Is Your Dental Practice a Cyber Target?

*The answer, increasingly, is **yes**! Here's what you need to know.*

Healthcare is now the most attacked sector in the U.S. for cybercrime, and dental practices are a growing target. Your patient files contain a uniquely valuable combination of personal, financial, and medical data while your IT defenses are typically far leaner than a hospital's. That's a combination cybercriminals are actively exploiting.

32%	**$9.8M**	**1.22M**
of all U.S. data breaches hit healthcare	average cost of a healthcare data breach	patients exposed in one 2025 dental breach

Why Dentists Are in the Crosshairs

Dental offices are attractive targets for several reasons most practitioners don't realize:

- Patient records hold SSNs, insurance data, and financial info. This is worth far more than a stolen credit card on the dark web.
- Small practices rarely have dedicated IT security staff or active system monitoring after hours.
- Third-party vendors (billing software, imaging systems, IT providers) are common entry points and you're still liable under HIPAA when they're breached.
- Legacy dental equipment often runs on outdated operating systems that no longer receive security patches.

"I turn my computer off at night, I don't need it"

Small businesses can't hide from cybercriminals by assuming they're too small or irrelevant to be worth targeting. In fact, the opposite is true. Limited resources mean limited defenses, and that's exactly what makes them attractive. Simply turning off your computer at night or keeping it in the office offers no real protection. Attackers don't need physical access. Inboxes are constantly flooded with carefully crafted emails designed to confuse and pressure your team into opening just enough of a crack for criminals to slip through. When it comes to your cybersecurity, your people are often your most vulnerable point of entry.

The Exposure Is Real

In 2024, the FBI's Internet Crime Complaint Center received 859,532 complaints, with financial losses exceeding $16.6 billion, a 33% increase from 2023. Globally, cybercrime costs were projected to reach $10.5 trillion annually by 2025, according to Cybersecurity Ventures. For a dental practice, that's not an abstract statistic. A single breach can trigger HIPAA notification requirements, regulatory fines, patient lawsuits, and days or weeks of lost productivity. The question isn't whether your practice could be targeted… it's whether you'll be prepared when it is.

This Is Exactly What Cyber Insurance Is For

Standard business insurance won't cover a cyberattack. Cyber liability policies are specifically designed to cover:

- Forensic investigation and patient notification costs
- Business interruption losses while systems are down
- Ransomware response and system restoration
- Regulatory fines and legal defense
- Patient lawsuits and settlement costs

Don't wait for an incident to find out you're unprotected… Work with R.K. Tongue.

Please contact your WVDA cyber insurance expert, **Elizabeth Holmen** at eholmen@rktongue.com or **410.752.4012** to review your current coverage or learn more about the importance of cyber liability for your dental practice. If you're ready for a conversation schedule a consultation by scanning the QR code and putting a time on the calendar.