Secure Your Data

A data security risk is a risk to the existence of your business

by Carolyn C. Shadle, PhD, and John L. Meyer, PhD

IMAGINE THIS HAPPENING AT YOUR PRACTICE: You are enjoying a staff holiday party when the police come and arrest your receptionist, in front of the entire staff. That is just what happened to a Los Gatos, Calif., small animal practice. Its receptionist was accused of stealing clients' credit card information, which she allegedly forwarded to a boyfriend. Of course, the practice then had to contact clients who may have been affected and to deal with two clients who threatened to sue.

Or imagine that your computer system is hacked. Instantly, your security has been compromised. Your records are exposed. Your clients have lost their privacy. The importance of data security now becomes vital to the existence of your business.

How can you tell your clients that you and they have been robbed? What can you say? What amends must be made? And how do you prevent it from happening again?

It could happen any time. You have clients who give you their checks or their credit or debit card numbers, trusting you to protect their personal information in addition to providing good treatment for their pets.

Craig Claney, the general manager of AVImark, observes that it is also necessary to consider the possibility of a team associate leaving the practice with a client list.

Exposure of such information not only is embarrassing, time-consuming to manage, and damaging to your reputation, but it can also be costly.

The more people and businesses are online, the more vulnerable they may become.

According to a 2011 study from the Ponemon Institute, the average reported data breach cost per individual compromised is $214. Multiply that by the number of client records you have, and then imagine writing a check for this total amount, losing this money right off your bottom line!

In addition to the direct costs of a data breach, such as notification and legal defense costs, there are also indirect costs, like lost customer business.

What is a data breach?

Data breach refers to loss, theft, accidental release, or accidental publication of personal identification information (PII). That includes Social Security numbers, bank account numbers, credit or debit card numbers, driver's license numbers, full names, home addresses, email addresses, telephone numbers, and even your employees' medical insurance numbers.

Increased awareness of cyber attacks

Following the widely publicized customer credit and debit card hacks experienced by Target in 2013, more businesses have taken note of the data security risk they might face.

However, in 2014, retailers such as Goodwill Industries, Dairy Queen, P.F. Chang, Neiman Marcus, and The Home Depot reported point-of-sale breaches. In 2015, new warnings to protect personal information were issued following a cyber attack on the health benefits company Premera Blue Cross as well as on Anthem—the largest health care data breach in history, potentially involving account information for 80 million customers.

In February of this year, 30 high-level security executives met in Chicago to network and share strategies to better protect themselves and others.

Small businesses are also affected

Unfortunately, large businesses are not the only ones affected; the cyber threat against small business is also growing. The 2013 Verizon Data Breach Investigation Report (DBIR) showed that 31 percent of all data breaches investigated in 2012 occurred in organizations with fewer than 100 employees.

Kevin Stecko, the owner of specialty T-shirt maker *80sTees.com*, was notified by Discover that cardholders using his website had experienced suspicious transitions in their accounts. It was finally determined that a former senior executive had breached the system. The company spent $200,000 to resolve the issue—and that figure doesn't count the sales the company lost when it was only able to accept payment through PayPal.

Why are cyber threats increasing?

Although business leaders are increasingly aware of the risk of data breach, the actual number of incidents is on the rise. Why is that?

Adam Little, DVM, who is the director of partnerships and innovation for LifeLearn in Guelph, Ontario, spends a lot of time working with practices to develop online marketing and client communication tools. He says a growing number of clients communicate with their veterinary team through social media, and many want their medical notes sent to them electronically after their visit. However, the more people and businesses are online, the more vulnerable they may become.

This vulnerability is because the mechanisms by which hackers can infiltrate computer systems have been growing by leaps and bounds, and because of the failure of practices to implement sufficient protections.

David Biadog and Thomas Driver, DVM, of Animal Intelligence Software, Inc., Port Orchard, Wash., consult with veterinary practices managing their data and observe that most practices lack technical know-how. Furthermore, if they're not using a cloud-based system, they have no plan to recover their data if it is lost.

Computer users have long thought that the installation of antivirus software would protect them. However, recent experiences have led Jerome Seguar, a senior security researcher at Malwarebytes, to note that antivirus software on its own is no longer sufficient.

