Responding in defensive or emotional ways does not resolve the situation and can make it worse. We need to control how we respond to what others say even if we are being criticized.

Listen

Listening can open the lines of communication by helping you understand what others are thinking. In addition, if you want to have others listen to you, you should listen to them. Having a better understanding of what is being said and why can go a long way to promoting better understanding and conflict resolution.

It's also important to understand the difference between being aggressive and assertive. Aggressiveness puts the emphasis on attacking or confronting another person. Assertiveness indicates that you have confidence and are self-assured so that you can be forthright and stand up for yourself appropriately. Each person should be able to stand up for himself or herself in a way that conforms to proper behavior and uses proper channels. Challenges in communication that lead to conflict need to be faced confidently, using facts and not emotions, and rely on each individual's empowerment to self-advocate.

Remain Confident

When speaking with a co-worker with whom you are in conflict, you should consider your tone of voice as well as its volume, your body language, and your ability to maintain eye contact. If you fail to maintain this control, a bully, among other personalities, can sense fear and will see that you lack confidence and can be manipulated. Your confidence should be based on having solid information to back your stance. It shouldn't be so overwhelming that you fail to listen to the other person and see his or her point of view. When you approach conflict by trying to resolve things so all benefit, the best results can be achieved.

WHEN COMMUNICATION FAILS

Some conflicts can't be resolved and may require us changing in our attitude or the situation itself. Some people refuse to respect co-workers and cannot handle conflict in a constructive way. When these types of things occur, it's important to be able to confidently protect your personal boundaries and end the conversation in a professional manner.

Clinical Significance

Conflict can develop even in the most solid relationships. The key is how to address the situation and resolve it professionally and in a way that everyone can see benefits. It's important to say what you need to say and seek to agree on a resolution, to let it go, or to evaluate whether you are in the best work environment for you. Having tough conversations is easier if you have practice and keep your eyes on the goal of creating a work environment that is open, peaceful, and personally rewarding.

Whiteley J: Navigating conflict with communication. *RDH Mag* 39:32-35, 2019

Reprints not available

CYBERSECURITY
Safeguards against threats

BACKGROUND

Although technology has provided great benefits to the practice of dentistry, new concerns and challenges are also associated with its use. A practice owner must be aware of the vulnerabilities of his or her information systems and consider the natural, environmental, and human threats that can compromise the reputation and finances of the dental practice. Being cybersecurity aware means to be cognizant of the criminal or unauthorized efforts to access the practice's servers, workstations, networks, programs, mobile devices, electronic devices, and stored data. The federal Cybersecurity Act of 2015 mandates the development of practical cybersecurity guidelines to help manage the risks facing the health care industry. Five cybersecurity threats have identified (Table). In addition, the Office for Civil Rights (OCR), which enforces HIPAA, has offered several basic cybersecurity practices to reduce the impact of these threats.

SAFEGUARDS

Encryption

Encryption converts electronic data into code that cannot be read without a decryption key. This prevents unauthorized users from viewing the data and can reduce the risk that patient data will be compromised. Dental practices can use encryption software or one of the e-mail service providers that encrypt messages. HIPPA-covered entities must determine if encryption is a reasonable and appropriate safeguard for protected health information that is stored or transmitted.

Table. Five Prevailing Cybersecurity Threats to Health Care Organizations

Threat	Potential impact of attack.
Email phishing attack	Malware delivery of credential attacks. Both attacks further compromise the organization.
Ransomware attack	Assets locked and held for monetary ransom (extortion). May result in permanent loss of patient records.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Accidental or intentional data loss	Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.
Attack against connected medical devices that may affect patient safety	Undermined patient safety, treatment and well-being.

Source: Technical Volume 1: Cybersecurity practices for small health care organizations, phe.gov/Preparedness/planning/405D/Documents/tech-vol1-508.pdf. (Courtesy of CDA Practice Support: Are you cybersecurity aware? CDA J 47:277-278, 2019.)

Social Engineering

Phishing is the term used to describe sending deceptive e-mails to users that entice them to disclose login information or to click on links that install malware, including ransomware. The phishing practice exploits user vulnerabilities such as inattention to detail, fear, and being rushed or feeling threatened. Practice owners must train staff members to recognize phishing attempts. This training can be accomplished using short videos found on YouTube, which may be promoted on posts by information technology (IT) or security companies. Security awareness training for all members of the dental office workforce is mandated by the HIPAA Security Rule.

Audits

Practice owners should be able to record network and system activity and monitor the activity by reviewing, or auditing, the logs. This can reveal suspicious activities or allow the owner to reconstruct events. Audit logs can be a vital tool in security if they are regularly reviewed. They are also required for HIPAA compliance.

Secure Configurations

Cybersecurity defenses can be improved by ensuring the proper configuration of information system devices, networks, and software. All of the safeguards, such as encryption, anti-malware, and audit logs, depend on having settings that allow them to function appropriately. Older versions of encryption software may be less effective than up-to-date versions, for example. It's necessary to maintain and update malware definitions to obtain maximum protection. The configuration of firewalls, workstations, routers, servers, and other components is important to minimize the risk of a security breach.

Clinical Significance

We hear about breaches of security throughout large corporations, including insurance companies and health care facilities. Most of us have small practices and may think that no one would think to attack such a small target, but we would be wrong to rely on that thinking. Not only can bad actors choose any target they like but to not protect against the threat is to be in violation of HIPAA mandates. Taking the time and effort to install and update the safeguards needed to protect our patients' information as well as practice data is part of providing the best care for everyone.

DENTAL TEAMS
Building morale in a dental practice

Check for updates

BACKGROUND

Much focus has been placed on the need to humanize the interactions between dentist and patient, with a strong trust relationship among the dentist, dental team, and patient seen as most desirable. However, team morale in a dental office is essential to a pleasant working environment. Low team morale can lead to burnout and poor patient care, whereas good morale and motivation can positively affect patient experience and care, which can feed back into the team's satisfaction with their performance. Studies indicate that several factors