Untangling Network Security

Protect Your Law Firm's Reputation and Data by Optimizing IT Security

Introduction

Information technology has grown by leaps and bounds ever since its inception. The release of Microsoft's Windows 95 and the arrival of the internet kicked this growth into high gear. IT innovation and development are now continually operating at breakneck speed.

This accelerated development brings law firms tremendous benefits by enabling them to better serve their clients; but it also comes at a price.

Unfortunately, while one group of IT professionals works hard to make technology secure and reliable for end users, another group of equally talented but malicious professionals works hard to wreak havoc in end users' lives by infecting their computer systems with viruses, malware and other computer illnesses.

The continual fight with viruses and other security challenges lowers law firms' productivity and wastes resources. It also undermines brand recognition and can reduce client loyalty.

Before we start on our journey on improving IT security in your firm, we need to take a closer look at what makes law firms financially successful, and how that success depends on technology.

Let us begin by going back to 2003...

David Maister is a leading authority on professional service firms. For his book, *Practice What You Preach: What Managers Must Do to Create a High Achievement Culture,* he conducted an extensive survey on what contributes to professional service firms' profitability. The graph below represents his findings.

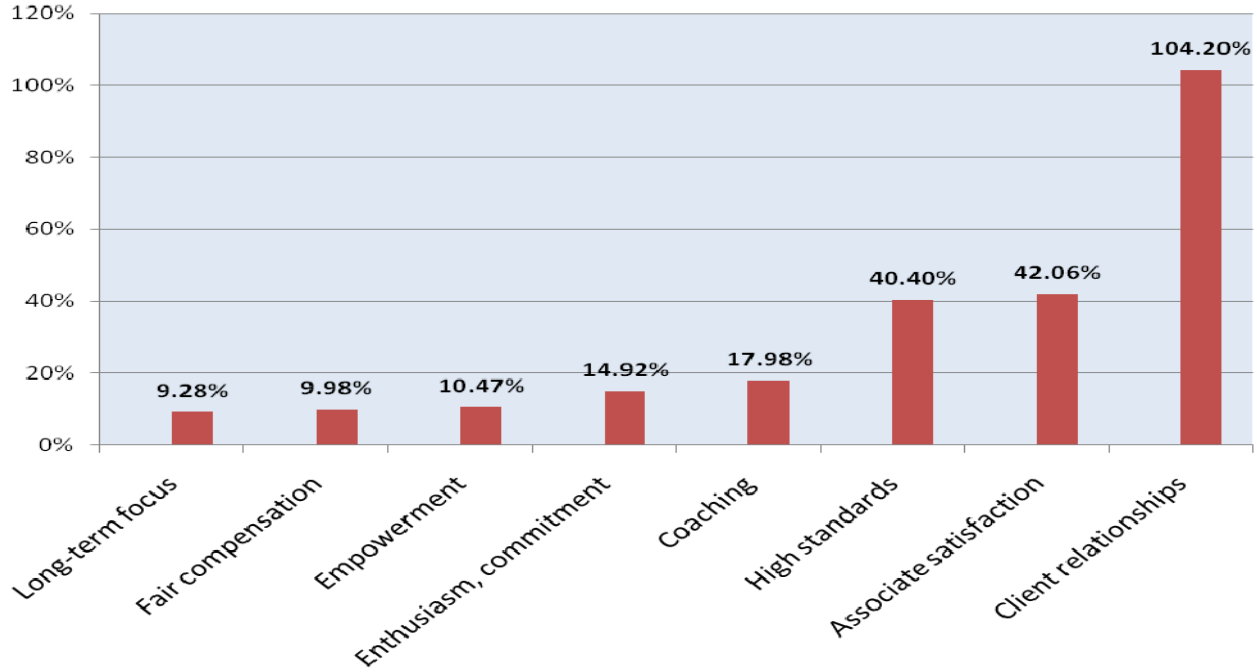

Figure 1: Performance contributors in professional service firms

Despite their general nature several of the categories shown above are technology-related. We can gain perspective by examining how even a small change in any of the eight categories can make a significant difference in the firm's success.

The percentage above each bar indicates the impact that can be made to the overall financial performance of professional service firms.

The method is fairly simple; rate your firm in each of the eight areas on a scale of 1 to 6. Increasing a value point can boost your firm's financial performance by the indicated percentages. For example, if you rate your firm as a '3' at "*High-quality client relationships"* and you are able push it up to '4'; your firm can achieve an as high as **104%** increase in financial performance.

Some may say that things like enthusiasm and commitment are human factors - and they are. However it's difficult to be

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

enthusiastic about serving clients when you are using a virus- or malware-riddled computer that keeps crashing.

Like it or not, the practice of law has become technology-driven. At times IT can be almost invisible but in reality law firms use many aspects of information technology to serve their clients. When technology fails, and it does, the performance and reputation of the firm will suffer.

