GFI White Paper

Strategies for boosting your practice's information immunity

Physicians know how to treat human-borne viruses but are often unprepared to deal with the ones disseminated by computers.

GFI®

Contents

Introduction

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 became 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]:

- Ninety-six percent 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.
- Thirty percent of breaches were the result of criminal attack, up from 20% in 2010.
- Fourteen percent 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.
- 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.

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

[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**

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

Although antivirus software can be installed on each machine individually, a practice reliant on its practice management and electronic health record systems will find it more efficient and effective to implement a practice-wide solution. The advantages of a practice-wide solution are many:

- Network-wide monitoring continuously evaluates the network and servers for viruses
- Each computer on the network is continuously monitored
- Frequent updates and scans run in the background without interrupting or requiring any action from everyday users
- Malicious attacks and costly system downtime are avoided, allowing the practice's staff and physicians to work uninterrupted by computer security related 'glitches'

Another critical practice-wide solution – patch management – should not be overlooked or undervalued. First of all, computers certainly aren't perfect, and thousands of 'patches' designed to resolve detected problems in computer programs are released each day by various software vendors. While many patches fix various 'bugs' or annoyances for users, they also thwart many of the new and emerging malware in order to keep your network, its computers and other devices safe from viruses, intrusions, Trojans and other hazards designed to exploit flaws in the software applications we use every day. And that includes software programs from leaders like Microsoft®, Adobe® and Google.

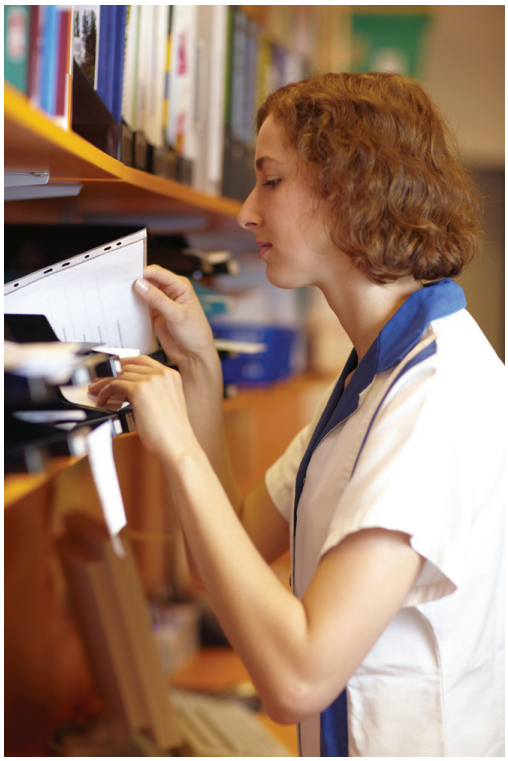
While it is important that patches are updated frequently, it is just as crucial that they are implemented immediately. These fixes to various programs – Microsoft® Office, for example – can be delivered to individual computers. Users who have not set their computers to automatically install new patches and updates may notice alerts popping up frequently on their computers. While it is common knowledge that these updates are necessary to ensure optimal productivity as well as prevent cybercriminals from attacking the latest exposed vulnerability, many users ignore or delay these updates. In the workplace of your medical practice, many staff may diligently install software patches when notified, but many others may not deploy them immediately – or ever. A medical practice has too much to lose from inconsistent installation of patches, which is why an automated network solution is the safest and most secure route to follow.

Effective patch management assures a consistently configured environment that is secure against known operating system and application software vulnerabilities. The challenge for medical practices is to manage all the updates for the numerous applications and operating system versions they use. Medical practices need a sophisticated, continuously updated solution that can manage patches across many platforms, as well as scan, detect, analyze and resolve vulnerabilities on the practice's network.

As the connectivity and accessibility to networks and the Internet improve and become indispensable features for today's users, the potential for exposure to computer malware increases. The best defense against these external hazards is a robust and vigilant antivirus paired with an automated patch management solution.

Internal challenges

Between 2005 and 2009, several hospital employees of the University of California Los Angeles (UCLA) Health System were caught peering at medical records of celebrities, including Britney Spears and Farrah Fawcett. As UCLA and other health organizations have learned the hard way (including six-figure settlements with federal regulators), a practice's own employees present another potential source of computer insecurity.



While your practice may not treat Hollywood celebrities, the potential of these illegal intrusions remains a possible source of legal liability, not to mention a public relations nightmare. Fortunately, monitoring tools can be put in place to track internal activities on computer networks to thwart many of these threats.

Think of how it is possible in your practice management system to view reports of registration errors and track which staff member is the most frequent cause. Usually, it is thanks to the employee's identification "stamped" by the system on those events. Monitoring software can similarly stamp and log each time data is extracted from your system. Important details, including what was viewed or extracted, the person who

logged in to do so, the workstation used and the date and time all can be logged. Continuous attention must be given to staff training about computer security, guarding one's passwords and the legal consequences of violating state and federal privacy laws.

Another internal threat comes from unintentional security breaches that employees and other authorized system users may cause. It is no coincidence that the surge of cyber-attacks correlates to the rise in the nearly unfettered use of search engines, social networks and other web-based applications by employees using workplace computers. Many practices make frequent contact with the Internet throughout the day for legitimate activities, such as corporate use of social networking sites for marketing, submitting or confirming prior authorizations of medical services, determining insurance claims status and verifying insurance coverage and benefits eligibility. With these contacts becoming much more frequent and spread across more staff, attention to monitoring usage becomes crucial.

