Cybersecurity and Business Continuity Planning

Tips, Tools, and Technology to Keep Your DSO Safe

planet DDS

Contents

Cyberattacks are rapidly evolving. Bad actors keep finding new ways to infiltrate systems, including sending email attachments posing as doctor referrals, new patient paperwork, or vendor-related announcements such as a product recall.

Understanding how to protect your DSO is crucial not just for compliance, but also for maintaining trust with your patients.

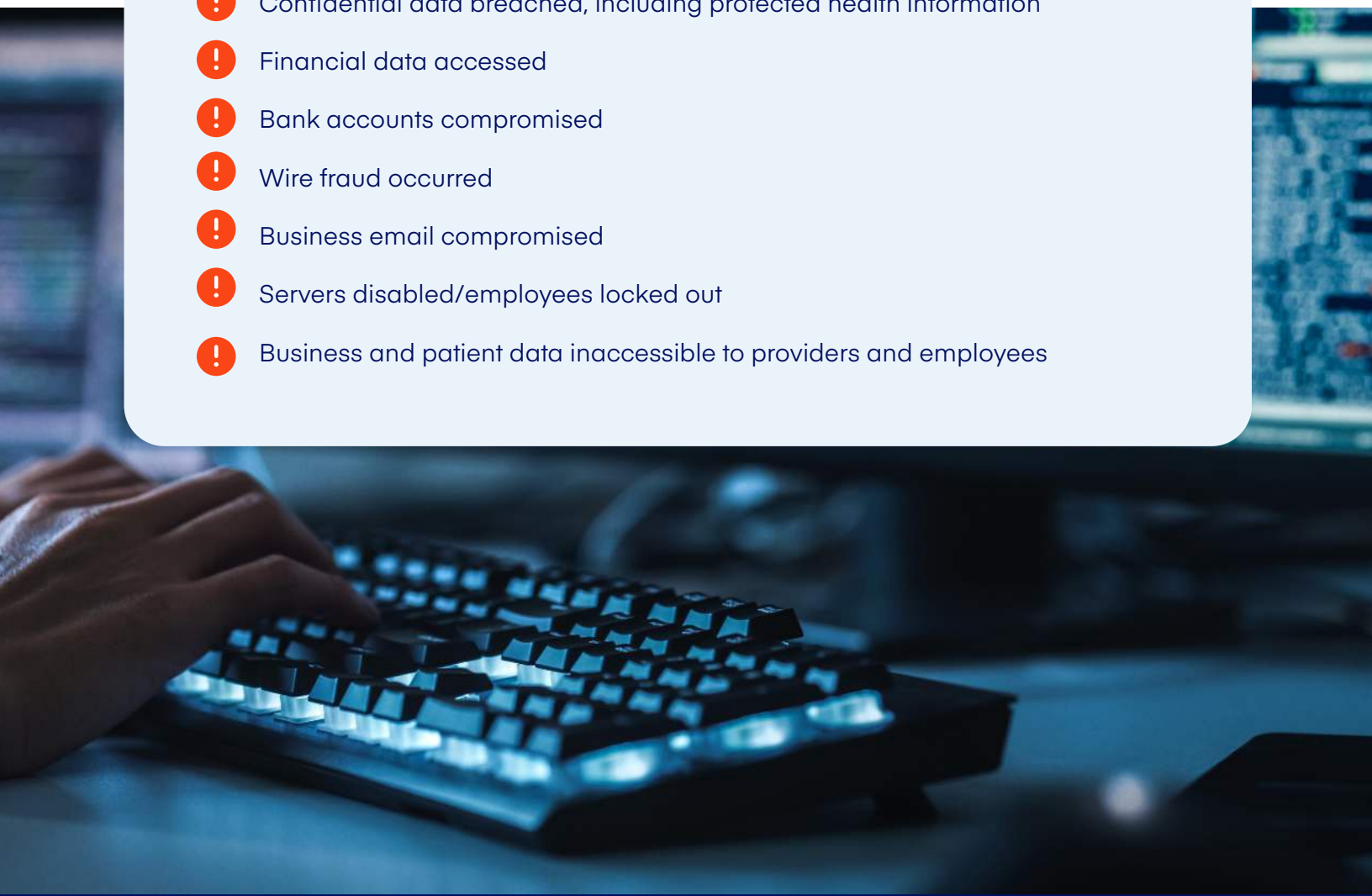
What Will a Cyberattack Cost You?

