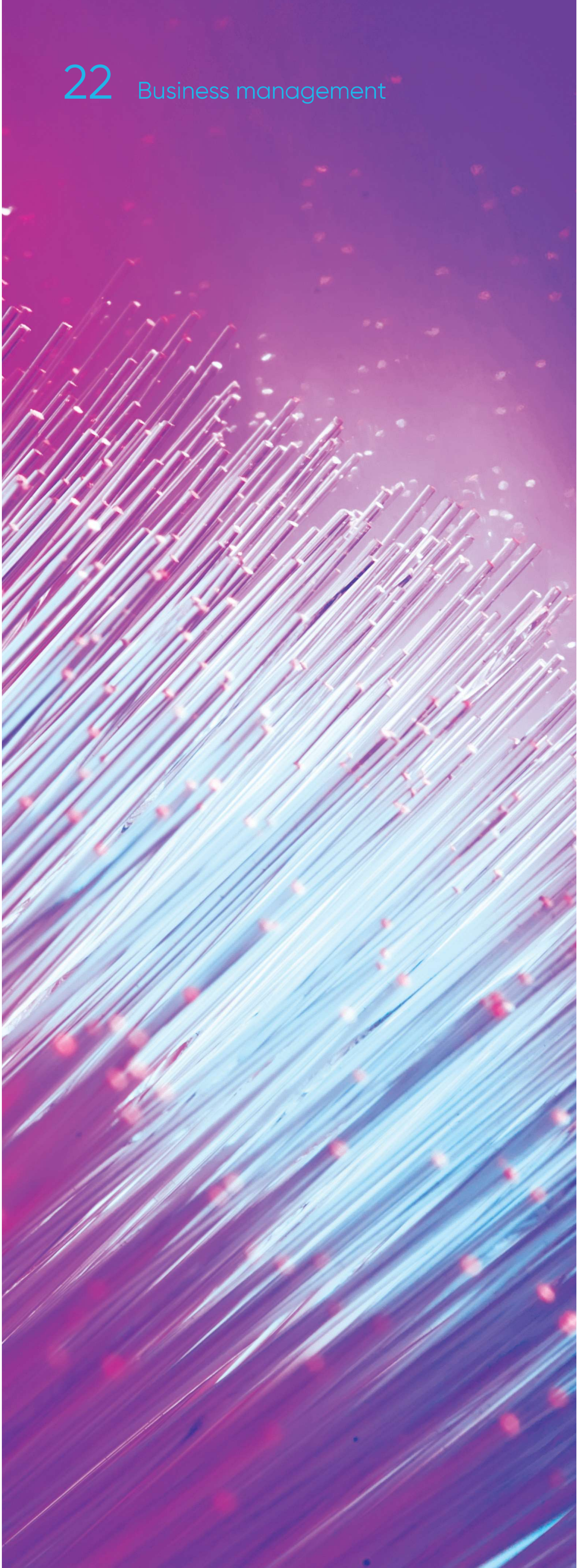

How to protect your veterinary practice from cybersecurity threats

Cybersecurity hygiene is crucial for your safety and success

Article by MWI Animal Health

As an independent veterinarian, it can be tempting to overlook cybersecurity measures. After all, how much do cybercriminals really target small businesses?

The answer to that question may surprise you. The latest report found that 46 percent of security breaches involved small and medium-sized businesses of all types, defined as fewer than 1,000 employees.[1] This is likely because smaller businesses tend to be easier to hack because they often don't have the security measures larger businesses do.

Veterinary practices can be a particularly attractive target for cybercriminals. Why? Because they store large amounts of the type of data would-be thieves crave, like customer names, addresses, and credit card data. If that wasn't convincing enough, data breaches can be expensive for any business, ranging anywhere from $826 to $653,587, with a median cost of $21,659.[1]

Translation: Cybersecurity is something all businesses, including veterinary practices, need to take seriously.

Common cyberthreats

Criminals use several different tactics to attack businesses.

- **Phishing**
  Phishing uses malware to gather sensitive data, usually through email. The email often looks legitimate, so the reader clicks on a link or opens an attachment that triggers the illicit data retrieval. Phishing is increasing too. It occurred in 25 percent of data breaches in 2020 and went up to 36 percent in 2021.[2]
- **Malware**
  Malicious software, also known as malware, is any software created to purposely damage devices, servers, computers, and networks.
- **Ransomware**
  Ransomware is a type of malware that disables the use of the computer or network until a ransom is paid. It's typically activated through phishing emails. Ransomware is also on the rise. It was used in 10 percent of breaches in 2021, more than double the amount in 2020.[2]
- **Viruses**
  Cybercriminals may use viruses to get into the system. As the name implies, these destructive programs spread to other computers, networks, and connected devices.

How to stay safe

Thankfully, there are tried-and-true steps veterinary practices can take to protect themselves from cyberthreats.

1. **Perform a risk assessment**

   Knowing where the practice is at risk is the best way to start down the road to better cybersecurity practices. There are several free online government tools that can help.

   - The Federal Communications Commission (FCC) has a cyberplanner you can customize.
   - The Department of Homeland Security (DHS) offers a nontechnical assessment of cybersecurity practices.
   - DHS has several different types of other cybersecurity assessments available too.