Seguar goes on to describe the broader threat of malware, like Trojans, which can open a back door into a computer for hackers; spyware that can record a user's every mouse click and keyboard stroke; and security flaws, like Heartbleed, that are immune to antivirus software.

Now there is another threat: cyber extortion. John Farley, vice president, Cyber Risk Practice Leader at AAHA preferred provider HUB International, explains this new problem causes your computer screens to go blank, and until you pay a ransom, you can't get back up and running.

Veterinary practices are also affected

According to court papers filed in March 2015 in Hempfield Township, near Pittsburgh, a woman who used to work as an office manager at a veterinary clinic was accused of stealing tens of thousands of dollars from the business. Investigators discovered that over a 4-year period, $168,000 more in cash was received than deposited in the bank. The woman was accused of deleting clinic account transactions in cash from the practice accounting program, and also of redeeming $3,200 in vendor reward programs.

Although no PII was stolen in this case, Marsha L. Heinke, CPA, of Veterinary Practice Made Perfect, in Grafton, Ohio, points out that this story highlights a not-so-uncommon theme in veterinary practices: Poor internal controls that don't use data to catch problems before they become large issues could literally bankrupt a practice. Perhaps, too, it serves as a warning to small animal practices to insist on background checks and drug tests for all employees.

It was important personal data that was compromised at the Kettering Animal Hospital in Dayton, Ohio. Twenty-three-year-old Michael Rohrer had worked at the front desk for only 3 months when police visited and accused him of making copies of customers' credit cards. He was fired, and the practice had to send letters to clients. One result: The practice updated its policies and procedures to say that employees can handle money and credit cards only in the presence of the customer.

Louise Dunn, DVM, of Snowgoose Veterinary Management Consulting, in Pfafftown, N.C., works with many practices, reminding them also not to forget to protect data stored in paper files. What is left on desks? Which file cabinets are not locked? One practice with which she worked realized that the files of terminated employees were simply placed in storage boxes in an unlocked area; these files contained a plethora of information, such as tax forms and personal medical information, left out for "easy pickings."

Another practice Dunn visited posted radiation exposure reports for team members in the management office, and on the reports were the names, birth dates, and Social Security numbers of each member. The team members were trusted not to use that data inappropriately, but, she asked, what about members of the cleaning company that came in at night?

Security of your data can go beyond protecting it from computer malware or human theft of information on paper files. What would happen to your data—and your business—in the event of a fire or flood?

Laws addressing data security

Losing data is disruptive. Exposing personal data can be embarrassing. Worse, loss of identity data can result in legal problems. Furthermore, compliance with identity theft prevention laws is not a choice, but a legal requirement—and there are many laws that address data security.

In 2003, the Fair and Accurate Credit Transactions Act was passed. The veterinary industry was ultimately deemed exempt from much of the act, including the Red Flags Rule. Still, Adrian Hochstadt, attorney for the American Veterinary Medical Association, cautioned that this was not cause for being lax or carefree. He wrote in

the online *JAVMA News* for February 1, 2011, "The federal compliance issue may go away now, but you still have a risk management issue. You still have the expectations that clients will be protected."

However, one provision under the Fair and Accurate Credit Transactions Act that applies to veterinary practices requires that businesses accepting credit cards have in place a credit card machine that will remove all but the last four or five digits of a card number and the expiration date from the sales receipt.

Speaking of credit cards, veterinary practices that accept credit cards, either directly or through a third-party vendor, must comply with the Payment Card Industry Data Security Standard. Five credit card companies have set standards and approve credit card software. They also may impose a fine in the event of a breach—as much as $500,000.

The Health Insurance Portability and Accountability Act, better known as HIPAA, does not apply to veterinarian animal health records, but it does include provisions to protect the personal identification information of a veterinarian's employees.

The Fedral Trade Comission (FTC) exists to protect commerce and might become involved in a large breach.

Antivirus software on its own is no longer sufficient protection from data security breaches.

The Federal Trade Commission Act, Section 5, says that a business cannot engage in unfair or deceptive practices. That's a broad statement, but if an unscrupulous nighttime cleaner found a credit card number left on a post-it note, that might lead to a breach and ultimately to an FTC fine.

