issn 2193-4673 • Vol. 6 • Issue 1/2025

1/25

digital

including AI supplement

international magazine of digital dentistry

practice management
Understanding and responding to cyber threats in dentistry

case report
A fully digital approach to soft-tissue and aesthetic excellence

AI supplement
Demystifying artificial intelligence: A welcome guide for the entire dental team

dti] Dental Tribune International

GOOD DESIGN AWARD® WINNER

Meet Cure.

Turbocharged intelligent post-curing.

Developed for 3D printing. Designed for you.

Take a closer look

asiga.com

ASIGA

Dr Scott D. Ganz

Editor-in-Chief

Exploring the next chapter in dentistry at IDS 2025

It is that time again! Every two years, the largest dental exposition in the world meets in Cologne in Germany. The International Dental Show (IDS) attracts dental clinicians, laboratory technicians, assistants, hygienists, manufacturers, importers, organisations and educators—and much more—from all over the globe. The main theme each year continues to focus on innovation. As we continue into 2025, the landscape of dentistry is undergoing a profound transformation, driven by rapid advancements in technology, a growing emphasis on patient-centric care and an increasing focus on sustainability. The innovations we are witnessing today not only enhance the quality of care but also redefine the way we think about dental health. At this point in time, many dental practices have adopted a range of digital tools, from intra-oral scanners to 3D printing, which streamline processes and increase accuracy and precision. Digital records are now the norm, allowing for seamless communication between dental professionals and patients. Artificial intelligence (AI) is revolutionising diagnostic and treatment capabilities in dentistry. AI algorithms can assist in identifying dental anomalies and recommending personalised treatment plans. For instance, AI can analyse radiographic images with greater accuracy than human practitioners, detecting cavities or periodontal disease in their earliest stages, or automatically segment the mandibular or maxillary bone and teeth with one or two keystrokes. As these technologies evolve, they will allow for earlier intervention, improving patient outcomes and reducing costs.

The evolution of dentistry is not just about technological advancements; it also involves a cultural shift in patient engagement. This year, more dental professionals will be employing interactive and educational tools such as virtual reality and augmented reality to improve patients' understanding of their dental conditions and treatments. Engaged patients who are well informed about their options are more likely to adhere to recommended care plans, leading to better health outcomes. The innovations in dentistry that we can expect this year are not merely tools and techniques; they represent a paradigm shift towards a more efficient, patient-centred and sustainable approach to oral healthcare. As technology bridges gaps and opens doors to new possibilities, dentists will be better equipped to provide high-quality care tailored to individual needs. We can be optimistic about the future of dentistry, where healthy smiles are supported by cutting-edge innovations that will be highlighted at the IDS exposition and that are illustrated within the pages of this first issue of 2025. Enjoy!

Respectfully,
Dr Scott D. Ganz
Editor-in-Chief

AI logo courtesy of
BAIVECTOR/Shutterstock.com

Cover image courtesy of
Dental Pro Content/Shutterstock.com

kuraray

Noritake

ULTRATHIN LAYERING. FUTUREPROOF YOUR LAB.

CERABIEN™ MiLai

For zirconia and lithium disilicate dental restorations.

CERABIEN™ MiLai is a set of porcelains and internal stains specifically designed for the micro-layering technique. It consists of 16 porcelains and 15 internal stains easy to select and manage. The innovative product based on synthetic feldspar enables dental technicians to add the final touch to their zirconia or lithium disilicate restorations in a simple and time-saving procedure – for outstanding aesthetics right from the start.

LEARN MORE

BORN IN JAPAN

Kuraray Europe GmbH, BU Medical Products, Philipp-Reis-Str. 4, 65795 Hattersheim am Main, Germany, +49 (0)69-30 535 835, dental.eu@kuraray.com, kuraraynoritake.eu

From chairside to cyberspace: Understanding and responding to cyber threats in dentistry

Part 2 of a four-part series on helping practices get prepared

Anne Genge, Canada

Dentists dedicate immense effort to building thriving practices, adopting advanced technologies and improving workflows, towards enhancing patient care. Technologies like practice management software, imaging systems and patient communication tools are essential for growth and success, but they can also become targets for cyberattacks. In Part 1, we explored the fundamental reasons why cybersecurity has become critical for dental practices.[1] The takeaway was clear: while the stakes are high, with a clear plan and some proactive steps based on the right tools and knowledge, these risks can be managed effectively.