2. **Educate employees**

   Employees that click on links or attachments in phishing emails are a significant cause of data breaches in small businesses. With this in mind, it's smart to make sure employees know the basics of good cybersecurity hygiene. A great resource for this is DHS's STOP. THINK. CONNECT. campaign. The site gives advice on how to practice good cybersafety habits and offers multiple resources such as tip sheets, videos, infographics, posters, and research. This can all be utilized to educate employees so they can help keep the veterinary practice safe.

3. **Back up data regularly**

   A good backup system is a must, especially when storing other people's sensitive information. Back up essential data — documents, spreadsheets, financial files, and customer records — regularly to multiple places (for instance, the cloud, a hard drive, and a portable storage drive). Do this at least every 24 hours, if not more often. Store extra backups away from the office. Only keep the data you absolutely need to do business. The less information you have stored, the less a cybercriminal can steal. Strong encrypting of that information is key too.

4. **Use complex passwords and enable multifactor authentication**

   Create passwords that use a mixture of characters — upper- and lowercase letters, numbers, and symbols. Always use different passwords for different accounts and don't reuse old ones. Change the passwords frequently. Get a password manager to generate new passwords, perform security checks, and keep track of the credentials for all your accounts.

   It's also a good idea to enable multifactor authentication, at least on the practice's most sensitive accounts (email, banking, accounting, etc.). Multifactor authentication means that when users sign in, they have to provide additional information to access the account. This could be a one-time security code that's sent via text, email, or an authenticator app, or a series of personal questions.

5. **Keep everything updated**

   Make sure that all your computers and devices are set to perform automatic updates. This keeps your systems and network secure. Enable automatic updates on all the software and apps you use too, such as Chrome, Adobe Reader, and Microsoft Office. If you're using an operating system that isn't supported anymore (such as Windows 7 or Vista), plan on an upgrade. Cybercriminals love targeting unsupported software.

6. **Invest in firewall, internet security, and antivirus software**

   A good firewall, internet security, and an antivirus subscription are a must. These protect your devices from viruses and malware, protect your data, and scan websites and downloads to keep you safe online. Whenever you connect a new device to your network, be sure to have your security software scan it for malware and viruses.

7. **Enable spam filters in email programs**

   As mentioned before, cybercriminals love using emails to hack people's systems. A spam filter can weed out a good chunk of the malware and phishing scams that come through.

Continued on next page

8. **Look into insurance**

   An insurance policy can protect veterinary practices if there's a data breach. The insurance broker can also help develop a plan, so practices know what to do if it happens.

9. **Consider further cybersecurity education**

   The U.S. Small Business Association has regular cybersecurity training events. So does the National Cybersecurity Alliance.

Vetting third-party vendors

Many veterinary practices use third-party vendors for solutions like telehealth and practice communications. But how do these third-party vendors enter into a healthy cybersecurity program?

It's unfortunate but true — more than half of organizations have had a data breach caused by a third party. Here's what to do to minimize risk.

1. **Ask questions**

   How much sensitive information will you need to share with the vendor? How much access and control of the practice's data will the vendor have? Does the vendor have the same values concerning customer privacy that the practice has?

   Is the vendor using proper security measures with their own devices and networks? Are they keeping them updated?

   Is the vendor compliant with all applicable regulations? For instance, if they're processing customer payments, are they complying with Payment Card Industry (PCI) standards?

2. **Get references**

   Ask the vendor for access to other customers — former and current — to find out what their experiences have been.

3. **Put it in the contract**

   When you choose a third-party vendor, it's best to get everything in writing. Here are some ideas for what to include in vendor contracts:

   - Decide who is liable for what should a data breach occur.
   - Determine what security standards the vendor will use to safeguard data.

4. **Restrict vendor access**

   Only give vendors the data they absolutely must have to do their job, for only the amount of time they need it. The rest should be off limits.

What to do if there's a data breach

Ideally, there's already a step-by-step response plan in case a data breach occurs. If not, here's what to do.

1. If possible, determine what happened and what data has been lost.
2. Call information technology (IT) experts who have experience with data breaches. They can find security holes and plug them, as well as give advice on the next steps. They can also help develop a response plan in case a data breach happens again.
3. If a third-party vendor has a breach, make sure they've taken steps to fix it.
4. Notify the affected parties. They may be at risk of identity theft. This is especially important because it's the law (check the legislation in your state). Transparency with customers about the problem is best anyway to nurture trust in your relationship.

Bottom line

Data breaches can cost veterinary practices time, money, and their reputation. Sometimes, the fallout is so great, businesses can't recover. This is why it's so critical to take proactive steps to protect your practice from cyberthreats. You're keeping your customers' personal information safe, guarding your business against harm, and making sure your practice is around for the long haul.

References

[1] Verizon. "DBIR: 2021 Data Breach Investigations Report." May 2021. Accessed 23 May 2021. Available online at **enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf**

[2] Verizon. "DBIR: 2021 Breach Investigation Report: SMB snapshot." 2021. Accessed 23 May 2021. Available online at **enterprise.verizon.com/resources/reports/2021-dbir-smb-snapshot.pdf**