"A Match Made in _____"

Cyber Threats and HIPAA Compliance - There is Hope

Are we at the beginning, middle or end? Please let it be the end. Recent events have caused many in the business community to think these thoughts, especially in healthcare.

Cyber Crime has exploded. The global cost of cybercrime will reach $2 trillion by 2019, a threefold increase from the 2015 estimate of $500 billion. Last year, IDG detected 38 percent more cybersecurity incidents than the year prior. Source – SecurityIntelligence by IBM

HIPAA enforcement is real. Due to the intensity of compliance and regulations, the costs per breach to organizations in the health care and financial services sectors top all other industry groups, according to the Ponemon study.

Small Business Beware! Small and midsized organizations (SMBs), defined as those with less than 1,000 employees, are hardly immune to cybercrime — actually quite to the contrary. According to Keeper Security's "The State of SMB Cybersecurity" report, a staggering 50 percent of small and midsized organizations reported suffering at least one cyberattack in the last 12 months.

A Cyber Attack may be considered a HIPAA breach according to the OCR's Wall of Shame and as outlined in the following headline from HealthITSecurity.

> *"The top 10 healthcare data breaches of 2016 were mainly caused by cybersecurity attacks, including ransomware and unauthorized access."*

So, the marriage has been made. Cyber-attacks are directly linked to HIPAA breaches. This presents a real and present risk to all dental practices. As we know, a breach can occur at any time and many dental practices are still open doors for cyber criminals.

We are not at an end, we are more near the beginning. Cyber criminals are well-funded and becoming increasingly organized.

Ransomware – the latest wave

What is ransomware? Ransomware is a virus designed to block access to the data in a system until money is paid. Ransomware usually is planted in a clinic's network environment via an attachment to an email. The virus immediately does three things:

1. Begins encrypting data on the computers
2. Sends the decryption key to their own "secret" location
3. Grabs all contacts and forwards the nasty email (then it looks like a "friendly email")

There is Hope

What can we do? In the IT Managed Services arena, the Dental Integrators Association (DIA) recent national conference discussed this topic at length with guests from the FBI Cybersecurity Division. DIA member companies are well aware of the threats and have been working diligently to create solutions. The best thing you can do, is work with a managed IT provider who will secure your systems before you have a breach.

In closing below are a few simple short-term tips for each of you. Beyond the short term, please build a plan for the long term.

Simple and Practical suggestions for all dental practices:

- Partner with a credible IT/Cyber Security company. The DIA and its member companies take these matters seriously.
- Make Cybercrime and HIPAA a higher priority and invest resources in solutions
- Cyber Tips
    - Allow the partners to deploy a credible firewall
    - Allow the partners to deploy a credible back-up solution that includes Business Continuity
    - Do not open email attachments! Make sure the attachment is clean. Clean can be because the email was sent via encryption, or just call the sender and verify they actually sent the email.
- HIPAA
    - Build a comprehensive plan to address HIPAA in your organization
    - Begin with a HIPAA risk assessment
    - Train your staff
    - Get Business Associate agreements in place
    - Go back to your comprehensive plan

Sunset's knowledgeable employees can help you when you need it the most. Their support lines are answered 24 hours a day, seven days a week. Sunset Technologies knows what to do and how to handle situations such as these to ensure downtime is kept to a minimum. Sunset also knows how to avoid these situations. Your company is important to you and to us, let us help you keep it protected.

"REST ASSURED" with Sunset Technologies.

Call Sunset Technologies at (855) 861-8833 or visit us online at www.SunsetSecure.com.