Accompanying the greater use of web-based tools for practice activities is the rise of employees' use of social networking in the workplace. Indeed, studies show that a significant percentage of employee time – forty percent of their Internet activity while at work, according to cyber-research firm International Data Corporation (IDC) – is not linked to work. Social networking sites are more than a distraction; they are also a target for attacks by cybercriminals. As social networking sites, search engines and online advertisers improve techniques to gather intelligence about users, cybercriminals, too, find tremendous value in knowing more about users. Unfortunately, the criminals' uses of information they gather can have unpleasant and sometimes expensive consequences.

Once upon a time, medical practices could limit Internet access to a select few, trusted employees. With everything from insurance verification to referral coordination migrating to the Internet, medical practices can no longer parcel out web access – most employees have legitimate business reasons to use the Internet. The best defense is one that improves, not impedes productivity: a solution that can monitor employees' Internet usage while maximizing employee productivity and practice compliance with security regulations and best practices.

A well-designed monitoring solution protects networks and data by:

- Controlling which types of files and applications may be downloaded from the Internet by workstation, by workgroup, by individual or network wide
- Providing detailed reports of employees' online browsing habits
- Maximizing available bandwidth by blocking streaming media and large file downloads and by setting thresholds for each user's bandwidth usage
- Blocking websites and social networking-fed phishing schemes and other online scams
- Actively monitoring employees' web browsing so as to filter and block suspicious Internet domain addresses without blocking useful, work-related browsing
- Supplying network and practice managers with understandable and customizable reports

A web monitoring solution can provide value to medical practices by keeping a record of each user's web activities including the websites they visit, the frequency of their visits, the length of time spent on which web pages and at what times of day.

A web monitoring solution should provide managers the ability to:

- Determine whether office computers are used for non-business purposes, by whom and how often
- Restrict access by individual user or groups of users, allowing the practice to block or limit access to non-work related sites, including personal webmail sites like Gmail and Yahoo!
- Track the time each employee spends on the Internet and on which websites
- Provide real-time monitoring of browsing and downloads
- Eliminate viruses and other malware through the use of antivirus engines that check each URL visited and each file or application downloaded
- Impose customizable limitations on each employee's use of the web, unauthorized software and devices and bandwidth
- Deliver an effective and frequently updated anti-spam solution

Finally, email is a primary communications tool. All practices should ensure they are archiving their email to not only leverage more cost-effective email storage solutions, but to protect against unintentional or purposeful deletion of sensitive information or conversations contained within them. Protect yourself and your patients by being able to search and retrieve any email communication sent or received by your practice.

Just the fax

While not likely the victim of your next cyber-attack, the fax machine is a prime candidate for a breach in security. Consider that inbound faxes wait on the machine for the appropriate user to retrieve. Often, these faxes sit for hours on or next to the machine where they can easily be viewed by anyone retrieving a fax as well as by all who walk by. Similarly, outbound faxes may wait to be transmitted – or reside in the outgoing tray long after they have been successfully sent. In a medical practice, these documents often contain confidential information about patients and are ripe for a security breach, intentional or not.

A breach of confidentiality isn't the only reason to seek a better solution for the fax machine. Medical practices that invest in electronic health records today welcome the opportunity to become paperless. That is, of course, until they realize that the fax machine is still spewing paper. Given the disparate flows of information into – and out of – a medical practice, it's virtually impossible for a medical practice to be paperless without also providing a solution for faxing.

Fax servers offer the ability for medical practices to receive and store inbound faxes electronically and then automatically distribute the faxes to pre-determined locations. Test results from a reference lab, for example, can be routed to the in-house lab. Alternately, each physician's nurse in the practice can have a designated fax number allowing the results to be transmitted to them directly.

Test results aren't the only candidates for improvement: consider the faxes that arrive daily from hospitals, nursing homes, pharmacies, vendors and the assortment of other stakeholders. Regardless of the source, these documents can be quickly and easily obtained, retrieved, viewed and, if applicable, distributed or saved to the appropriate data file when received by computer.

Inbound faxes are only one side of the equation: medical practices transmit faxes to many stakeholders. A specialty practice may fax information to referring physicians for each patient. Without a fax server, the task involved in printing and faxing these communications for each patient can mean generating reports and ensuring that each report gets to the right location. It also requires extra efforts in security vigilance as each outbound document and its cover page must be rounded up and then filed or shredded – hardly the road to a paperless practice!

A fax server permits the reports to be transmitted seamlessly to the designee, allowing staff to store up-to-date contact information for referring physicians (or other stakeholders) and effortlessly and securely transmit reports to designees. It also saves time by allowing staff to electronically retrieve and use standardized fax templates. Most importantly, the fax server can be integrated with the practice's electronic health record to better manage the flow of patient data, particularly that which originates from a fax.

Whether inbound or outbound, a fax server allows a practice to store, search and retrieve faxes with ease – a benefit if data is misplaced or lost in the event of disaster recovery. By eliminating the need to print hundreds or thousands of pages each day, automating the management of faxes significantly improves the environmental footprint of the practice. The cost savings from the reduction of paper and printing offers a boost to the practice's bottom line.

Don't let this area of your practice remain mired in paper – seek out a solution that is truly paperless.

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
- Addressing 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 ensuring 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

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 comprehensive and effective solutions to protect against computer malware and untimely patch management as well as to solve internal challenges for web monitoring and faxing.

About GFI®

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States, UK, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

More information about GFI can be found at **www.gfi.com**.

GFI 2012 August08

USA, CANADA AND CENTRAL AND SOUTH AMERICA

33 North Garden Ave, Suite 1200, Clearwater, FL USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit **http://www.gfi.com/contactus**