Getting struck by a cyberattack can cost a dental company millions of dollars.

Gary Salman, CEO of Black Talon Security, says it takes on average 10 business days to recover from a ransomware attack. The firm recently helped a 14-location dental support organization (DSO) that was hit with a $2 million ransomware demand. Even smaller attacks can cost a minimum of $100,000, Salman said.

Black Talon Security receives multiple calls each week. The problems include:

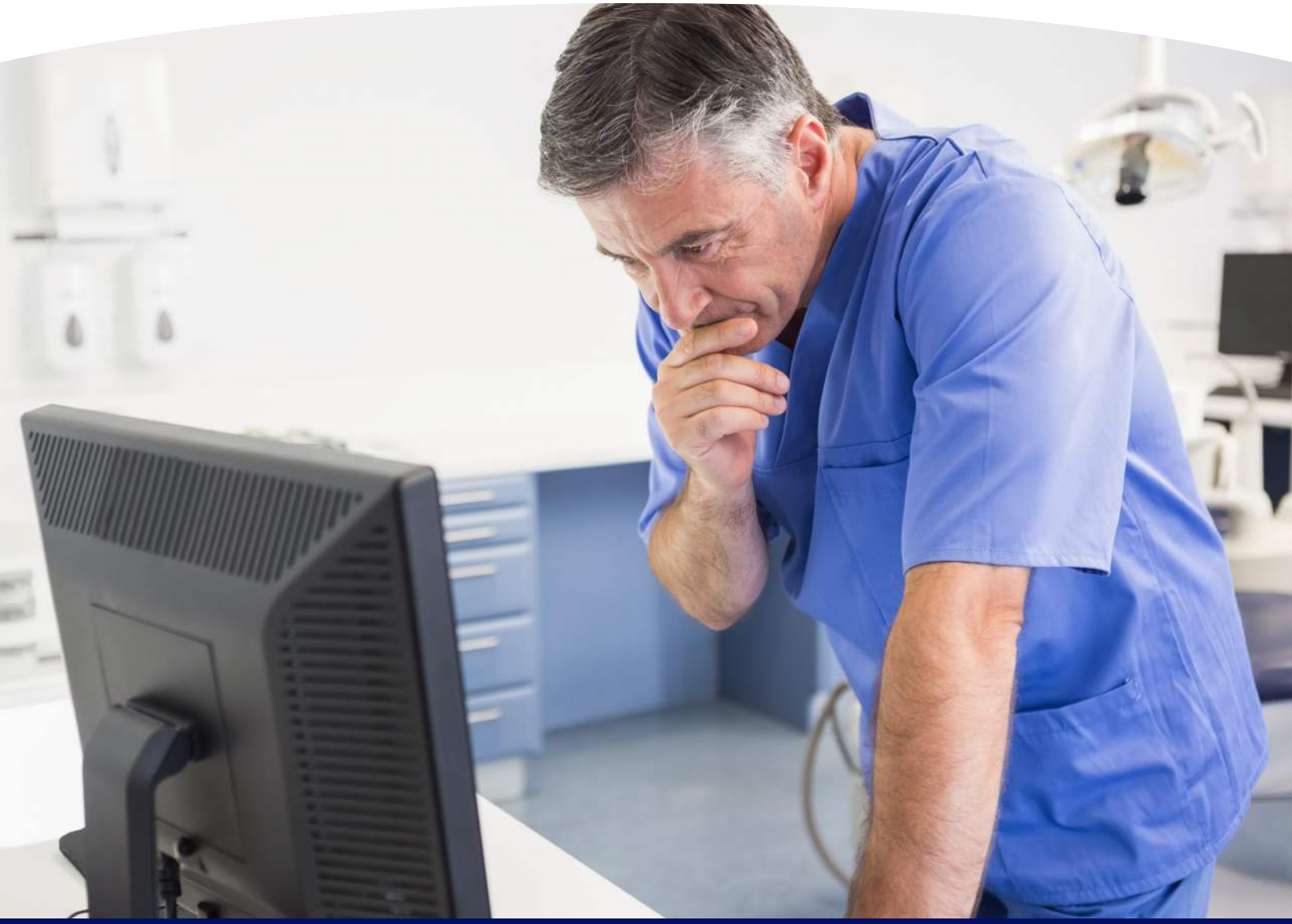
- Confidential data breached, including protected health information
- Financial data accessed
- Bank accounts compromised
- Wire fraud occurred
- Business email compromised
- Servers disabled/employees locked out
- Business and patient data inaccessible to providers and employees



