10 Hidden IT Risks That Threaten Your Practice

(Plus 1 Fast Way to Find Them)

Your practice depends on intelligence. But can you count on your technology?

You may not be in the intelligence technology business, but it's probably impossible to imagine your practice without IT. Today, computing technology plays a vital role in the way you serve, work with, and communicate to your patients and clients. Thanks to advances that have made technology more powerful yet less expensive, even the smallest operation can enjoy capabilities – in everything from marketing and sales to delivery and fulfillment – that were once the sole domain of large enterprises.

Have you assigned appropriate access levels and authority to restrict data and applications to the right people?

But today's big IT advantages come with major risks. Your networks and systems serve as your silent partner in operations. Should they fail – and when they do, it's usually without warning – you're exposed not just to an IT problem, but to a potentially large business problem.

This brief paper exposes 10 silent threats that might be quietly undermining your operations now – and proposes one quick, easy and FREE way to bring these threats under control, fast.

Healthcare Briefing Report sponsored by [YOUR COMPANY NAME]

[YOUR COMPANY LOGO]

Risk #10: Wrong keys in wrong hands

It's just common sense: you restrict crucial information, such as bank accounts and inventory access, to carefully designated

employees. Yet many companies have lost control of their network's user level access privileges, exposing vital company data to people without authorization. Patient data is precious: under the audit provisions of the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH), the maximum penalty for breach of HIPAA compliance is up to $1.5 million. One of the first steps toward security is to be sure the right people have the right level of access to appropriate applications and data.

Can you create and review permission reports that tell you which devices and personnel have access to which data and applications?

Risk #9: Bring your own headache

On the one hand, new devices such as smart phones and tablets can increase employee productivity – and when employees use their own devices, save the practice money. But this new "bring your own device" (BYOD) environment brings new headaches, too. These devices are easily lost and stolen. When they are,

any information available to the device – including confidential business and patient data – may be vulnerable to illicit access. Yet fewer than 50% of businesses report the ability to use data encryption and/or remote data wiping to protect their assets. Take stock of your data inventory: you need to share permissions reports that reveal which devices and users have access to which files and applications.

Risk #8: Who's knocking at your backdoor?

Your practice isn't limited to your own systems. Thanks to access to outside servers and systems, you can leverage potent tools like Gmail and Dropbox to manage customer communications, share files and more. While these cloud

services increase your capabilities without busting your IT budget, it's important to remember that every connection that reaches out from your network may open an opportunity for someone else to reach in. Protect your portals: run an external vulnerability scan that reveals every "backdoor" through which an intruder might break into your network.

Risk #7: "Wet paper bag" passwords

Are the connections you use to access online services protected against backdoor invasions by unauthorized intruders?

Your password protections are only as strong as the passwords themselves. Having no passwords – or using obvious passwords such as "12345" – undermines the very protection you seek. Yet employees often fail to establish passwords or, when they do, frequently use ineffective ones. Review your passwords' strength to identify weak spots any unauthorized user could punch through.

Risk #6: Whoa, back up

If you lost a significant chunk of your data right now, how much business would you lose as well? Too many businesses run without sufficient policies, plans and procedures for backing up critical data essential to their ability to operate. If your practice depends on manual procedures that are executed inconsistently, you're exposed to unnecessary losses; it's time to look for automated backup solutions that are always at work – even when employees might be forgetful.

Risk #5: Show me the compliance

Patient data demands special attention. In fact, when you're in the healthcare industry, the law obliges you to preserve client confidentiality – and demonstrate that you have processes in

place to ensure compliance with numerous regulatory standards, including HIPAA, HITECH, Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), and Federal Rules of Civil Procedure (FRCP). The best way to prepare for a regulatory audit is to run regular compliance audits of your own that allow you to take corrective actions before your operation is called into account.

Risk #4: Printing (lost) money

Are your data and applications password protected, and are your employees using sufficiently strong passwords to ensure security?

Despite high hopes for the "paperless" office, the reality is that businesses spend lots of money printing, faxing, copying and scanning paper documents. Consider the math: paper plus toner plus maintenance plus employee time, etc. It's possible to bring these printing costs under control, but the first step is to discover who prints what, how often, and why. By monitoring your multi-function printers, you can limit access to authorized users, discourage unnecessary or wasteful usage, and encourage less-expensive options – such as scan to email or scan to file directories – that save time and money.

Risk #3: "Ghosts" in the machines

There may be "ghosts" haunting your networks – inactive users or inactive computers that remain part of your system, even if they are no longer contributing to your productivity. While the threat may not be immediately obvious, defunct computers represent an expense you don't need to carry. Worse, inactive users may reflect open accounts (perhaps of people who are no longer employed by your practice) that could present security holes for unauthorized access. Run audits that show you what's active or not, then clean house – and close security loopholes –

by burying the “dead” devices and accounts.

Risk #2: When IT can’t keep up, your practice goes down

Smart businesses and wise managers protect their critical networks with redundancy: backup servers and routers that are designed to kick in should the main system go down. But the contingency plan is only as good as the processes and practices behind them; should these be inoperative, your practice will not maintain continuity in an emergency. To safeguard your operations, analyze your network before disaster strikes to be sure that your contingency technologies – such as your backup designated router or alternate domain control – are online and ready for action.

Do you use automated backup programs for data protection, rather than random and irregular manual backups?

Risk #1: Hiding in the dark

You want to run your practice, not an IT department. While IT may not be top of mind, it should never be out of sight. Lack of vision into the true status of your technology, and the quality of your defenses against attack or failure, may leave your practice vulnerable to disruption, legal consequences and loss of revenue. By implementing regular monitoring and review procedures, however, you can anticipate challenges before they become problems, and take adequate measures to ensure the smooth conduct of your practice.

Have you inoculated your practice?

According to a Forrester Consulting report, 89% of healthcare organizations have some percentage of their staff working off-site at least one day a week; more than 10% have experienced

more than one security breach in any given year. Given the ethical demands of patient confidentiality and the legal requirements imposed by numerous regulatory bodies, every healthcare practice needs safe, simple and secure ways to:

- Maintain consistent security policies across ALL devices, including computers, laptops, tablets, smart phones and more – anyplace where data may be exposed
- Remove sensitive data remotely from lost or stolen devices
- Block unauthorized access to data, devices and applications
- Distribute and enforce password protection, encryption and security updates

If the regulators arrived at your door, are you confident you comply with legal and regulatory mandates for your data?

Are you sure your IT is a sure thing?

We all depend on IT. Given the stakes, it's important our confidence is well placed. Are you sure the technology you rely upon is adequately protected? In our experience, **nine out of ten companies have undetected vulnerabilities** that could lead to data disaster.

Take a moment to complete this quick self-analysis. If you cannot answer yes to every question, request our FREE network assessment to give yourself – and your practice – the confidence you deserve.

- Is your system cleared of **ghosts users and computers** that waste resources and expose your network to unauthorized access?
- Can you verify that your **data recovery and network**

restoration plans are operative and ready to work in an emergency?

- Do you have **timely and actionable visibility** into your IT status, so that you can intercept problems before they interrupt your practice?

Give yourself, and your practice, a “yes” vote of confidence by requesting our FREE network assessment, a $1,500 value! Your network assessment will give you insight into the true status of your IT system, and point the way to appropriate corrective actions you can make to secure your practice effectively and efficiently. To get your FREE network assessment, visit [YOUR WEBSITE].

YOUR COMPANY
YOUR CONTACT INFO
YOUR LOGO