A critical factor in firm profitability is client loyalty. This is something every law firm dreams of but only a few can achieve.

"Switchers" vs. "Loyals"

Loyals: Respondents who report they are not likely to switch away from their current service provider in the next two years.

Switchers: Respondents who either feel they are likely to stop using current providers and seek new ones, or feel they "might or might not" switch (proof enough that they are open to the possibility).

When buyers were asked about their likelihood to consider switching legal service providers in the next two years, **52%** indicated a tendency towards switching, and **48%** to staying with their current providers.

Although between 2005 and 2010 the rate of Loyals has gone up from **13%** to **48%**, there is still a long way to go to improve client loyalty.

It's also important to note that **71%** of Loyals are "Very Satisfied" with their legal service providers and **21%** are only "Somewhat Satisfied". But **31%** of Switchers are "Very Satisfied", and **46%** are only "Somewhat Satisfied".

This leads us to two frustrations that clients can have with law firms, which are:

1) "They did not listen to me"

2) "They did not respond to my requests in a timely manner"[1]

A high level of trust is one of the most important factors when buyers select law firms. Law firms gain or lose this trust through their communication with potential clients before the engagement and money exchange. At **24%** of clients' opinions, communication is the number one trust-building tool law firms can use to engage buyers.

In today's high-speed world when technology keeps everything alive, buyers crave the high-touch communication more than ever before but often do not receive it.

When asked about some of their main frustrations with their legal services providers, **41%** of buyers responded with "*They did not listen to me*" and **38%** responded with "*They did not respond to my requests in a timely manner*".

Both of these problems can be caused by the condition of the firm's information technology.

The good news is that when law firms clean up their acts, **55%** of the "*they did not listen to me*" and **56%** of "*they did not respond to my requests in a timely manner*" respondents are willing to forgive the firm and do business with them.

This white paper takes you on a guided tour into the rapidly changing land of Internet security and how it affects the profitability of your law firm. By changing habits, practice leaders can improve their firms' productivity by keeping the information technology systems in peak-performing condition.

This white paper was written for established law firms, particularly in Vancouver and Lower Mainland area. It contains several general recommendations, but some points are specific to this geographic location.

As you're read this document, please keep two concepts in mind:

1) Long-term focus

2) Prevention

With those in mind, let us begin.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

Where the Legal Industry Is Headed - In Relation To Information Technology Usage

Software companies are developing and releasing applications more quickly than ever before. This increased quantity of applications is not commensurate with increased quality. This divergence mad rush for new releases provides a fertile ground for those who choose to develop malicious applications to exploit security holes.

Many law firms are operating in constant cost-cutting mode. One critical area where they try to save money is the IT department.

In order to be competitive, some law firms want to hire the best lawyers they can afford. This can lead to decreasing budgets, and firms compromise on the quality of other professionals, such as those in IT.

A Chain of Technical Problems Can Create Business Symptoms

In many cases, the computer errors that show upon your display are actually symptoms of much deeper problems. But in many cases "affordable" IT professionals don't have the expertise to dig deep enough to uncover the root causes.

As we build a case for IT security, we must approach the solution from three angles:

1. The *symptoms* both lawyers and support staff experience on a daily basis.
2. The *effects* these symptoms have on both lawyers and support staff.
3. The business *causes* that drive effects via the experienced symptoms.