Common Cyberthreats

Data breaches can lead to identity theft, financial loss, and severe damage to your organization's reputation. Three common entry points are:

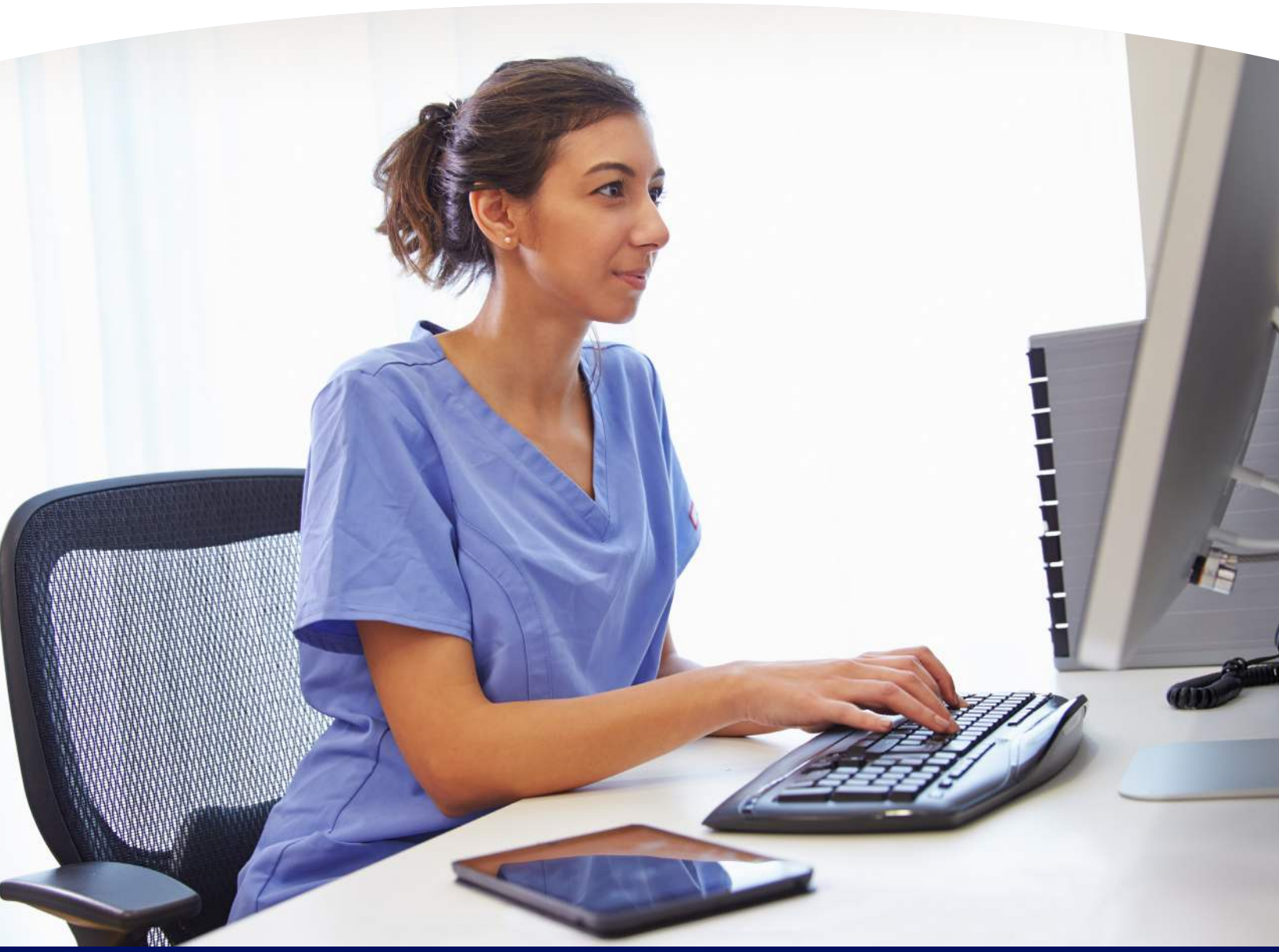
1. **Phishing attacks:** deceptive emails designed to steal login credentials or financial details, and may contain malicious links or attachments
2. **Ransomware:** malicious software that encrypts your data, demanding payment for access
3. **Data breaches:** unauthorized access to patient data, often due to weak passwords or unpatched systems