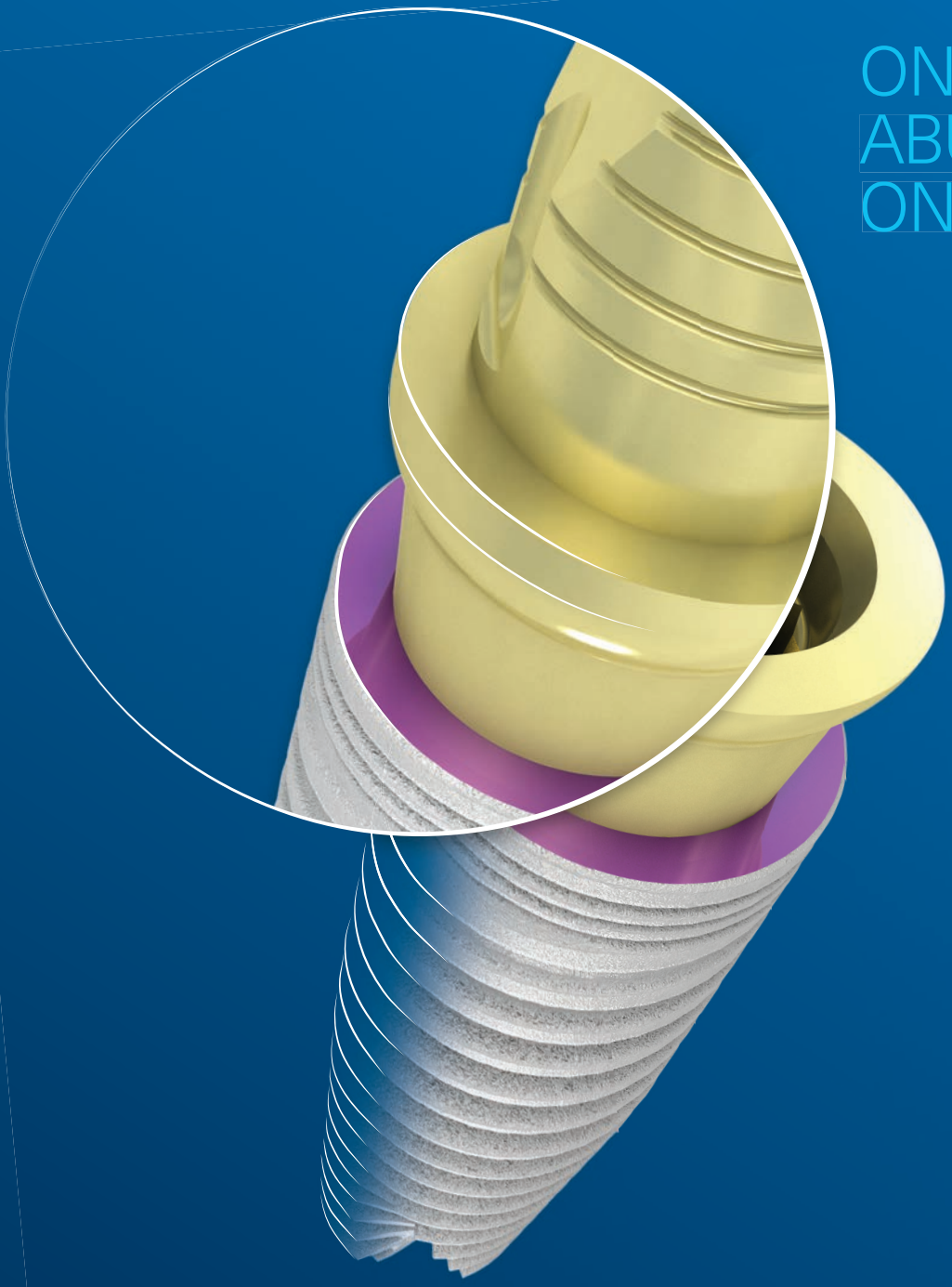
This article will focus on the most common cyber threats facing dental practices today—including emerging ransomware tactics that target both practices and patients. We will also outline practical, actionable steps you can take to strengthen your defences. Our aim is to empower you with the knowledge and confidence to protect your practice and your patients in today's digital landscape.

