The evolution of cyberthreats impacting OMSs

By Gary Salman, CEO
Black Talon Security, LLC

During the last five years, there has been an evolution of cyberthreats impacting oral and maxillofacial surgery practices. In 2017, a hacker's methodology included encrypting servers and possibly workstations, with payments ranging from $5,000 to $6,000 for a small OMS practice and recovery typically taking a few days.

As ransomware attacks escalated over the years, there was a dramatic shift in the severity of these events. Hackers could now gain access to every computer on a network, install screen-sharing software, and find and destroy all backups, impeding a practice's ability to recover. Hackers also started encrypting every computer on a network with ransomware, resulting in practices having to shut their doors for days.

In 2021, hacking groups started to deploy triple-extortion methodology, stealing all data from a practice, publishing it on the dark web and contacting impacted individuals (i.e., employees and patients) with additional demands. This approach is highly effective because it almost guarantees an OMS practice would pay the ransom to prevent the data from being released.

The hacking groups create "leak sites" where they showcase some or all of the data stolen from a victim. These sites often include highly confidential details, such as patient health history forms, lab reports, pathology, driver's licenses, insurance cards, banking and financial information. If payment is not made, hackers will then sell or auction data on the dark web.

The legal and public relations nightmare associated with this type of event is significant, and the cost and reputational damage to the practice can be severe. In almost all extortion cases, legal counsel will recommend an OMS practice make the ransom payment regardless of the availability of recoverable backups. In late 2021 and into 2022, ransom demands and costs associated with cyberattacks against OMS practices continue to increase. Victims experienced business interruptions in excess of 10 days and six-figure expenses.

Many OMS practices do not understand the full value of cybersecurity until the practice falls victim to an attack or a close friend or colleague has been extorted for hundreds of thousands of dollars. The lack of advanced cybersecurity solutions, feelings of "it won't happen to me" and promises made by IT companies are the primary drivers of these attacks.

These cyber events in the dental, medical and small/medium business space have a financial, operational and emotional impact on organizations. In almost all the attacks investigated, the root cause was a lack of proper security measures and employee cybersecurity training.

Why cyberattacks are increasing

How do experts keep up with the ever-changing methodologies hackers use to target OMS practices? Digital forensic investigations provide an in-depth understanding of the latest trends and attack methodologies. As part of responding to a cyberattack against a healthcare entity, a digital forensic investigation is required to determine if electronic protected health information was accessed or stolen. This utilizes highly sophisticated forensic software to gather details about the incident. Credentialed analysts then comb through the data to piece the crime together, paralleling what a police detective would do when performing a criminal investigation.

continued on next page

How do attacks against OMS practices typically occur and why are they on the rise? Most who fall victim believed their IT company had them properly protected using firewalls, antivirus software and backups. Unfortunately, this type of protection is now considered basic security and won't stop many other types of attacks.

Hackers will typically breach a network in one of two ways. The first is known as social engineering, where they trick team members into clicking on a link, opening an attachment or giving up their credentials. This type of attack is often highly effective because computers may not be able to defend against it, since the employee initiated the action. Cybersecurity awareness training is an easy way to prevent this type of attack. This training is required under HIPAA and empowers teams to identify email and web threats and take corrective actions to prevent them.

Exploiting known vulnerabilities in a company's firewall, computers and other devices is the second methodology. Hackers use sophisticated tools to scan devices and locate weaknesses. They often then use the devices to gain access to a network where they can remain for weeks prior to executing an attack. During this period, they gather intelligence on everything done on a network. For instance, hackers will watch how and where files are backed up, the type of antivirus software used, cloud system access, applications and the target's type of business.

This intelligence-gathering exercise provides them with leverage when launching the final phase of an attack: executing their ransomware code. Only at this point will a company realize it has been attacked. Once all computers are encrypted, hackers will leave a ransom note, which typically indicates how to contact them and may include information about the amount of money demanded.

Common misperceptions

To address firewall and network vulnerabilities, a practice should implement a real-time vulnerability-management and penetration-testing solution that constantly monitors, tests and evaluates network weaknesses so they can be remediated. Since hackers exploit vulnerabilities, the elimination of high-risk issues reduces the likelihood of an event.

New vulnerabilities are being discovered every day on computers, firewalls and devices. Without an effective cybersecurity program in place, a practice could become the next victim of a ransomware attack.

Here are a few common misperceptions OMS practices make about cybersecurity:

- My firewall and antivirus software will protect me.
- My backups will prevent me from having to pay a ransom.

- I am in the cloud, so I have nothing to worry about.
- My IT company has me protected, so I have nothing to fear.
- Hackers won't find me; there are too many "big fish" out there.
- Even if I get hit, I will be able to get back up and running quickly.
- The FBI has tools to decrypt my data.
- I don't have any data that hackers would care about.
- I have insurance, so I am covered.
- I am just an OMS practice, not a hospital, so security does not matter to me.

OMSs should consider the following measures to help build a ransomware-resilient practice:

- Have a comprehensive onsite and offsite storage solution that includes a disconnected backup.
- Implement real-time vulnerability management technology to identify and address issues on devices within the office. Make sure the medium- to high-risk vulnerabilities are addressed on an ongoing basis.
- Have an external penetration test done annually to identify network entry points hackers will exploit.
- Utilize a cybersecurity awareness training platform to empower and educate doctors and other team members about the various types of threats.
- Test employees to determine the effectiveness of the cybersecurity awareness training by utilizing a simulated phishing platform that sends emails that appear to be malicious.
- Perform a security assessment (required under HIPAA) to help the practice understand where it has operational risks.
- Implement artificial intelligence-based antivirus and threat-hunting software known as "extended detection and response." This technology can replace traditional, outdated antivirus software.
- Utilize an independent third party to perform the tasks mentioned above. It is critical the company's IT vendor does not test and evaluate its own security measures.
- Implement a password management tool that creates unique and strong passwords for every website and application utilized.
- Implement multifactor authentication for financial institutions, credit cards, email systems, insurance carriers and software applications.

The financial and reputational damage a cyberattack can cause an OMS practice may be well-known, but rarely are practitioners aware of the personal and psychological impact of these events. Cyberattacks, by nature, are personal. Hackers gain access to personal emails, read them and often engage with the victim's friends, family and colleagues.

During ransomware attacks, organizations often cannot function, and most OMS practices go through the traditional victimization stages. Many also wonder whether they will even be able to recover from such an event. It sometimes may take months or even years to recover from the personal, financial and reputational ramifications. Many practitioners report suffering from PTSD as a result of these events. Every day they wonder, "Is it going to happen to me again?" Some will even decide to close their doors after falling victim to a ransomware attack.

Cybersecurity is a rapidly changing landscape with new threats and hacking groups appearing almost weekly. Implementing the above multilayered solutions and technologies will help give practices a fighting chance against these highly sophisticated adversaries. ■

Gary Salman is CEO of Black Talon Security, which specializes in cybersecurity and incident/breach response.

This is number 187 in a series of articles on practice management and marketing for oral and maxillofacial surgeons developed under the auspices of the Committee on Practice Management and Professional Staff Development and AAOMS staff. Practice Management Notes from 2002 to present are available online at AAOMS.org.