Mitigating cyberattacks through training and

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) strive to raise cybersecurity awareness nationally and internationally by providing an array of resources, tools, assessments and training to help identify risks and potential threats. It is vital for oral and maxillofacial surgery practices to train staff in cybersecurity measures and make a contingency plan in case of a cyberattack.

Q What is Cybersecurity Workforce Training and where can I find resources on how to implement training for my staff?

A Cybersecurity Workforce Training includes efforts to instruct staff on common and pertinent cyber threats. Staff members are the first line of defense when it comes to cyberattacks, and they must learn to recognize and identify potential threats to ensure the safety and security of patients and the practice. Cybersecurity training should include:

- Teaching staff to recognize email phishing techniques with the assistance of phishing simulation tools.
- Educating staff on the risks of insider threats. If you see something, say something.
- Providing staff with constant and relevant training with actionable steps that apply to current threats.
- Instilling the importance of password protection procedures, such as never sharing or writing down passwords.

Check out detailed resources at 405d.HHS.gov and CISA.gov/resources-tools/cyber-security-workforce-training-guide.

Q What is ransomware and how can I protect my practice and patients?

A Ransomware is an ever-evolving form of malware designed to encrypt files on a device and render them unusable. Malicious actors then demand ransom in exchange for decryption of the files.

To prepare the practice and keep patients safe in the event of an attack, HHS recommends following these industry-tested best practices:

- **Prepare** – Be sure to understand the organization's incident response plan, identify the IT/cybersecurity point of contact, and practice paper and pen operations in case of an attack.
- **React** – If an attack occurs, implement the practice's protocol for incident handling.
- **Recover** – After an attack, take steps not to reinfect unaffected/clean systems. Document any lessons learned and adjust policies and response plans accordingly.

Practices should work with their IT and cybersecurity vendors to establish policies and procedures and implement appropriate protections. For additional resources, visit CISA.gov.

Q If a cyber-related security incident occurs, what immediate steps should be taken?

A In the event an entity experiences a cyber-related security incident or ransomware attack, the HHS Office for Civil Rights (OCR) provides a quick-response checklist outlining the necessary steps to take. The checklist can be accessed at hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf. As a HIPAA-covered entity, the practice should complete the following in the event a cyberattack or similar emergency occurs:

- **Execute any response and mitigation procedures and contingency plans**. This includes fixing any technical problems to stop the incident and taking steps

planning

to mitigate impermissible disclosure of protected health information (PHI).

- **Report the crime to law enforcement agencies**. The practice should notify agencies such as state or local law enforcement and the FBI.
- **Report all cyber-threat indicators to federal and information-sharing and analysis organizations (ISAOs)**. This includes the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response and private-sector cyber-threat ISAOs.
- **Report the breach to OCR**. For breaches affecting 500 or more individuals, OCR must be notified no later than 60 days after the discovery, along with affected individuals and the media – unless law enforcement has requested a delay. For breaches affecting fewer than 500 individuals, affected individuals must be notified no later than 60 days after the discovery, and the OCR must be notified within 60 days after the end of the calendar year.

Note: Entities must adhere to the HIPAA Privacy Rule when reporting cyber-related security incidents and should not include PHI. More information is available at HHS.gov. ■

For additional staff training, visit the AAOMS CE Online Library to access the on-demand recording, "Cybersecurity – What's the Cost of Doing Nothing?"