10 HIDDEN IT RISKS

You Should Know About

+ 1 Fast Way to Find Them

QUEEN CONSULTING & TECHNOLOGIES

How Information Security Affects Your Business

Over 50% of cyber-breach victims occur at companies with fewer than 100 employees.

More than half go out of business as a result.

It is always a good time to evaluate your IT.

Your business 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 business *without* IT.

Today, computing technology plays a vital role in the way you serve, work with, and communicate to your clients.

Thanks to advances that have made technology more powerful yet less expensive, **even the smallest practice can enjoy capabilities** – in everything from marketing and sales to delivery and fulfillment – that were once the sole domain of large enterprises.

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.

What's Ahead:

Wrong keys in wrong hands

Bring your own headache

Who's knocking at your backdoor?

Weak passwords

Whoa, back up

Show me the compliance

Printing (lost) money

"Ghosts" in the machines

When IT can't keep up, your business goes down

Hiding in the dark

Consider the Massachusetts model

Are you sure your IT is a sure thing?

TIP

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

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 businesses have lost control of their network's user level access privileges, exposing vital company and client data to people without authorization.

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.

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 company 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 practice and client 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.

#9 TIP

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

RISK #8

Who's knocking at your backdoor?

Your business 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 communicate with customers, 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

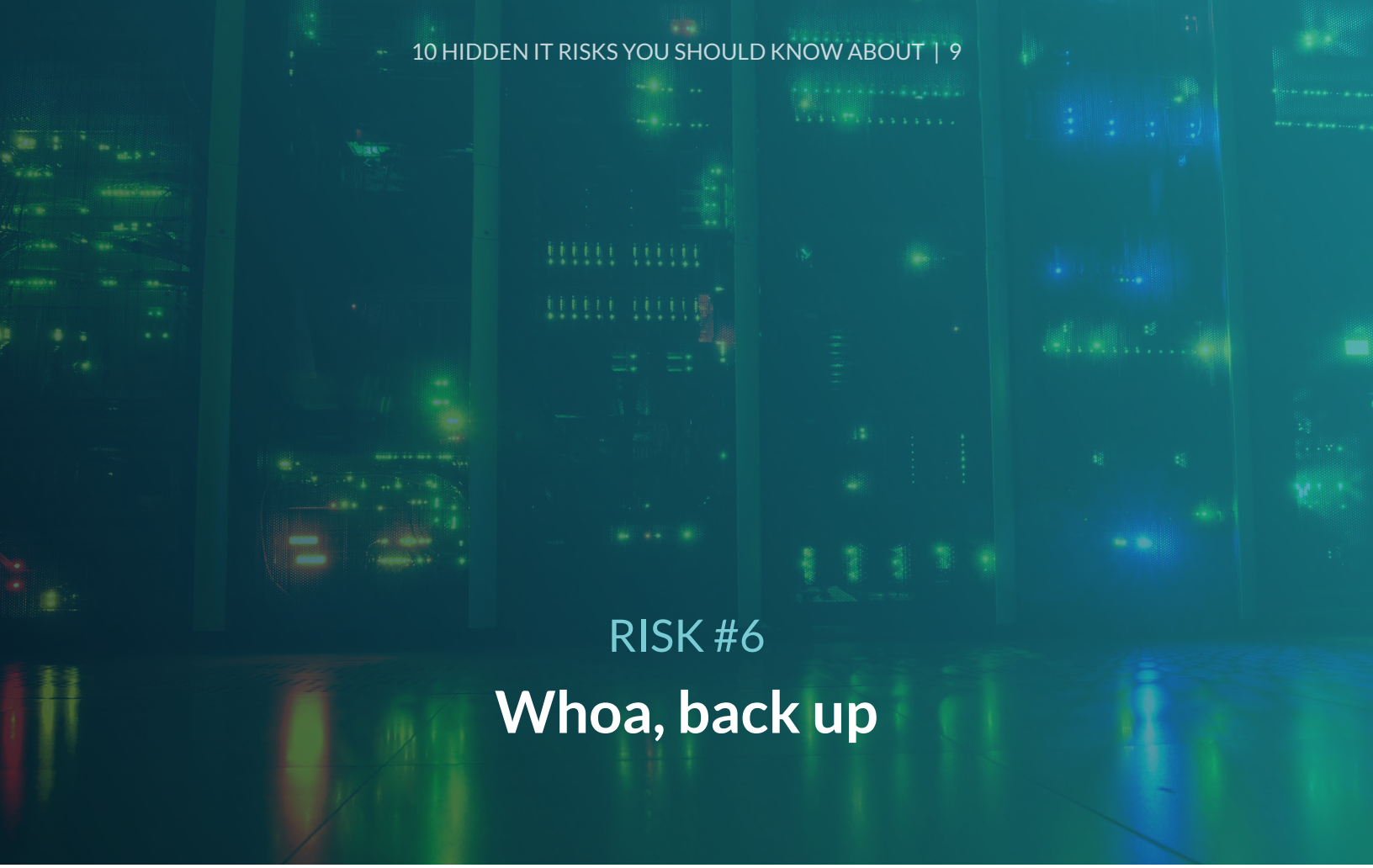
Weak passwords

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

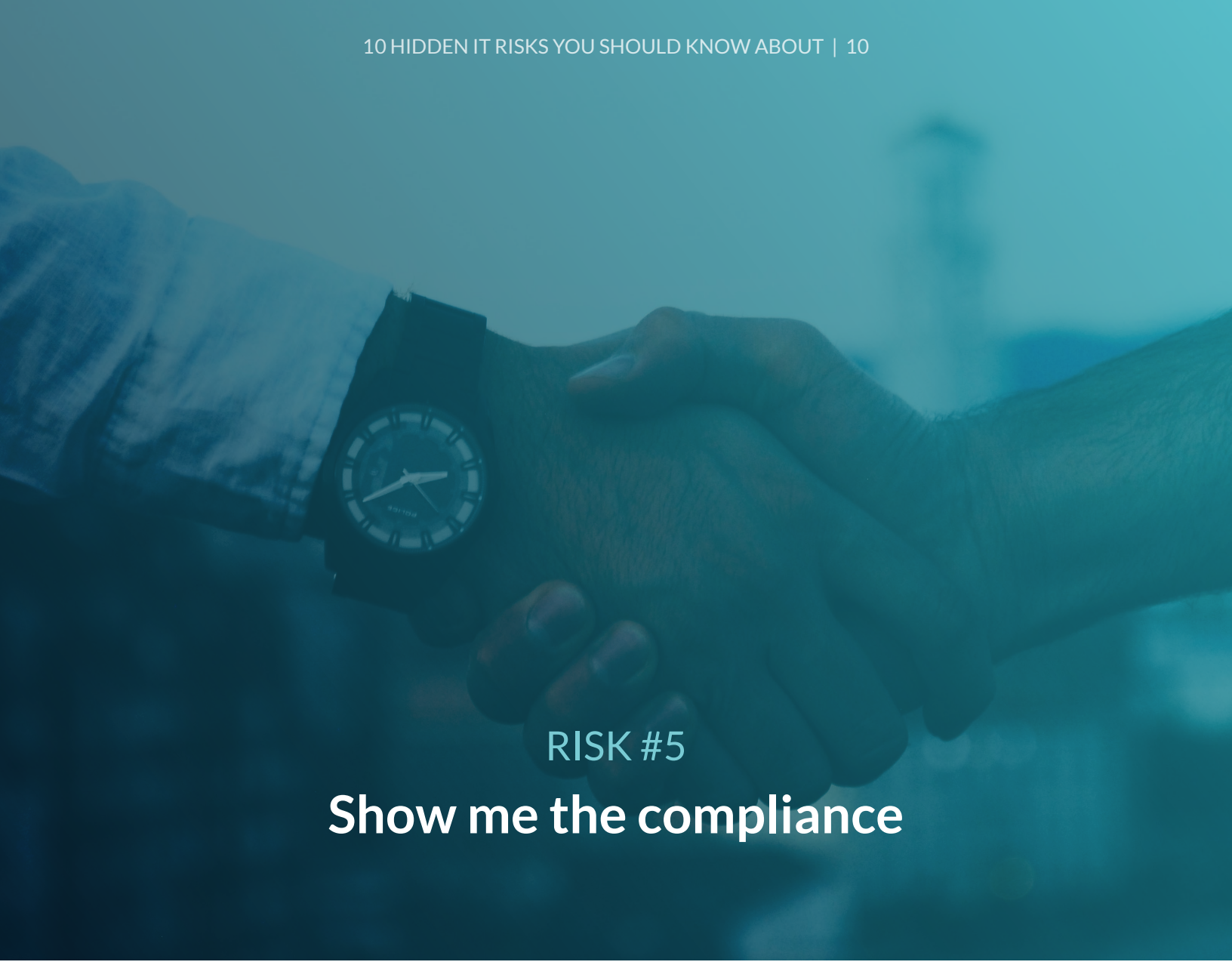
If you lost a significant chunk of your data right now, how much business would you lose as well?

