Dental Cybersecurity: Protect Your Practice

By Gary Salman

Over the last 20 years, an evolution in computer technology has taken place in the dental practice. Computers were previously only used for basic recordkeeping and billing. Then came their application in appointment scheduling, digital radiography, charting, and now, digital dentistry. As the amount of data stored in systems has increased, so have the frequency and sophistication of cyberattacks. The days of simply relying on a firewall and antivirus software to protect a practice's network and patient data are over. If these devices were truly effective at protecting networks from data breaches, there would be no breaches.

In the past 12 to 18 months the focus of cyberattacks has shifted dramatically. Now, more than ever, hackers are setting their sights on healthcare entities and the frequency and severity of malware and ransomware attacks have increased, with practices of all sizes being impacted. Such attacks can shut down and compromise networks, resulting in an inability to access patient records and in loss of revenue.

Practices store a wealth of very important information that can be used for identity theft and blackmail purposes: names, addresses, dates of birth, social security numbers, identities of family members, scans of driver's licenses, insurance cards, health history forms, 2D and 3D images, lab reports, etc. To the average hacker, this information is a treasure trove of targets that could be used personally by the hacker or sold on the Dark Web (the black market of hackers).

Many dentists may think that because they don't store "medical records" in their system, they don't have to worry about protecting patient files. In the eyes of Health and Human Services, whether you are a cardiologist, dentist or a laboratory, any patient data in your system needs to be protected. In addition, if your practice were to suffer a data breach, the HIPAA Breach Notification Rule requires that you notify every patient of record that a breach has occurred. Imagine the negative PR your practice would encounter in the local community. Moreover, identity theft monitoring would need to be offered to all affected patients. Health and Human Services and the Office of Civil Rights are just two of the reporting agencies the practice would have to work with; 49 of 50 states now have equal or more stringent breach notification rules. If a practice treats patients from multiple states, reporting a breach to all relevant states may be required.

Oklahoma has specific statutes related to the protection of personal information. The Security Breach Notification Act (§ 24-161 to 24-166) stipulates that "Federal and State Laws require that if you maintain, as part of a database, a consumer's name and other personal identification numbers (i.e., social security number, driver's license, credit card or

financial information with the personal security code), such information must be encrypted or redacted so that in the event of a breach, this information cannot be obtained and used by a third party."[1] The requirements are intense and not something that an IT company can typically address. Implementing a complete HIPAA solution along with the Cybersecurity solutions outlined below will help with most of the state's data protection laws.

When asked what they do to protect their networks most dentists reply, "My IT company handles that." However, IT companies are not Cybersecurity companies. Since IT companies cannot audit their own work, IT providers typically partner with a Cybersecurity company that independently audits their work. It takes the expertise and knowledge of a Cybersecurity company to help ensure the security of the network. Imagine your Internist informing you of a heart condition that will require bypass surgery. Would you want your Internist or a Cardiac Surgeon performing the procedure?

Ransomware attacks have been impacting the healthcare community at a staggering rate. The unfortunate mistake practitioners make is having their IT company "clean it up and restore their data." If your practice's data was stolen and is being bought/sold on the Dark Web and this breach was not reported to the Office of Civil Rights, you could be subject to massive fines. If your practice falls victim to a ransomware attack or other possible breach, there are steps you must follow to determine if ePHI (electronic protected health information) was compromised. This often involves hiring a forensics company and working with a Cybersecurity company to harden the practice's infrastructure. It's very probable that if you were the victim of an attack once, you will most likely be a victim again because of vulnerabilities in your network that enabled the initial attack. To recover from the attack, you cannot simply restore your data and hope for the best.

To secure your network and combat against these sophisticated attacks, you need to implement four key pillars of Cybersecurity: [1] Cybersecurity Audit; [2] Cybersecurity Awareness Training; [3] Vulnerability Scanning; and [4] Penetration Testing.

Cybersecurity Audit
During this audit, a Cybersecurity company works closely with your practice and your IT company to understand the complete landscape of your IT footprint. The Cybersecurity company will inquire about where and how data is stored, what protocols are in place to protect the data, and how it is accessed. Are there remote team members? Does the practice contract with a billing company that "logs in" to the practice's network? Do you leave the office with any device that stores ePHI, leaving the practice exposed if the device is stolen or lost? Is ePHI transmitted and stored using encryption technologies data protection?

