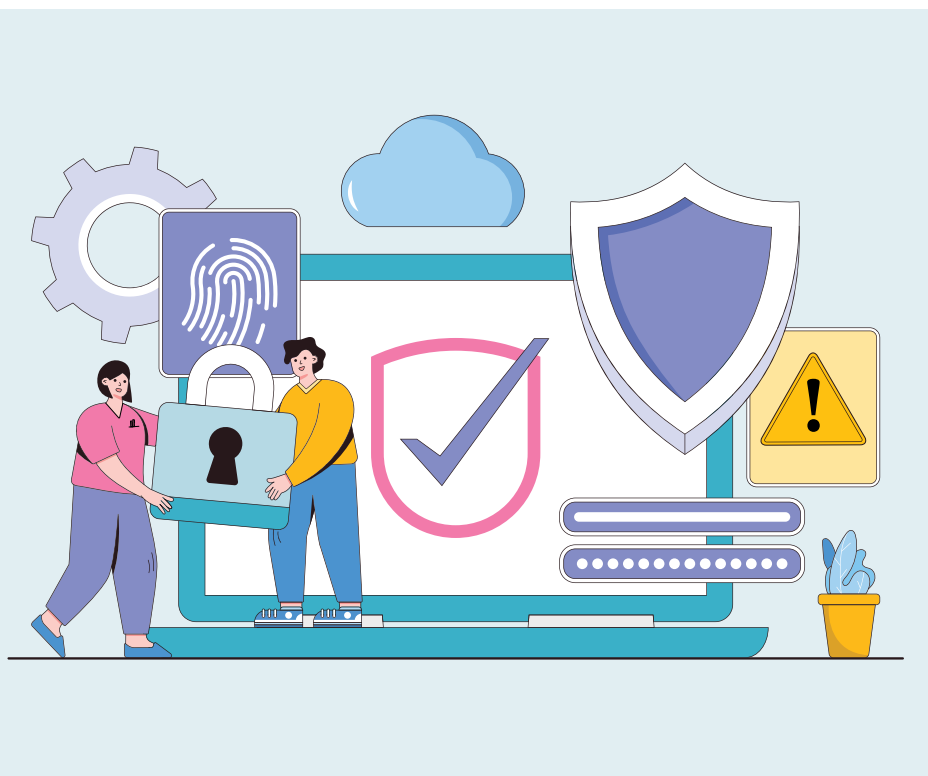


5 Cybersecurity Trends Affecting Your Practice

Protect your hospital, clients and employees by taking a proactive approach to potential threats

BY CLINT LATHAM, JD



As technology continues to advance, veterinary practices are increasingly reliant on digital systems for managing patient records, communication and financial transactions. However, these advancements come with a heightened risk of cybersecurity threats. In order to stay ahead of potential threats, it is crucial for veterinary practices to stay informed about cybersecurity trends and implement appropriate measures to protect their business and clients.

Here are some of the key cybersecurity trends that should be on every veterinary practice's radar:

Increased Reliance on Cloud-Based Systems

The shift to cloud-based systems has been steadily increasing over the past few years, and it is expected to continue this year. Cloud-based systems offer a range of benefits, including improved accessibility, scalability and cost-effectiveness. However, they also come with an increased risk of cyberattacks, as all data is stored in a central location that can be targeted by hackers.

Veterinary practices should ensure that their cloud-based systems are properly secured and that they are

using reputable providers with strong security measures in place. If you really want to be thorough, dig into the pages of your provider's User License Agreement to try to spot any potential red flags. However, there are a couple of quick indicators you should keep in mind. Use firms that promote the ways they protect data. This could mean touting their GDPR, CCPA or even HIPAA compliance. Also, be on the lookout for clauses that claim providers can share data with third-party partners — if you see ambiguous statements about data usage rights, it's worth asking questions.

Growing Threat of Ransomware Attacks

Ransomware attacks involve hackers encrypting a company's data and demanding a ransom in exchange for the decryption key. These attacks have become increasingly common, and the veterinary industry is not immune. In fact, a number of veterinary practices have been targeted in high-profile ransomware attacks. We have seen an increase in the number of fake associate and veterinary nurse/technician applications that are actually ransomware. When the unsuspecting manager or owner opens the résumé, their entire system goes down. The bad news: Without good backups in place, you have to pay to get everything unlocked. If you pay, you also get registered on the dark web as a "payer," thus putting a direct target

on your back for future attacks. To protect against these threats, practices should ensure that their systems are properly backed up and that they have a robust incident response plan in place.

Increasing Importance of Employee Training

One of the biggest cybersecurity vulnerabilities for any organization is its employees. In many cases, cyberattacks are successful because of human error, such as employees falling for phishing scams or using weak passwords. It is crucial for veterinary practices to invest in regular employee training on cybersecurity best practices. This includes everything from password hygiene to recognizing and avoiding potential threats.

It is also important for hospitals' cybersecurity to develop a psychologically safe work environment, which is a critical factor in creating a positive and supportive workplace. When employees feel safe to speak up, ask questions and share ideas without fear of retribution or judgment, it fosters a culture of trust and collaboration. This, in turn, can lead to increased job satisfaction, improved communication and teamwork and ultimately better patient care. In a high-stress and emotionally charged environment like a veterinary hospital, where employees are regularly exposed to difficult cases and volatile situations, psychological safety is especially important. It allows employees to feel supported and valued, reducing burnout and turnover and helping to create a more resilient and successful workplace.