Conducting a Risk Assessment

Identify vulnerabilities by conducting a thorough assessment of your current IT infrastructure, including:

- **Network security**, including malware detection software and email security tools
- **Employee training** with videos, alerts, and simulations to teach them how to spot fake emails, text messages and links
- **Software updates** with patches applied across all devices

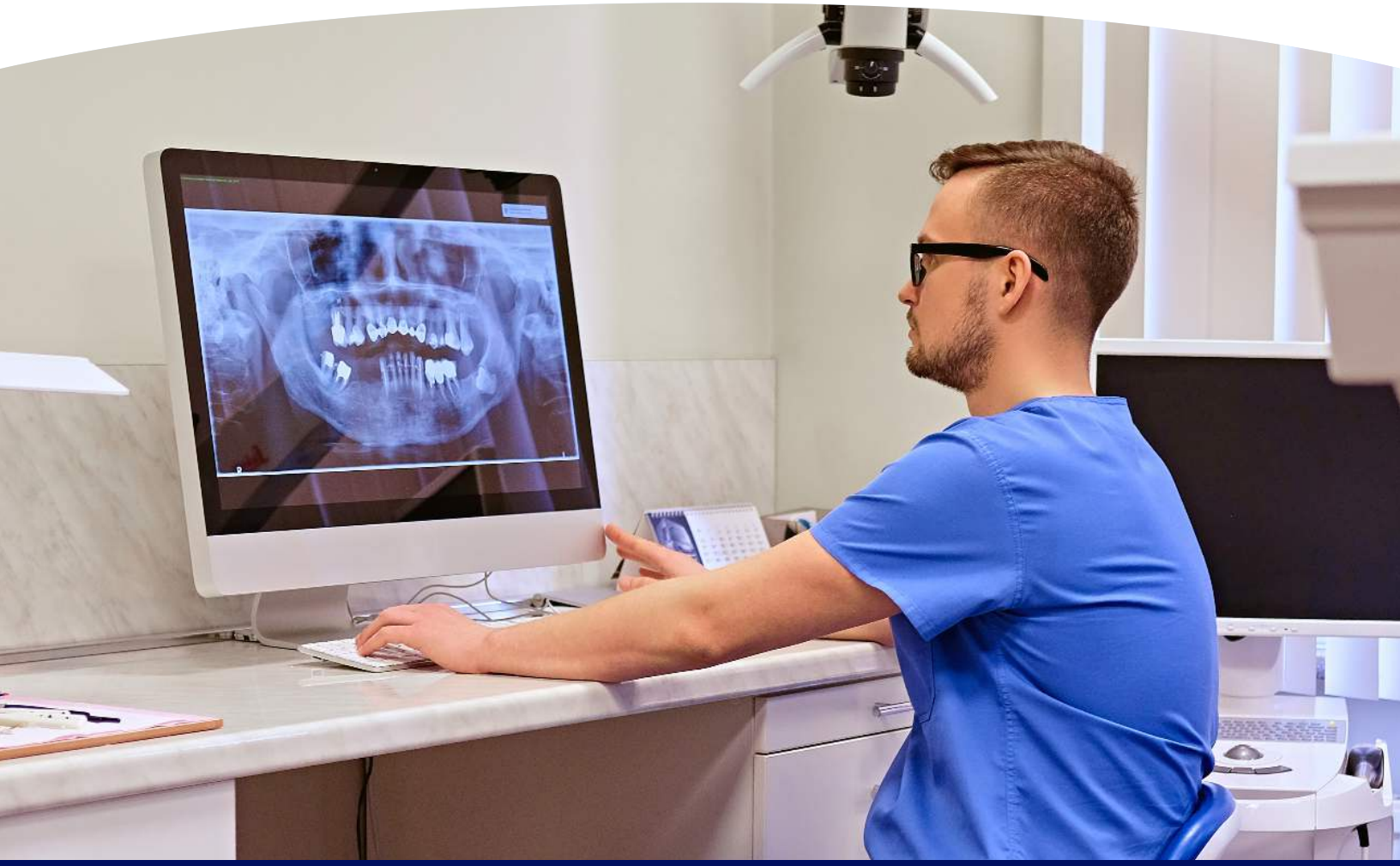


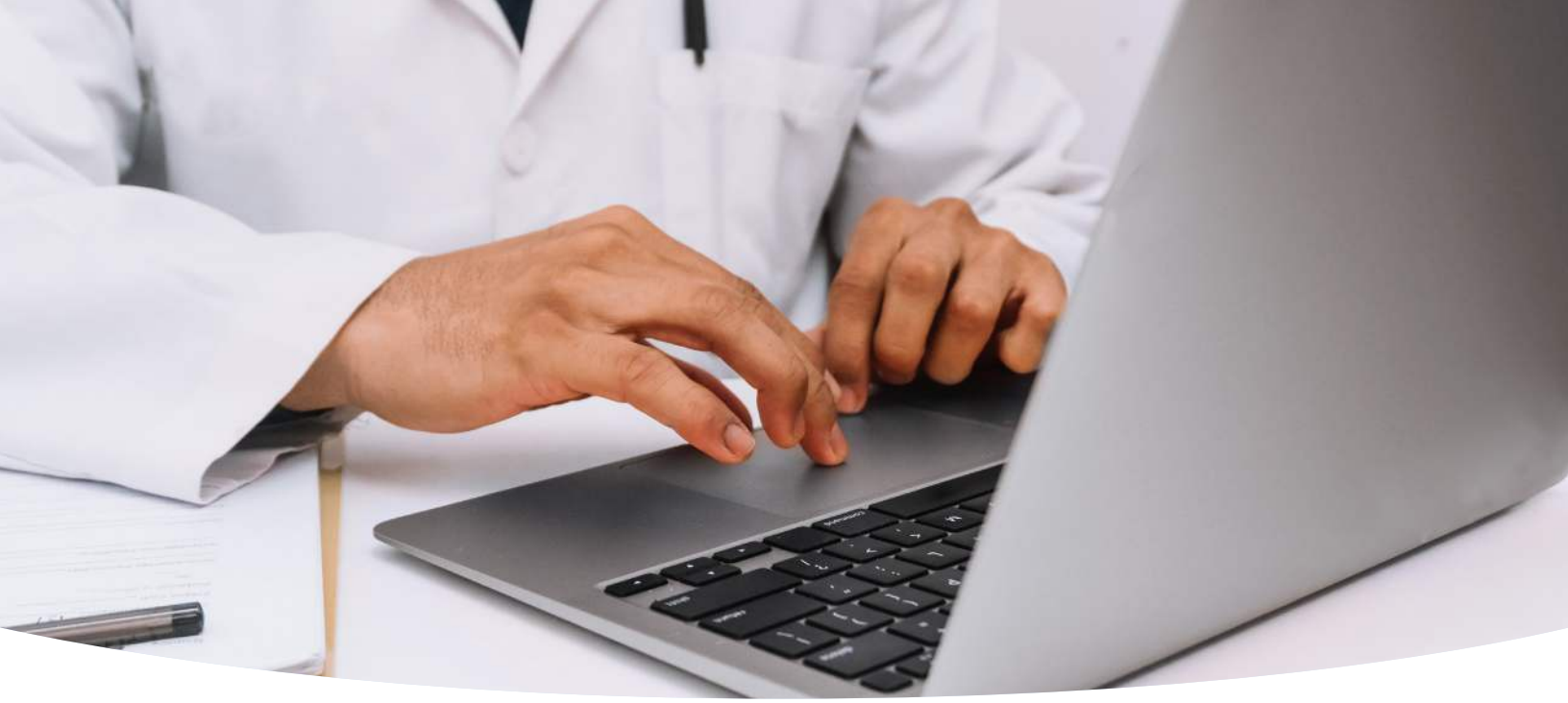
Building a Cybersecurity Framework

There are two important vulnerabilities to address: your people and your technology.

To limit the damage that could be caused inadvertently by a team member, develop a cybersecurity policy that outlines the acceptable use of technology, data protection protocols, and incident response plans. Ensure all team members are trained on the policies and procedures, and foster an environment of awareness and vigilance, including:

- **Use only work devices** to access work files
- **Verify URLs and documents** are legitimate before clicking
- **Ban password-sharing** among team members





To limit technical vulnerabilities, implement technical controls such as:

- **Firewalls** to protect your network from unauthorized access
- **Encryption** to safeguard patient data both in transit and at rest
- **Software updates** including authorized patches to keep software programs and systems current
- **Constant vulnerability scanning** with quick remediation and annual penetration testing
- **Multi-factor authentication (MFA)**, which adds an extra layer of security by requiring someone to enter a code sent to their phone, scan a fingerprint, or answer a question to access the website or application
- **Pre-set account restrictions** to limit access based on factors such as time of day or IP address
- **File alerts** that trigger when file shares and/or file servers are unexpectedly renamed
- **Backup system** for critical functions, such as medical records, payroll, communications, phone systems and computer systems

While most IT companies excel at setting up networks, they may have only limited knowledge of data security controls that can prevent a breach. You may want to have an independent third party validate and manage your security.

Developing an Incident Response Plan Before You Need It

An Incident Response Plan is also called an Emergency Action Plan or a Business Continuity Plan. The key is to have it created and posted in the workplace where employees can view it—even if the computers are locked up.

The Incident Response Plan should include:

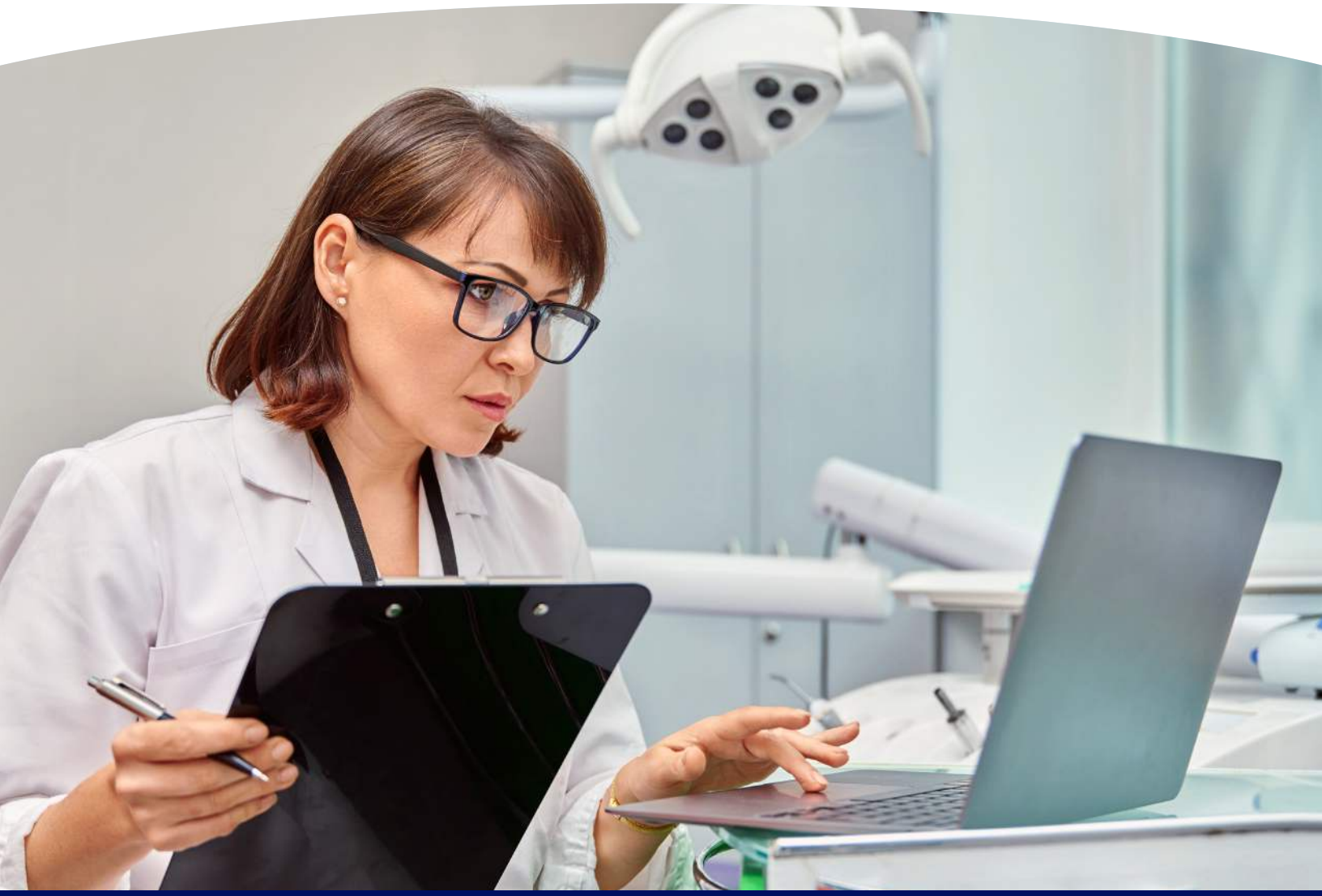
- Procedures and contact information for reporting the emergency
- Names and job titles of every employee who may be contacted for information
- Defining employees involved in critical operations and their role in the emergency
- Process for communicating information to staff and, if needed, to patients

Best practices include training employees on the incident response plan and having them sign an acknowledgment form and participate in mock exercises.

Defining Your Business Interruption Recovery Strategies

Law enforcement officials, insurance companies, and security firms such as Black Talon Security will need information to start their investigation, including:

- **Date and time** the incident was discovered
- **Names and contact information of anyone involved** with the discovery and the response
- **What was accessed** and/or viewed improperly
- **When a ticket was submitted** to your practice management system provider



Selecting the Right Partners

Cybersecurity firms like Black Talon Security can help you design, implement, and maintain a cybersecurity framework tailored to your DSO.

Selecting a practice management provider with a proven focus on security also helps. Planet DDS is the first practice management solution provider to achieve Soc 2 Type 2 attestation for all of its products including Denticon, Cloud 9, Apteryx, and Legwork. This is the "gold standard" for stringent data protection in the healthcare industry.

To learn more about how Planet DDS can help your DSO or group, visit PlanetDDS.com.

Planet DDS solutions are designed to optimize operations for your DSO or group.

- Cloud-Based Practice Management
- Ortho Practice Management
- Digital Imaging
- AI for X-Rays
- Dental Marketing
- Online Scheduling
- Digital Forms
- Easy Analytics & Reporting
- Patient Communication
- Two-Way Texting
- RCM Automation
- Online Bill Pay

TALK TO OUR TEAM

planet DDS

planet DDS

denticon | apteryx | legwork | cloud 9

Planet DDS is the leading provider of cloud-enabled dental software solutions, serving over 13,000 practices in the United States with over 118,000 users. The company delivers a complete platform of solutions for dental practices, including Denticon Practice Management, Apteryx Cloud Imaging, Cloud 9 Ortho Practice Management and Legwork Practice Marketing. Planet DDS is committed to creating value for its dental practice clients by solving the most urgent challenges facing today's dental practices nationwide.