State laws are also important. Forty-seven states (plus Puerto Rico, Washington, D.C., and the Virgin Islands) require notice to clients after unauthorized access to their private information. Many also require notification of the state attorney general, state consumer protection agencies, and credit monitoring agencies. States have differing laws outlining what information is protected and the required notification procedures. Given that each state is different and the laws are constantly being updated, it is wise to seek the aid of a privacy lawyer or other consultant to interpret the applicable laws.

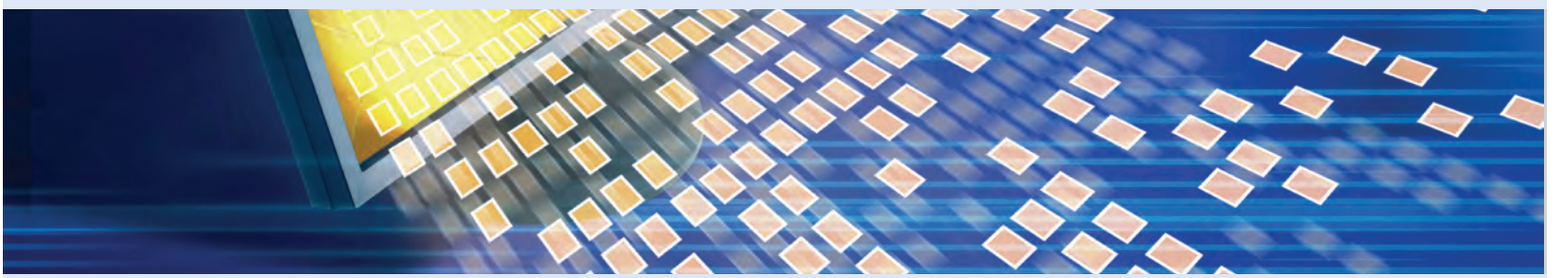
James Iafe, VMD, is one source for consultation and training. He is a 1993 graduate of the University of Pennsylvania School of Veterinary Medicine and has been practicing small animal medicine in Pittsburgh for the past 8 years. After becoming a victim of identity theft and receiving a breach notification letter from his mortgage lender, he determined to help other victims of data breach, particularly veterinary practices. In 2004, he became a Certified Identity Theft Risk Management Specialist (CITRMS) through the institute of Fraud Risk Management and, with Ken Kirschner, CITRMS, formed PrivacyEdge, located in Cranberry Township, Pa.

Six things veterinary practices can do to mitigate their risk

To prevent the headaches described above, it is best to take steps toward prevention. Below are some things you can do.

1. **Prepare an inventory of the private personal information you collect.** For example, know the answers to these questions: What data do you collect, and why? Where is it? How well is it protected? Who can access it? When do you use it? How do you use it?

2. **Prepare a risk assessment, including third-party vendors and contractors.** Talk to your operation systems vendor. Eric Jungmann of the VetFM



Glossary

(terms defined by Wikipedia)

Antivirus software (often abbreviated as AV and sometimes known as antimalware software), is computer software used to prevent, detect, and remove malicious software.

Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read them.

Firewall refers to a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

Heartbleed is a security bug disclosed in April 2014.

HIPAA is an acronym for the Health Insurance Portability and Accounting Act of 1996 and includes provisions for the protection of personal information.

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Phishing is the attempt to acquire sensitive information, such as usernames, passwords, and credit card details—and sometimes, indirectly, money—by masquerading as a trustworthy entity in an electronic communication.

PHI is an acronym for personal health information and is a term widely used in HIPPA regulations.

PII is an acronym for personal identification information, either electronic or on paper.

PCI is an acronym for payment card industry.

Ransomware is a type of malware that restricts access to the computer system that it infects and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

The **Red Flags Rule** was created by the FTC, along with other government agencies such as the National Credit Union Administration, to help prevent identity theft.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. (SQL is a popular database programming language.)

Spyware is software that aims to gather information about a person or organization, without their knowledge, by using their computer. It may send such information to another entity, or sometimes assert control over the computer, without the consent of that person or organization.

A **Trojan** is a non-self-replicating type of malware program containing malicious code. When executed, it carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

A computer **virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be “infected.”

software product swears by systems that operate exclusively on the Mac operating system, which, to date, has been impervious to hackers. Steve Rutkovitz of Choice Technologies recommends that your system have the highest certification level, which is the CompTIA (Computing Technology Industry Association) Security Trustmark. Whatever your system, your assessment should include a review of your contract for ongoing support and updates. It should ensure that you have encrypted all your personal data, enabled your operating system's firewall, and made sure your records are backed up.

