Cyberspace: The Modern "Wild West"

By Kathy Noe, CPCU, ARM; Veterinary Insurance Services Company (VISC)

Former President Barack Obama once referred to cyberspace as the "Wild West" where everybody expects the government to act as the sheriff. In reality, while law enforcement certainly has a role to play, it falls upon each of us to recognize the risks and respond accordingly.

By now, it has become a common experience to receive notification from a business regarding a data breach. Generally these notifications come from large business entities such as airlines, hotels, retail and restaurant chains, and even credit bureaus. However, small businesses can also become targets. Veterinary practice owners, therefore, have a dual exposure, not only for themselves as individual consumers, but in their business capacity as well, with respect to third party liability. We will quickly review a few of the most common risks.

Your practice likely stores various data from both clients and employees, including personally identifiable information such as a name, date of birth, social security number, address, email address, phone number, etc. Basically anything that either alone or in combination with other data points, serves to confirm an individual's identity. Certain data is legally protected and any breach may impose liability upon the business, where you may incur considerable expense to notify each affected individual and possibly remedy the consequences. It is also interesting to note that while we tend to think of this in the context of modern "cyber" risk, in reality, old-fashioned paper documents can also be accessed and

used in a fraudulent manner, so simply not being online is no guarantee of safety.

Your practice website or social media presence may be a source of legal liability if you use images of your employees, clients, or their pets without written consent. You are also potentially liable if you post material from other sources which may be copyright protected.

Another possible security gap may occur if you have staff working remotely, typically in roles such as bookkeeping, marketing, etc. In such cases, the employee may use their own laptop, tablet, or email-enabled mobile phone to conduct work tasks. These devices may be more vulnerable to external intrusion if not subject to the same security standards as those used onsite at the practice and directly under the employer's control. Even if the employee is using business-owned devices, those may be stolen or lost, rendering any unprotected data on, or accessible via, the device vulnerable to exploitation if it falls into the wrong hands.

On a side note, aside from cyber security issues, there is another potential liability if employees use personal email or text for client contact. Imagine that a malpractice allegation or Veterinary Medical Board complaint arises and your practice records are incomplete because your employed associate has been communicating with the client via their personal email rather than business email. This will complicate your legal defense immensely.

E-commerce extortion, popularly known as ransomware, is yet another common scenario. These intrusions not only potentially breach confidential information but also may render your entire system inaccessible to you, bringing the practice nearly to a standstill.

Remote "cloud" data storage is one way businesses attempt to manage risk. It certainly has its advantages; however, it does not relieve the business owner of liability for proper use, storage, and protection of third party data.

There are various risk control measures which can be implemented to at least partially address these and other related exposures. They include the following:

- Replace factory default settings on new devices for appropriate security.
- Maintain up-to-date versions of all software on all devices (for example, if you are still running Windows 7, be aware that effective January 14, 2020, Microsoft discontinued any further updates).
- Use robust anti-virus, intrusion detection, and similar programs, also regularly updated.
- Utilize data encryption if you allow remote access to your systems.
- Regularly backup important data, store elsewhere from the primary database, but be aware that external drives are yet another point of vulnerability, in that they are another piece of hardware which can be lost or stolen.
- Explicitly outline company policy regarding acceptable use of employer property and data.

In many cases, it may be advisable to retain the services of an IT professional to assist with these tasks, ideally with a service contract which would require the IT vendor to maintain professional liability insurance.

Most of the risks touched on here are beyond the scope of a standard business owner's policy. However, specialty "cyber insurance" products are available, which typically offer a modular coverage approach where the policyholder can choose from a menu of options. Should you wish to learn more, do not hesitate to reach out to a VISC representative by calling 888.762.3143 or via email at info@visc-ins.com. ■

VISC VETERINARY INSURANCE SERVICES COMPANY

Kathy Noe, CPCU, ARM

Ms. Noe entered the insurance field while still in high school. She obtained her insurance license in 1979 and joined the CVMA's endorsed insurance brokerage firm in 1985. Kathy holds the Chartered Property Casualty Underwriter (CPCU) and Associate in Risk Management (ARM) designations.