Too many businesses run without sufficient policies, plans and procedures for backing up critical data essential to their ability to operate.

If your business 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.

#6 TIP

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



RISK #5

Show me the compliance

Sensitive data demands special attention.

In many businesses, the law obliges you to preserve client confidentiality – and *demonstrate* that you have processes in place to ensure compliance.

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

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 business) 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.

#3 TIP

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

RISK #2

When IT can't keep up, your business 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 business will not maintain continuity in an emergency.

To safeguard your business, **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.

RISK #1

Hiding in the dark

You want to run your businesses, 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 business 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 firm.

#1 TIP

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

Consider the Massachusetts model

Effective March 1, 2010, Massachusetts law M.G.L. c. 93h imposed the most comprehensive confidentiality requirements yet for the safeguarding of "personal information" such as Social Security numbers, driver's license numbers and other means of individual identification.

Among the requirements are these:

- Encryption of all transmitted records and files containing personal information that will travel across public networks
- Encryption of all data containing personal information to be transmitted wirelessly
- Encryption of all personal information stored on laptops or other portable devices.

To ensure compliance, law firms should consider implementing practices that can:

- Enforce **strong password policies** on all computing devices.
- **Automate backup and restore** functions for all systems.
- Restrict data, devices and applications to **authorized individuals.**
- Deploy **remote lock and wipe capabilities** for all lost and/or stolen devices.

A QUICK SELF ANALYSIS

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 business – the confidence you deserve.

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

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

IT TIP

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

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

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

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

- **COMPLIANCE**
  If the regulators arrived at your door, are you confident you c**omply with legal and regulatory mandates** for your data?

- **CONTROL PAPER**
  Can you monitor and **control printing, faxing, scanning and copying** to lower costs?

- **GHOST USERS**
  Is your system cleared of **ghosts users and computers** that waste resources and expose your network to unauthorized access?

- **RECOVERY & RESTORATION**
  Can you verify that your **data recovery and network restoration** plans are operative and ready to work in an emergency?

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

Give yourself, and your business, a **"yes" vote of confidence** by requesting our FREE network assessment!

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 business effectively and efficiently.

Take advantage of our experience, tools, and support.

Contact us today for your FREE network assessment to see where your security stands.

Visit us online at

www.queencontech.com

A good game and good business both need the same thing: foresight.

Of all the pieces on the board, the Queen is the most versatile and can press the best advantage. She is able to go any distance, in any direction.

Queen Consulting and Technologies is an IT Management and IT Support company, founded on the principles of the Queen piece.

Take the initiative before things break down and get the Queen on your side of the board. Time is money, so never lose time, deals or money again from IT downtime.

Start leveraging today the ease of mind and excellent service you need to thrive.