VIPRE®
AntivirusBusiness

Strategies For Boosting Your Practice's Information Immunity

Cyber Threats are Real.
Protect Your Healthcare Practice Now.

Every day, viruses – along with worms, spyware, Trojans, bots, rootkits and other malicious intruders – infect millions of computers and shut down businesses large and small all over the world. Medical practices are not immune to these threats and their ensuing data breaches.

Rich repositories of personal, clinical and financial data, combined with relatively modest information management capabilities, make medical practices prime candidates for numerous cyber threats, from hacking to computer viruses. These threats will likely be more widespread as practice management systems increase in sophistication, patient information becomes more connected through electronic health records and health information exchanges and health data becomes more accessible as practices increase their use of tablets, smartphones and other mobile devices.

According to a 2011 patient privacy and data security benchmark study of 72 healthcare organizations[1]:

- 96% of healthcare providers said they had at least one data breach during the previous two years.
- Data breaches cost healthcare organizations approximately $2.2 million on average – not including time and productivity loss, brand or reputation diminishment or loss of patient goodwill.
- 30% of breaches were the result of criminal attack, up from 20% in 2010.
- 14% of breaches were the result of a malicious insider, about the same percentage as in 2010.
- While 81% of organizations said they're using mobile devices to manage some form of protected health information (PHI), 49% said their organizations are not doing anything to protect those devices.

Physicians know how to treat human-borne viruses but are often unprepared to deal with the ones infecting their PCs.

Rich repositories of personal, clinical and financial data, combined with relatively modest information management capabilities, make medical practices prime candidates for numerous cyber threats, from hacking to computer viruses.

- Nearly half of data breaches occurred due to lost or stolen computing devices.
- More than 50% of healthcare organizations said that neither billing nor information technology (IT) personnel in their organizations understand the importance of patient data protection.

The promise of technology can be wiped away in seconds with just one incident, so now is the time to assess your practice's information systems risk. It's truly business critical to implement strategies that can both reduce that risk and help ensure compliance with privacy and security rules, including those created as a result of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

> **With its storehouse of patient personal information, your practice is a tempting target.**

Here's a closer look at a few of the common cyber threats your practice faces today – as well as strategies for mitigating them.

External Threats

Malware attacks have become increasingly prevalent, with more than 55,000 new malicious programs uncovered each day[2]. Malware – short for malicious software – creates a bevy of problems for its victims, from annoyances to catastrophes, such as total system failure. Cybercriminals use software (or code) to achieve unlawful access and control of computer systems, interrupt the operation of computers, collect confidential data or log keystrokes to harvest passwords and access financial accounts.

Cybercriminals, for example, may seek to harvest email contact lists through phishing schemes, such as sending emails that mimic communications sent by banks and credit card companies in an attempt to get recipients to reveal personal information. These emails also can be crafted to seed computer viruses through malicious email attachments – even images – that, once downloaded, can pilfer passwords, account numbers and other personal data from unsuspecting victims. Years ago, these malevolent emails were easy to identify by their "fake" appearance; today's electronic communications scammers are more sophisticated and can develop sham emails convincing enough to fool even the seasoned user.

Malware attacks are designed to gain access to data to later use for the criminal's gain, infect machines or an entire network to destroy or corrupt data or literally turn the computer under attack into a robot. A prevalent and dangerous form of malware is a Trojan program. Unlike a virus, it does not cause harm by replicating itself, but rather works quietly to locate passwords or financial data. It may permit another person to take control of the infected computer or network from a remote site so as to spread malware, spam or phishing schemes – often, without the knowledge of the infected computer or network's owners. Software and utility downloads from websites are common routes of entry for Trojans.

With its storehouse of patient personal information and financial data, including credit card numbers and health insurance identification numbers, your practice is a tempting target for those who want to use or sell this type of data – and the criminals need only one weak link, such as an under-secured computer or portable device, to gain access.

With new, more sophisticated and increasingly harmful malware circulating each day, cybercrime is a frightening but real proposition for medical practices.

So how do you protect your practice – and your patients? Start with a robust antivirus solution. While there are literally hundreds of antivirus programs on the market, a medical practice serious about arming itself against cyber predators needs a solution that features:

- Innovative technology that will not decrease employee productivity by slowing down computers and networks, a common problem with many antivirus solutions
- Efficient detection intelligence that automatically monitors and identifies security deficiencies
- Comprehensive, user-friendly administration tools that allow the manager to effectively and quickly detect problems

- » An intuitive interface that's easy to learn and use
- » Fast, straightforward deployment

Conclusion

The rapidly accelerating adoption of electronic health records and mobile technologies is not likely to reduce the type and frequency of cyber threats practices face. These threats, which carry legal, financial and public relations consequences, must be managed effectively to protect your practice and its patients.

You can start by:

- » Understanding the privacy and security regulations with which your practice must comply
- » Picking the low-hanging fruit: address the common information privacy and security threats outlined in this paper
- » Conducting a practice privacy and security risk assessment to identify vulnerabilities
- » Establishing policies and procedures for handling sensitive and critical data, and ensure employees receive adequate training in those policies and procedures
- » Instituting an Internet acceptable use policy for staff and communicating the benefits of having such a policy

Now is the time to assess your practice to reduce risk and help ensure compliance with privacy and security rules.

Technology offers incredible value to you and your patients. If not managed appropriately, however, the very strengths and opportunities that technology offers can be used by cybercriminals – or even innocent employees – to cause devastation for medical practices. Don't let your medical practice be a victim: safeguard your practice today with a comprehensive and effective solution to protect against computer malware.

About VIPRE® Antivirus Business™

VIPRE Antivirus Business combines the latest antivirus and anti-spyware detection and removal technologies to protect against next-generation malware threats in a comprehensive and highly efficient manner. Built by IT administrators for IT administrators, VIPRE is easy to install, easy to deploy and easy to manage with minimal network and system performance impact. The solution delivers superior endpoint protection against viruses, worms, spyware, Trojans, bots and rootkits via a single, powerful anti-malware engine.

For more information, visit **www.ThreatTrackSecurity.com/VIPRE**.

[1] Second Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute Research Report, December 2011.

http://thielst.typepad.com/files/2011-ponemon-id-experts-study.pdf

[2] AV-TEST Institute, February 2012. www.av-test.org/en/statistics/malware

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security, Inc makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security, Inc makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.