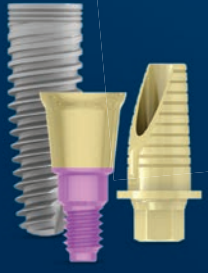
The most common cyber threats to dental practices

Common cyber threats include ransomware attacks, phishing scams, data breaches and insider threats. Dental practices are targeted because they possess valuable data and are perceived to be vulnerable. Patient records contain sensitive information that is lucrative on the black-market section of the internet called the dark web. Many dental practices may not have robust cybersecurity measures, making them attractive targets for cybercriminals. Additionally, cyber awareness tends to be low among staff members because dental

MIS® | Dentsply Sirona

ONE ABUTMENT, ONE TIME





MIS® CONNECT

TISSUE-LEVEL SCREW-RETAINED SYSTEM
MAKE IT SIMPLE

The MIS CONNECT is a stay-in abutment placed immediately after implant insertion and remains in place throughout the restoration process. Its design allows the prosthetic procedure and restoration to be performed away from the bone and within the soft tissue. Learn more about MIS at: www.mis-implants.com

practice owners often feel that they do not have time to implement proper policies and training.

Ransomware attacks

Ransomware is a type of malicious software designed to block access to a computer system or data until a sum of money is paid. It uses encryption to scramble data to make it unreadable unless an encryption key (long, complex password) is used. Encryption was designed to protect data; however, cybercriminals have learned that using encryption to paralyse organisations' operations is an easy way to extort money. In the dental industry, such attacks can be particularly devastating, leading to significant operational disruptions and financial losses.

A dental practice experienced a severe ransomware attack after a staff member clicked on a phishing email with an attachment labelled "X-ray results" which appeared to be from a patient.[2] This action encrypted all patient files, bringing the office to a standstill for several days. Because a reliable backup system was not in place, the practice was compelled to pay a substantial ransom to regain access to the data.

Ransomware attacks have evolved into double extortion schemes, where attackers not only encrypt a practice's data but also steal patient information. The hackers then demand two payments: one for decrypting the files and another to prevent them from publishing sensitive data on the dark web. Their criminal activity has now also extended to extortion of patients directly. In November 2023, Fred Hutchinson Cancer Center in Seattle in the US experienced a cyberattack by the Hunters International ransomware group, leading to unauthorised access to its clinical network.[3] The attackers claimed to have stolen 533.1 GB of data, including sensitive patient information such as names, US Social Security numbers, medical histories, laboratory results and insurance details. After the breach, patients began receiving personalised extortion emails demanding US$50 in Bitcoin to prevent their data from being sold on dark web markets. These emails included personal details to validate the threat.

This incident underscores the increasing trend of cybercriminals directly targeting individuals when organisations refuse to pay the ransom, highlighting the critical need for robust cybersecurity measures in healthcare institutions. The direct targeting of patients adds a new layer of reputational and legal risk for dental practices. It is no longer only the practice that is vulnerable; patients too are now at risk of extortion, and this can severely damage trust.

Phishing scams

Phishing is one of the most effective methods for attackers to infiltrate dental networks. These scams often involve emails or other messages that appear legitimate but contain malicious links or attachments. With the rise of AI, phishing campaigns are becoming more sophisticated, leveraging AI-generated content to create emails that are nearly indistinguishable from genuine communications. Cybercriminals are using AI tools to craft convincing phishing messages, mimicking official language, branding and even tone. These AI-powered attacks make it more difficult for dental staff to detect fraud. In a study on the performance of phishing emails, 60% of participants fell victim to AI-generated phishing emails, and research by the same authors found that AI phishing automation allows cybercriminals to enjoy a 95% increase in efficiency.[4,5] A white paper by the US Department of Health and Human Services on the threat of AI-augmented phishing to the health sector also pointed out that AI has made phishing attempts more effective, and it reported that

ransomware attacks and data breaches often begin with a successful phishing attack.[6] From this, it is easy to see why training for all team members using email in a dental practice must be improved.