3. **Develop policies and procedures.** Policies and procedures can clarify for all of your staff how to keep PII data secure. For example, you will want to define who can have what access to sensitive data, plan for a regular review of your state laws, plan for proper disposal of sensitive data by shredding documents prior to recycling or clearing devices before you dispose of them, and prepare a disaster and recovery plan. Like the aforementioned Los Gatos practice is now doing, you may include a policy not to record clients' driver's license and Social Security numbers.

4. **Conduct training for all staff.** All team members must be aware of the presence of data in its various forms and understand the basics of safeguarding and changing passwords. Your training will ensure that staff members know not to open potential spam or phishing emails and to be cautious about downloading things onto computers. Training should include a discussion of paper files and data in storage cabinets and removable storage devices (like a thumb drive or CD).

   Training for those managing the reception desk should include ensuring that staff verify a client's identity by looking at the driver's license or other picture ID and comparing the signature on the driver's license with the signature on the check. Staff should also secure all checks in a locked drawer or safe.

5. **Review your insurance coverage.** Your general insurance policy won't cover a data breach attack. The company *80sTees.com*, mentioned above, did not have insurance to cover its data theft incident, and the cost of the attack was devastating. Think, too, of the regulatory quagmires you might run into with such a breach.

   To avoid *80sTees.com*'s experience, veterinarians are beginning to consider the wisdom of data breach coverage. Since 2011, AVMA has been offering such insurance. AAHA also offers a Business Insurance Program through HUB International Limited.

   Whether as a rider on existing insurance or a separate policy, coverage can be expected to include the cost of lawsuits that might follow after confidential customer data is stolen. Also included are the costs of notification expenses; public relations and crisis management; and business interruptions due to attacks that cripple websites, acts of extortion, or the introduction of malicious code or viruses.

6. **Plan for a response to a possible data breach.** Hopefully, all of your preventive work will protect you from a hacker or data breach, or even a flood or fire that would compromise your data. But what if there is a breach? What do you do?

   If you have data breach insurance, first, contact your provider. You'll soon learn that there are many things you'll need to do, such as:

Resources

AAHA Business Insurance Program and HUB International, "Data Breach 101—How to Avoid a Virtual Catastrophe," (video), no date, *bit.ly/1KE0qln*.

HUB International Limited, "Data Breach: New Coverage Available for Privacy Exposures," (a description of AVMA data breach insurance), 2015, *bit.ly/1Gku9C0*.

Marc Goodman, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It (New York: Doubleday, 2015).

PrivacyEdge, LLC, *theprivacyedge.com*.

- Taking stock internally—reporting to your staff and contacting your insurance broker
- Reaching out to experts—a breach coach, perhaps a forensics expert, and probably someone with experience in public relations
- Addressing notification obligations outlined by state and federal law as well as by the payment card industry
- Addressing multiple inquiries, such as those from state regulators (for example, the state attorney general), federal regulators (dealing with optical character recognition), maybe federal agencies (for example, the U.S. Securities and Exchange Comission and FTC), consumer reporting, and plaintiffs

Clearly, a data breach can be confusing, costly, and frightening, but regulations are purposeful and remedies are available. Iafe likes to point to the history of the veterinary industry with regard to federal Occupational Safety and Health Administration (OSHA) requirements. OSHA regulations seemed burdensome at first, until it was understood that they were there to protect employees from accidental damage, such as getting acid in their eyes. Likewise, the regulations in place and the protocol that you maintain to protect personal identification information are designed to make your venue a safe place for everyone.

There is much you can do to keep you and your staff and clients' personal data secure. Now is the time to get on the road to data security. ※

Carolyn C. Shadle, PhD, earned her degree from the State University of New York at Buffalo in interpersonal and organizational communication. She now provides writing and training through ICS, Inc. (*icsworkplacecommunication.com*).

John L. Meyer, PhD, earned his degree from the University of Minnesota in communication studies. Through ICS, Inc., he writes and provides training in interpersonal communication as well as speech arts.