This is important when it comes to cybersecurity. The quicker we can act against the hacker, the better we can mitigate the damage. Often, employees will click on links or sign into fake websites and then try to

Safety First

Veterinary practices can take these steps to improve their overall security.

1 Regularly update software and systems to ensure that they are using the latest security patches and features.

Just like any other business, veterinary hospitals are vulnerable to cyberattacks, and regular updates are essential for maintaining strong cybersecurity. A veterinary hospital's digital assets, including sensitive patient records and financial information, are valuable targets for hackers. Regular updates to software and security systems help ensure that these assets are adequately protected. Updates also help address any vulnerabilities or weaknesses that may be exploited by hackers, including those that could lead to data breaches or other security incidents. Failure to keep up with regular updates can put the hospital's systems and data at risk, potentially resulting in financial losses, legal liabilities and damage to the hospital's reputation.

2 Implement multifactor authentication to prevent unauthorized access to sensitive data.

Two-factor authentication (2FA) is a security measure that provides an additional layer of protection against unauthorized access to digital accounts or systems. With 2FA, users are required to provide a second form of identification, such as a unique code sent to their phone, in addition to their login credentials. This added layer of security significantly reduces the risk of unauthorized access, as it makes it much harder for hackers to gain access to an account even if they have obtained login credentials. Implementing 2FA helps to protect sensitive data and prevent costly security breaches, making it a critical component of any strong cybersecurity strategy.

3 Conduct regular security assessments to identify potential vulnerabilities and threats.

Conducting regular security assessments is a vital aspect of any effective cybersecurity strategy. Security

assessments involve systematically evaluating an organization's digital infrastructure, processes and policies to identify potential vulnerabilities and threats that may compromise data security. By regularly assessing security measures, veterinary hospitals can stay ahead of evolving threats, proactively addressing potential weaknesses before they can be exploited. This helps ensure that data and digital assets remain secure. Moreover, regular security assessments help identify areas for improvement and provide valuable insights for strengthening cybersecurity measures over time. By continuously monitoring and improving their security posture, veterinary hospitals can remain resilient against ever-evolving cyber threats.

4 Train all employees on cybersecurity best practices.

Training employees on cybersecurity best practices and enforcing strong password policies are essential components of a strong cybersecurity strategy for veterinary hospitals. In the event of a cybersecurity breach, veterinary practices should have policies in place for employees to safely report the incident without fear of retribution.

5 Develop a robust incident response plan in case of a cyberattack or other security incident.

Developing a robust incident response plan is critical for veterinary hospitals to respond quickly and effectively in case of a cyberattack or other security incident. An incident response plan outlines the steps to take in the event of a security breach, including who to notify, how to isolate the affected systems and how to recover data. A well-designed plan also includes protocols for communicating with staff, patients and other stakeholders to minimize the impact of the incident. Developing an incident response plan ensures that the hospital can respond quickly and effectively in the event of a security breach, reducing the risk of lasting damage to the hospital's reputation and financial stability.

When it feels like you
against the world,

remember you're
never alone.

delete the email and web history to cover their tracks, all while the hacker has complete access to the hospital's network. However, when an employee in a positive work environment makes a mistake and gets caught in a hacker's scheme, they will immediately ask for help. When psychological safety is built into the hospital's culture, we can greatly reduce our risks of a catastrophic cyberattack.

When
psychological
safety is built
into the hospital's
culture, we can
greatly reduce
our risks of a
catastrophic
cyberattack.

Greater Use of Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are becoming increasingly common in the veterinary industry, from diagnostic tools to data analysis. While these technologies offer many benefits, they also come with increased cybersecurity risks. For example, AI algorithms can be manipulated to produce inaccurate results, or ML systems can be used to carry out more sophisticated cyberattacks. Veterinary practices should ensure that they are using reputable AI and ML systems and that they are properly secured against potential threats.

Emphasis on Supply Chain Security

As veterinary practices rely on a range of third-party vendors for services and products, supply chain security has become an increasingly important topic in cybersecurity. Hackers often target these vendors to gain access to a company's systems or data. To protect against these threats,

veterinary practices should conduct regular security assessments of their vendors and ensure that they are properly secured against potential attacks. An example of this would be the large-scale attack seen in late 2019 against a 400-hospital consolidator. The hackers gained access to a software application that was deployed to all the hospitals. They then used this tool to deploy ransomware to all 400 hospitals overnight! As we move more and more to the cloud, we need to make sure our software partners take cybersecurity seriously or you could fall victim to their lack of concern.

Overall, cybersecurity threats are an ongoing concern for veterinary practices and hospitals, and it is crucial for practices to stay informed about the latest trends and best practices in order to protect their business and clients. By taking appropriate measures to secure their systems and train their employees, veterinary practices can reduce the risk of cyberattacks and minimize the impact of any incidents that do occur. ■

Community | Education | **Growth**
Advocacy | Support

NAVC
YOUR VETERINARY COMMUNITY

NAVC.com/**Community**

Clint Latham is the founder and CEO of Lucca Veterinary Data Security, a firm dedicated to helping veterinary practice owners realize the value of their data and take the steps necessary to protect it. He is a Purdue Law graduate and a former HIPAA and finance data compliance specialist.