Cybercriminals are leveraging AI to automate attacks, strengthen malware, and exploit gaps faster. AI allows attackers to launch phishing campaigns on a massive scale, tailoring messages to individuals based on data harvested from social media and other online sources. AI-enhanced malware can adapt in real time, making it more difficult to detect and neutralise. AI tools can scan networks and identify vulnerabilities more efficiently than traditional methods can.

Data breaches

Data breaches can occur through vulnerabilities in software, weak passwords, or even accidental insider actions, such as being captured by phishing emails or simply being tricked into handing over log-in credentials through various means. These breaches expose sensitive patient information, potentially resulting in significant financial and reputational damage for dental practices.

In December 2023, Hapy Bear Surgery Center, a paediatric dental surgery centre in Tulare in California in the US, experienced a data breach.[7] Sensitive patient information, including names, Social Security numbers, health insurance information and medical records, was compromised. The centre agreed to a class action lawsuit settlement, offering affected individuals up to US$8,050 in compensation and two years of credit monitoring services. Managed Care of North America Dental, a major dental insurer, experienced a cyberattack between 26 February and 7 March 2023.[8] The LockBit ransomware group stole approximately 700 GB of data, affecting nearly nine million patients. Compromised information included names, Social Security numbers, health insurance details and dental records. The company refused to pay the US$10 million ransom, and the cybercriminals released the stolen data online in early April.

Beyond compliance issues, data breaches erode patient trust and can have costly legal consequences. Cybercriminals often use stolen data for identity theft or sell it on the dark web. Health information is not like a credit card that can simply be cancelled and replaced when breached. Health histories, for example, often contain some of the most sensitive and potentially embarrassing information about an individual, such as medications, treatment, and diagnoses.

Insider threats

Insider threats, whether intentional or accidental, pose a significant risk. Some examples are:

- Employees may unknowingly expose the network to malware by falling victim to phishing attacks.
- Systems and software may be configured improperly, allowing staff members access they should not have.
- Team members may surf the web or access personal email through practice systems, exposing the network.
- Lack of training about common telephone or other scams can put the practice at risk.
- A team member may act in a nefarious manner by trying to copy or steal data or manipulate systems to cover his or her tracks in cases of internal fraud.

Simple steps to strengthen cybersecurity in dental practices

It is evident from what has been explained in this article series so far that it is vital to create a budget for cybersecurity management. In many cases, a practice's IT support providers do not have the necessary skills, certifications, and experience to monitor and maintain the many aspects of compliance and cybersecurity best practices. Rather you should work with experts who understand dental cybersecurity to implement tailored defences. Cybersecurity is a specialty requiring many years of training, a professional certification process and experience. In order to select the appropriate provider for your practice, consider the following:

- *Specialisation in dental practices:* Ensure that the provider understands the unique technology used in dentistry, the compliance requirements relevant to the country in which you practice and the workflows in dentistry.
- *Certifications and expertise:* Look for a provider with credentials like Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information Privacy Professional (CIPP). Experience in managing dental office security is also paramount.
- *Proactive threat management:* Verify the provider's ability to provide continuous monitoring, incident response and solutions like end-point detection and response, which monitors devices such as computers, servers and digital imaging systems for threats.
- *Data protection and compliance:* Confirm that the provider offers robust encryption, secure data backups, and tools to maintain patient privacy and compliance with legal regulations.
- *Training and support:* Choose a provider that offers ongoing cybersecurity training for staff and responsive technical support to address issues quickly.

Once you have found the appropriate certified cybersecurity professional for your practice, here are the main strategies you should work on together:

1. Develop a comprehensive cybersecurity programme

- A strong cybersecurity programme is essential for protecting patient data and preventing cyber threats. To achieve this, you should:
- formalise a cybersecurity programme that includes clear security policies that define how data should be accessed, shared and stored, as well as regular security reviews