Cyber Risk in Dentistry: Why Every Practice Is a Target—and What to Do About It

By E. Andrew Gerner, CFP®
CEO, R. K. Tongue Co.

Dentistry has always been a profession built on trust. Patients trust you with their health, their privacy, and increasingly, their data. Today, that trust is under growing threat—not from clinical risks, but from cybercrime.

Dental practices of all sizes are now prime targets for cybercriminals. The reason is simple: you hold a combination of sensitive personal data, health information, and payment details, often within systems that lack enterprise-level security.

Dental Practices Are Being Targeted

Cyberattacks against healthcare—and dentistry specifically—are no longer hypothetical. Healthcare is now one of the most targeted industries for cybercrime, with hundreds of reported incidents annually .

Why dentists? Because attackers understand that you cannot operate without your systems. When scheduling, imaging, billing, and patient records go offline, practices often face immediate financial pressure to restore operations—making them more likely to pay.

Real-World Examples from Dentistry

- True Dental Care for Kids and Adults LLC in Pennsylvania was required to notify 17,640 individuals about a ransomware attack. A hacker gained access to its network on February 3, 2025, and downloaded ransomware, which was used to encrypt files on its network. The forensic investigation of the incident identified unauthorized access to patient data prior to file encryption.
- A single compromised email attachment forced one dental office to shut down for three days and pay a $71,000 ransom
- A cyber incident involving a Wisconsin dental IT vendor impacted an estimated 432 dental practices simultaneously
- Indianapolis-based Westend Dental agreed to a $350,000 settlement after a ransomware attack exposed the protected health information of its patients.

Virginia Dentist and R. K. Tongue Co. client Pearson Pediatric Dentistry, PLLC experienced a reportable network intrusion during the 10 overnight hours between installing a new router completing firewall configuration. You can listen to the whole account at https://youtu.be/qaKYookf7N8?si=emB1zHAkxlfTKevN

Even more concerning, many attacks originate from everyday vulnerabilities—phishing emails, weak passwords, or unpatched software.

The True Cost of a Breach

The financial and operational consequences extend far beyond ransom payments:

- Consider the prototypical breach: theft or encryption of 4,000 – 5,000 patient records. Response costs, including forensics, notification, credit monitoring and legal costs average $250 per record and can top $1 million total. Add ransomware demands, regulatory fines and a week of lost production, and total costs often land between $1.2 million and $1.4 million.
- HIPAA penalties can reach up to $1.5 million annually for serious violations
- Practices may face:
    - Business interruption and lost revenue
    - Patient notification and credit monitoring costs
    - Regulatory investigations
    - Reputational damage and loss of patient trust

In short, a cyber event is not just an IT issue—it is a business survival issue.

How Cyberattacks Typically Occur

Most dental practice breaches follow a predictable pattern:

1. Phishing Email – A staff member clicks a malicious link or attachment
2. Credential Theft – Hackers gain access to systems or email accounts
3. Network Penetration – Malware spreads through the practice network
4. Data Exfiltration & Encryption – Files are stolen and systems locked
5. Ransom Demand – Payment is demanded to restore access and prevent data release

Understanding this lifecycle is critical because it highlights where prevention is most effective.

Practical Risk Management Steps for Dental Practices

The good news: most cyber incidents are preventable with disciplined, layered controls.

1. Train Your Team (Your #1 Defense)

Human error is the leading cause of breaches. Conduct regular phishing awareness training and simulated attacks.

2. Implement Multi-Factor Authentication (MFA)

Require MFA on:

- Email accounts
- Remote access (VPN/RDP)
- Practice management systems

3. Maintain Secure, Tested Backups

Backups should be:

- Encrypted
- Stored offsite or in the cloud
- Regularly tested for restoration

4. Keep Systems Updated

Unpatched software is one of the most common entry points for attackers.

5. Use Endpoint Detection & Response (EDR)

Modern cybersecurity tools go beyond antivirus to actively detect and stop threats.

6. Vet Third-Party Vendors

Many breaches originate through vendors. Ask:

- What security controls do they maintain?
- Do they carry cyber insurance?

7. Develop an Incident Response Plan

Know in advance:

- Who to call (IT, legal, insurance)
- How to isolate systems
- How to communicate with patients and regulators

The Role of Cyber Liability Insurance

Even with strong controls, no practice is immune.

A properly structured cyber liability insurance policy can provide:

- Coverage for ransom payments (where legally permissible)
- Data recovery and system restoration costs
- Business interruption losses
- Legal defense and regulatory fines
- Patient notification and credit monitoring
- Access to breach response experts

Importantly, insurers increasingly require minimum cybersecurity standards (such as MFA and backups), reinforcing best practices while providing financial protection.

Final Thoughts

Cybersecurity is no longer optional—it is an essential component of running a modern dental practice. The frequency, sophistication, and financial impact of cyberattacks continue to grow, and dental practices are firmly in the crosshairs.

Dental practice owners are not expected to develop network engineering knowledge and skills but they *are* expected to protect sensitive data at high security levels. For most practices, that means contracting a managed services provider or similar IT vendor to manage and harden the security of your IT infrastructure and purchasing cyber insurance to respond and pay expenses in the event that best risk management efforts are not enough.

By combining proactive risk management with robust cyber insurance, practices can protect not only their data, but their reputation, their patients, and their long-term viability.

References:

https://www.hipaajournal.com/ransomware-attack-true-dental-care-for-kids-and-adults/

https://www.oralhealthgroup.com/nextgen/a-71000-ransomware-nightmare-how-one-dental-practice-recovered-and-lessons-for-every-dentist/

https://www.dentists-advantage.com/Prevention-Education/Risk-Alerts/Risk-Alerts-Index/Content/Ransomware-attack-hits-over-400-dental-practices

https://decisionsindentistry.com/2025/01/dental-practice-faces-350000-fine-over-ransomware-attack/

https://youtu.be/qaKYookf7N8?si=emB1zHAkxlfTKevN

https://insuranceformembers.com/2025/07/how-much-cyber-insurance-does-a-1-million%E2%80%91revenue-dental-practice-need/

As the proudly Endorsed Insurance Partner of the West Virginia Dental Association, R.K. Tongue Co. (RKT) specializes in helping dental practices design and manage customized insurance and employee benefits programs. If you have any questions or would like a complimentary review of your current plan, please reach out to us at 410.752.4008 or email us at info@rktongue.com.