think their client and patient information wouldn’t be valuable to a hacker, but it’s really about how valuable the information is to the clinic. How much are veterinarians willing to pay to get their patient files back?

Ransomware can linger in the background on a computer network until it’s triggered. “The hacker doesn’t care when it happens, since they’re doing this to multiple people or businesses,” says Dewitz. “They just look to have it triggered to take over the system, so the owner/user can’t get any access to their files.”

For Dr. Croskery, it was tempting to pay the ransom, so he could continue operating for the day. “We had a fully booked schedule for the day,” he says. “Shutting down the entire server meant we couldn’t call clients. We didn’t know which clients had appointments booked. We had clients coming into the clinic, but we didn’t know what they were here for. I had 15 staff scheduled, but there was nothing they could do. I just thought, ‘That’s it, we’re done because we’ve lost everything’.”

After Brassard screened all computers, he was able to determine only the hard drive was infected, not the backup drive. The process of getting an IT team to the clinic to “clean” the computers and download the backup took eight hours. It ended up being a costly day. Luckily, the ransomware was discovered first thing in the morning, so Oakpark only lost 90 minutes of data.

**Prevention**

Prevention is key when it comes to protecting your data and patient files. Whether it’s preventing viruses and ransomware or a fire or a flood, prevention of data loss is important.

Dewitz has witnessed significant data loss in a veterinary practice and knows how expensive it can be for a hospital. She says most clinic teams are unaware of what information is being backed up sufficiently.

“Often, hospitals will purchase auxiliary systems such as a digital X-ray, plug it into its existing network and assume it will be backed up with the rest of the hospital’s digital information,” she says. “But it doesn’t work that way.” Radiographs and ultrasound images are especially important because they’re a snapshot in time and can’t be duplicated once lost.

It’s important to take inventory of the types of data you store. Go through every computer in the hospital to see what kind of files are on each computer. Determine if the data is:

1. **Mission critical:** Practice management data, medical record data, images, accounting data, lab data
2. **Critical:** Client documents, document templates, employee records
3. **Noncritical:** Newsletters, past calendars, anything that may never be needed again but is important to have on file
4. **Personal:** Staff pet pictures, vacation pictures, funny videos, etc.

Once you’ve collected inventory of the data stored, you can determine what needs to be backed up to off-site storage. Mission critical and critical information should be backed up both on site and off site automatically. Dewitz strongly recommends backing up everything on site because it provides immediate access to data, it’s less expensive and Internet access isn’t required. However, in the event of a catastrophic event, on-site data storage can be destroyed. By having both on-site and off-site backup, a problem with one can be offset by data recovery from the other.

**On-site vs. off-site storage**

Consider your on-site and off-site options for backing up your hospital’s information. Off-site back up means using cloud-based storage.

“Storing data in the cloud means you send data over the Internet to a secure server (the cloud) where it’s stored,” says Dewitz. When considering cloud storage, Dewitz says it’s important to research and choose the right company. “Be sure it is a reputable business where everything sent to the cloud is encrypted, including the information from your practice management software,” she says.

On-site storage entails storing important data on a regular basis on local storage devices, such as network attached storage (NAS), removable hard drives or tape storage. NAS drives connect to a router via ethernet or Wi-Fi and are visible to any computer connected to that network. Because they operate over your network, NAS drives centralize backup for all the computers in the hospital.

Removable hard drives allow for easy transfer and better connection from your computers’ internal to external hard drive. The main disadvantage is they can be easily damaged if dropped or shaken, and removable hard drives can be affected by heat, magnetism and sunlight.

Tape storage is one of the least expensive forms of storage, allowing you to store more data for less money than other options, but it can be slower to access the data.

**Educate, protect and backup**

In Dewitz’s experience with vet clinics, a computer virus is usually traced back to a staff member “unintentionally opening the door and giving the hacker the key.” Sometimes staff are contacted over the phone by a person posing as a Microsoft representative who will walk the staff member through a few steps that allows the hacker to gain remote access to infect the computer.

“There tends to be a misconception that the younger generation knows technology and therefore they will be careful not to infect a computer by clicking on an infected link or giving a hacker access to the computer network, but that’s not the case,” says Dewitz. “This can happen to any of your staff.”

While most clinics have a version of anti-spy and anti-virus software, which is still imperative in keeping computer files protected, many clinics don’t keep it updated. “It’s really important to work with a good IT group to keep up-to-date with protective software,” says Dewitz. “The programmers who create these viruses or ransomware are constantly working on how to get around anti-virus software, so it would be easy for them to infect a vet clinic’s computer system if its anti-virus software has lapsed.”

Separate Wi-Fi for staff and guests is another protective step. Staff, clients or industry representatives may innocently request Wi-Fi access, making it easy for anything infected on their device to get onto your computer network.

A separate computer in the clinic is recommended for times when a device, such as a USB stick or mobile phone, is needed to upload or transfer files. “Sometimes staff will upload pet pictures from their phone or a USB stick, and end up infecting the clinic computers because of a virus on their device,” says Dewitz.

Dr. Croskery used to back up his hospital’s data once a week, but now it’s backed up three times a day to an off-site server. He also unplugs the external hard drive. “We would have to start from square one if the backups were infected, so we’re doing everything possible to ensure that doesn’t happen.”

Brassard recommends regular testing and maintenance of back-up servers. He says it’s also important to know where all your disks are to reinstall your software and to know your passwords. “It will help save time if you must rebuild your system,” he says. “With a good backup and disaster recovery strategy, you should be back up and running within a few hours with minimal data loss.”

Dewitz says veterinary hospitals need to make data protection a priority to prevent expensive, unnecessary loss of patient files, images and other documentation. “A clinic is only as good as its last back up,” she says. Everyone on the team needs to understand the importance of backing everything up and understand the consequences of data loss. Dewitz recommends talking about it at every staff meeting so it’s top of mind for everyone.

“Making sure that data is constantly backed up is just as important as locking the door at night, and it needs to be part of the regular routine in running a hospital,” she says.

--

SIDEBAR

**What’s the difference between malware and ransomware?**

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer.

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Paying the ransom doesn’t guarantee your data will be restored.

For more information about cyber crime, and cyber and crime insurance, see page XX.