7 Urgent Security Protections Every Dental Practice Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on dental offices who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

Provided By: Sagester Associates Group, Inc.
Author: Fred Sagester
P.O. Box 681, Columbus, IN 47202
www.sagester.com, 812-314-6724

Sagester Associates Group

Are You A Sitting Duck?

You, the doctor of a small practice, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of dental practices like yours to steal credit cards, patient information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more practices utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

1. **Train Employees On Security Best Practices.** The #1 vulnerability for dental practice networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **Create An Acceptable Use Policy (AUP) – And Enforce It!** An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices to access practice e-mail and data.

If that employee is checking unregulated, personal e-mail on their own device that infects that device, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase practice data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your practice at risk.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **Have An Excellent Backup.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

Sagester Associates Group

6. **Don't allow employees to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.

7. **Don't Scrimp On A Good Firewall.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

Want Help In Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our security consultants to your office to conduct a free **Security And Backup Audit** of your company's overall network health to review and validate different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

Sagester Associates Group

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.
- Is your firewall and antivirus configured properly and up-to-date?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your practice is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the dental practices we've audited over the last 15 years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your practice, your reputation, and your data are protected. Call us at 812-314-6724 or you can e-mail me personally at fred.sagester@sagester.com

Dedicated to serving you,

Fred Sagester
Web: www.sagester.com
E-mail: fred.sagester@sagester.com

Sagester Associates Group

Here's What A Few Of Our Clients Have Said:

Sagester's response time is Great

"Sagester Associates Total Care support provides proactive monitoring and maintenance of our office computers. **When we have an issue, a quick email gets us an immediate response.** A big benefit of the Sagester Total Care package gives us an annual assessment of all supported computers. This helps me as owner, stay on top of aging equipment and needed upgrades without any surprises.

Sagester' s response time is great. With our other vendor it would take several days to receive service now urgent needs are right away. On days when our office isn't super busy the Sagester tech team works through a "punch list" at a scheduled time which really helps with our schedule.

In the dental field, it is nice knowing that Sagester Associates has probably encountered this problem before. If they have not, they definitely have the resources to work with software and hardware specific to the dental field." – **Drs. James and Gina Saindon – Somerset, Kentucky**

They are professional and courteous, and always address any problems in a timely fashion

"Our dental office has been working with Sagester Associates Group for many years. We had recently switched from Softdent dental software to Dentrix, and were in the process of transitioning to a paperless office. Fred Sagester and his staff assessed our needs, and implemented a computer system that works for us. They are professional and courteous, and always address any problems in a timely fashion. We would highly recommend Fred and his team to any office in need of a computer system overhaul, or something as simple as dependable technical support." - **Dr. Jimmy Hill - Lexington, Kentucky**

No more frustrations!

"I have had Sagester Associates Group take care of all my hardware and computer network needs since I opened my office in 2005. I opened from scratch and that was stressful enough. The last thing I needed was to worry about my computer system and software integration. Sagester was easy to deal with and they helped my start-up open smoothly. I had such a great experience that I still use them for my network support. They are always very responsive and quick to help whenever I have issues. I think that one of the main things that separates Sagester from their competition is that they understand dentistry and the software involved. I remember how frustrating computers were while I was an associate. I now understand that the frustration came because the support company did not understand dentistry. I have never had that frustration with Sagester. I would highly recommend Sagester!" - **Dr. Jon Erickson - Danville, Indiana**

Sagester Associates Group

Sagester Associates Group is prompt to find a solution

"We are a very busy, multi-doctor pediatric dentist office that schedules 90+ patients a day. For years we had numerous, reoccurring problems with our computer network. Since Sagester Associates Group "tweaked our network system," our 30+ network stations are running smoothly with minimal problems. On those rare occasions that we have a problem arise, Sagester Associates Group is prompt to find a solution. They have been aptly handling all of our "IT" needs as well as our daily back-ups for over 5 years!!!" **- Drs. J. Stritikus and J. Robbins - Dickson, Tennessee**

I could not believe how efficiently they installed and networked our computer and digital equipment.

"I have been a client of Fred Sagester for several years. He and his associates are very reliable and skilled with their services. I relocated my dental office a few years ago and greatly expanded my digital and computer technology. I could not believe how efficiently they installed and networked our computer and digital equipment. In a fully computerized office, it is great to know the Sagester Associates Group is there when I need them!" **- Dr. Kim Nichols – Lexington, Kentucky**

Sagester keeps us up and running, with very few problems

"We purchased our practice management software in December 2004, Sagester provided the hardware, installation, and maintenance 24 hrs. a day since we started. We looked back and couldn't believe how long we have been involved with Sagester. 12 years doesn't seem possible. The most remarkable thing, and we say it with fear and trepidation, is we have been down only one 8-hour day and that was for a scheduled hardware installation. We believe that is pretty amazing. They are on call for our office 24 hours a day, 7 days a week, and we always get our problems solved quickly. If a problem arises above the technician, Sagester is always there to solve it. We of course do everything they recommend and we always do have Sagester do our practice management updates. We have never had a problem with, "It is the hardware, No it's the software problem!?!" They absolutely work in conjunction with each other. Sagester keeps us up and running, with very few problems. Sounds like a marriage made in heaven. We recommend Sagester whole heartedly. They know our practice management and imaging software inside and out." **- Dr. David Walters – Princeton, Indiana**