How to Protect your Practice by Strengthening your IT Network

As the world has migrated to operate more heavily on the internet, unfortunately, cybercrime has also migrated there, as well. For dental practices, this means that their offices are ideal targets for a breach, but the good news is that these cyber-risks are mitigated by understanding the health of their IT network. As always, the first step is awareness, and in this whitepaper HTI Consultants shares the 5 key risk factors a dental IT network faces and how dentists can protect their offices from data loss, data breach or costly downtime to keep their practices up and running strong.

As dental offices are focused primarily on improving patient care, their IT network is often overlooked as a critical aspect of the business, however, dental offices are facing pressure on two sides. Firstly, more dental offices are being targeted by cybercriminals due to the sensitive nature of the data stored at dental practices. As cybercriminals continue to engineer new ways of breaching networks, dental offices need to be protected from this dark innovation. Secondly, dental offices are facing additional pressure from regulators and practices are now being fined up to six-figures for incompliance and they can also face malpractice penalties.

While most dental practices still don't believe they will be breached, they often overlook the larger concern, which is the costly downtime that could affect them in the event of an unexpected flood caused by a broken pipe, a hot water heater upstairs breaking or even an accidental fire.

“Unfortunately, inaction is just too big of a risk for many practices. Nobody thinks a breach will happen to them. But this is the problem, once it does, it’s a major headache. A dental office can face $250,000 in fines, attorney’s fees and unnecessary expenses that could’ve been avoided simply by taking a few, minor preventative steps. The cost for inaction is too high and if rectified early enough, preventative measures can thwart these problems for a miniscule fraction of the cost they’d be facing during a downtime period.” states **Christine Basile,** Senior Systems Consultant at HTI.

For dental offices who decide to be proactive, there are five key areas for them to consider when assessing the health of their network.

Hardware/Software

Is your office running a contemporary operating system? Are your servers up to date? For example, Windows 10 is the most current operating system available and is 100% necessary because Microsoft no longer provides security patches to support offices who are still running Windows 7. Outdated technology exposes the office to threats which can be rectified simply by updating your software and hardware.

Backup

Every dental office needs a sound disaster recovery and data backup plan. This means that in the event of an unplanned outage, staff can still access patient data Data backups should happen on a regular basis, should be kept secure and be updated daily to minimize data loss and downtime.

Dental Applications

Lots of dental offices forget to include software application upgrades to their annual overhead and then are shocked when they’re hit with a sizable bill to upgrade the hardware specifications. For example, many dentists don’t allocate budget to regular upgrades and then are faced with large bills when they need to upgrade from Dentrix G5 to Dentrix G7, for instance. Every office should forecast expenses and expect to invest $15,000-$30,000 into higher performing software every 5 years or so.

Network Security

The best fix here is by utilizing a layered approach. In the same way that a submarine is separated into various self-contained compartments so it can still seal itself off and still operate during a breach, dental networks should be protected in the same manner. At a minimum, they need to have an enterprise firewall with daily firmware updates, enterprise-grade anti-virus and anti-malware, and due to their prevalence, dentists should also consider an anti-ransomware solution, as well.

Cybersecurity

This is one of the most compelling reasons to consider partnering with an external IT provider like HTI, who explicitly specializes in dental. Many dentists assume that if they have a single IT person responsible for the upkeep of the network, that they're covered. However, it's very difficult for lone IT personnel to remain aware of all of the new tactics cybercriminals are inventing to beat security systems, when compared to a company that has a department that specializes in dental cybersecurity.

HTI has developed networking standards and security protocols based on years and years of experience. Our FREE TECHNOLOGY ASSESSMENT is the simplest way to understand the needs of your practice. Contact today!

Call us today at 877-222-1508 to ensure the right solution is in place for your practice!