By Ed Branam, DVM, CIC

The Hidden World of Cybercrime

Poor network security can leave a veterinary practice's data and other assets vulnerable to theft and exploitation.

No business is immune to cybercrime. Unfortunately, smaller companies are easier to victimize because they frequently lack the organizational depth, expertise, and technical and financial resources of larger businesses. They also are more likely to use outdated computer operating systems. Would you believe that 10% of companies reportedly still use Windows 7?

During a presentation at the 2023 VMX conference, the presenter, an attorney specializing in cyber-related exposure, was quoted as saying, "There are two types of businesses — those that have been hacked and those that don't know they have been hacked." The assertion might be slightly exaggerated, but a critical point was made.

Ransomware is the most common form of cyberattack. It typically focuses on charging a ransom to prevent a hacker's destruction of critical business computer data or its release into the public domain, typically the dark web. Lacking the resources to address a ransomware incursion immediately, some businesses see paying the ransom as an inviting solution. Unfortunately, studies show that agreeing to such a demand increases the likelihood of a recurrence. After all, the infiltration became a proven payday for criminals.

Think Outside the Box

Given the global outsourcing of services, veterinary businesses look to vendors, a relationship that often requires sharing sensitive data. Partners such as call centers, point-of-sale credit card processors, payroll administrators and cloud-based data storage providers handle sensitive information on behalf of businesses. Still, the customer (your veterinary practice, for example) bears ultimate responsibility for protecting the information and responding appropriately in case of a breach.

An IBM Institute study revealed that almost half of all data breaches occurred while the information was with a third-party vendor. Therefore, when you do something as simple as transmitting point-of-sale credit card information to your financial institution, you likely incurred significant cyber exposure. It doesn't matter whether you save the credit card in your computer system because hackers can access the data during its electronic transmission or from the point-of-sale device's cache.

A Google search illustrates how easily and inexpensively someone can use the dark web to purchase information about an individual or business.

- For $1, you can obtain the tools to install a malware application on a business computer system.
- For $4, you can get someone's date of birth and social security number.
- For $15, you can receive bank account or credit card CVV (card verification value) information.
- For $20, you can acquire a digital copy of a fake driver's license or passport.

Cyber thieves commonly use such information to fraudulently:

- Withdraw money from bank accounts.
- Obtain new credit cards.
- Make online purchases.
- Borrow money from a bank.
- Submit health insurance claims.
- Pay off debt.

Problem Areas

How is your veterinary practice at risk? Let's focus on vendor-related cyberthreats, including:

- **Supply-chain vulnerabilities:** All practices rely on vendors for an ever-expanding list of products and services. For example, some vendors help maintain inventories. If a vendor has weak cybersecurity, attackers could exploit the company's computer system to access your network.
- **Third-party software:** Poorly designed software and applications might have security vulnerabilities or back doors that cybercriminals can use to compromise your data.
- **Data sharing:** Vendors often require access to your data for legitimate purposes. Mishandled or inadequately secured information can be exposed, leading to a breach.
- **Subcontractors:** A vendor sometimes hands off work to third parties. You're probably not aware of their cybersecurity practices.
- **Lack of monitoring:** Most veterinary businesses do not closely watch or audit their vendors' security. The lack of oversight can create vulnerabilities and financial liabilities.
- **Cloud services:** Many businesses rely on cloud data-storage providers. If the vendor experiences downtime or a breach, your operations can be disrupted and your data exposed.

Security Checklist

Veterinary practices can protect themselves from cyberattacks originating with vendors through:

- **Risk assessment:** Ask about a vendor's security policies and procedures and its compliance with standards such as the HIPAA Security Rule or General Data Protection Regulation (GDPR).
- **Contracts:** Make sure vendor agreements include clauses that cover cybersecurity responsibilities, incident responses and liability.
- **Communication:** Maintain open channels with vendors.
- **Teamwork:** Collaborate with vendors to establish how they would address a breach promptly and effectively.
- Training: Inquire how vendors teach their employees about security best practices and data protection.
- **Data security:** Ensure that sensitive information exchanged with vendors is encrypted during transmission and storage.
- **Logging:** Continuously monitor vendor activities on your network to detect suspicious or unauthorized actions.
- **Exit strategy:** Develop a plan for transitioning to another vendor seamlessly and without compromising security.
- **Third-party insurance:** Consider purchasing cyber insurance to mitigate the financial risks associated with vendor-related incidents. Among the top cyber insurance coverages requested by businesses are data breach, data restoration, cyber extortion and ransom, business interruption, funds transfer fraud, and social engineering.

Many proactive risk-management strategies require a significant amount of expertise. I recommend contacting your insurance agent, risk-management team or outside cybersecurity professional for assistance. Also, check out the Federal Trade Commission's "Cybersecurity for Small Businesses" top 10 tips at bit.ly/3FH8NkC.