Cybersecurity Awareness Training
As part of the HIPAA Security Rule, covered entities (e.g., your practice) are required to undergo Cybersecurity awareness training to help mitigate the risk of human error and minimize the chances of being exposed to an attack. Recent data points to a 50% to 75% reduction in cyberattacks against healthcare entities that properly train their staff.

Perhaps the most vulnerable components of a network are the people using it – you and your staff. Social engineering, often referred to as "hacking the human," is the most prominent threat vector impacting practices and is often the least discussed. As advancements are made in security, hackers are relying increasingly on humans making mistakes. For example, most ransomware attacks are initiated via spear phishing, which is designed to fool an email recipient into opening an email that appears to be coming from someone they know or trust. An email may be sent to the staff, purporting to be from you, asking them to open an attachment or click on a link to update or download something. Once they initiate the action, an executable file may run, which is a ransomware attack. The ransomware typically encrypts the current computer and then searches the network for other machines. Once it finds the server, depending on the complexity and lethality of the attack, the ransomware will encrypt most or all of the files on the server, resulting in the files becoming inaccessible unless the user pays the ransom to the hackers to have the data decrypted. This is typically done using a cryptocurrency such as Bitcoin or Monero. Often, the files are not returned; if they are, a timebomb attack may be set up that will impact the files again shortly thereafter. Any hacking should be immediately reported to law enforcement authorities.

Most practices don't think to ask their IT vendors, imaging companies, billing companies, software vendors or third-party solutions if they are following HIPAA laws related to compliance and Cybersecurity.

Vulnerability Scanning
For a network breach to occur, the network typically must have vulnerabilities such as unpatched operating systems, outdated equipment, weak passwords, open ports on computers or firewalls, unsecure network protocols, and/or improperly configured firewalls. Cybersecurity firms deploy very sophisticated tools and technologies to search for "open doors and windows" on your network that can be exploited by hackers. These tools gather information on your network and run tests against the devices searching for vulnerabilities. This data is then turned over to your IT company for remediation purposes; the IT company can effectively lock the "doors and windows." Cybersecurity companies invest heavily in best-in-class vulnerability scanning technologies that can detect thousands of vulnerabilities on a practice's network. Testing should be performed quarterly or whenever network devices are upgraded, modified or added to.

Penetration Testing
Penetration testing utilizes a "white hat hacker" (ethical hacker) who uses the same tools, techniques, and protocols that a cyber-criminal would use to gain access to your network. Unlike a vulnerability scanner, an ethical hacker has the capacity

to problem-solve during the testing. For instance, a vulnerability scanner will get to a locked "door" and not know how to progress. Essentially, it stops and moves on to something else. A hacker, based on his/her level of experience, will see that the "door" is locked but may run a certain script to open it. Ethical hackers use their experience to exploit networks in a way an automated tool simply cannot. After ethical hackers finish their testing, they turn their findings over to your IT company so that risks can be mitigated.

Most practices don't think to ask their IT vendors, imaging companies, billing companies, software vendors or third-party solutions if they are following HIPAA laws related to compliance and Cybersecurity. As business associates, these entities are often required to follow the exact same laws as you do. Imagine if your IT company has a breach or ransomware attack that spreads from their network to yours. Now what happens when your records are compromised? Whose fault is it? During the investigation, it would be discovered that you were working with a company that is not HIPAA-compliant which may expose your practice to additional scrutiny, liability and risk.

You have spent years to become a dentist and to grow and build your practice, your reputation and your patient's trust in you. The risk of a data breach is real and you should not be passive. You need to take a proactive approach to secure your network before this happens to you. Practitioners who have experienced data breaches all say the same thing, "This is one of the worst things that can happen to you." The financial and social impact on your practice is debilitating. The cost for mitigating a breach can run into the hundreds of thousands of dollars and may result in a significant loss of patient trust. Fortunately, if a practice implements sound Cybersecurity solutions, properly trains its staff and puts a strong focus on security, almost all attacks can be thwarted.

About the Author
Gary Salman is Chief Executive Officer of Black Talon Security, LLC, a computer security service located in Katonah, New York. He has over 26 years of experience in software development and computer IT in the dental marketplace.

[1] https://www.ok.gov/OREC/documents/Security%20Breach%20Notification%20Act.pdf