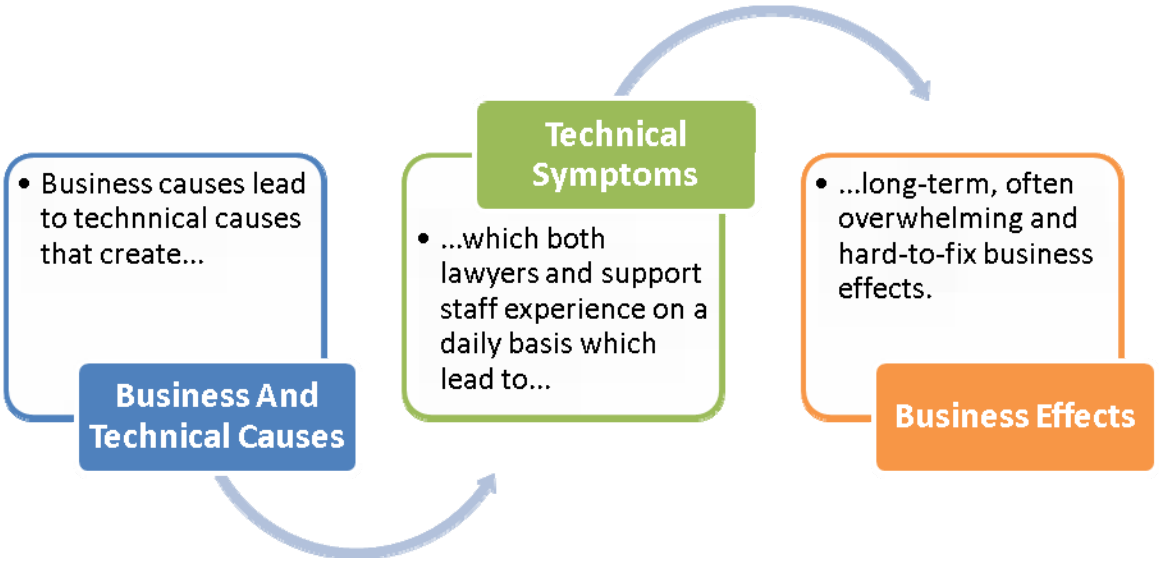

Figure 2: The *cause*, *symptom* and *effect* ripple

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

IT Solutions Vancouver Inc

Business And Technical Causes

Every problem starts with a business decision that can lead to a technical problem:

- A reduction in IT budget leads to...
  - Hiring "affordable" IT staff, which in turn leads to...
    - Poor decisions regarding hardware and software acquisition
    - Poor documentation of IT policies and procedures
    - Less thorough updates of hardware and software
    - Not being fully up-to-date about IT industry developments
  - Purchasing lower-quality hardware and software which leads to...
    - Compromising the overall performance of your IT Infrastructure
      (Even a single piece of low-profile equipment can result in firm-wide problems.)
    - Running your IT system below its true "earning" potential
    - Creating security loopholes in IT infrastructure
  - Reducing or cutting preventive maintenance which leads to...
    - Attacks through web application loopholes[2]
    - Unfettered malicious software distribution[3]
    - Password theft
    - 'Phishing'; criminals stealing information via misinformed users
    - 'Spambots'; your PC becomes a hub of a junk email distribution network
    - Failure to detect viruses

Technical Symptoms

These technical problems then lead to specific technical symptoms:

- Lawyers and staff members experience technical symptoms in their day-to-day work…
  - Computers crash constantly, requiring frequent reboots
  - Computers work more slowly than they should
  - Programs 'step on each other's toes' leading to more crashes

Business Effects

And these technical symptoms lead to specific business effects...

- Hard effects
  - Stressed people - the best may leave the firm, increasing talent replacement costs[4]
  - Even if they don't leave, their work engagement levels drop[5]

---

[2] According to IBM X-Force 2009 Trend and Risk Report, this problem alone represents **49%** of all vulnerabilities. IBM reports that some of the most vulnerable applications are content management systems, like Drupal (2,7%), Joomla! (2,6%), TYPO3 (1,5%) and the now so popular WordPress (0,4%). Furthermore, 86% of third party applications don't have service patches to fend off invaders.

[3] "**75%** of all corporate PCs are infected with some sort of malware." *Putting Trust Back Into Computing: How Enterprises Can Secure Systems and Data* by Brian Berger, in *Enterprise Networks & Servers*, August 2007.

[4] According to Dr. Bradford Smart (http://www.topgrading.com), talent expert and the author of *Topgrading: How Leading Companies Win by Hiring, Coaching, and Keeping the Best People*, the replacement cost of one good employee can be as high as **15 times** the employee's gross annual compensation.

[5] A Gallup Poll study indicates that **59%** of the workforce is disengaged, and **14%** of the workforce is actively disengaged - that is, actively sabotaging their employers' success. And a mere **27%** are engaged. These disengaged employees show up at work like sleepwalkers, trying to get through the day with as little effort as possible.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

- Frustrated employees stay home sick even when not sick, leading to increased medical costs
- Increased production downtime[6]
- Clients can't be effectively served and some of them may leave the firm
- Managers fall behind on their normal work by trying to put out fires

- Soft effects
  - Compromised brand, market, and community reputation
  - Market perceives the leadership team as ineffective or even incompetent
  - News raises red flags in the investor community
  - Losing respected expert status and becoming a mere vendor

Hotbeds of IT Security Problems

A law firm can have the 'best of the best' lawyers, but that firm also needs a secure and reliable technology backbone that makes it possible for top-notch lawyers to deliver a top-notch experience for their clients.

This brings us to some points for consideration in the context of IT security.

Acceptable Computer Use Policy

Many computers are infected with malware applications and viruses when users install software that has not been approved by the company. The users know that they should ask the IT department to install the application, but that takes time. In many cases the application is not work-related, and the users choose install applications themselves.

Unapproved applications may conflict with the official applications that have been deployed firm-wide. The result is that the applications start battling it out on computers that are used for daily work. The computer then becomes both a platform for the application that the operator is using, and a battleground between fighting applications.

What kind of performance can we expect of such a computer? The reality is that this leads to extremely poor performance.

In order to avoid this, law firms should create acceptable computer use policies to stipulate what types of modifications users are, and are not, allowed to make to their computers.

For instance, modifying the viewing panes of Windows Explorer is perfectly acceptable. Installing a third-party program that has not been tested and approved by the company's IT department is not acceptable.

Segmented File Access for Different Users (aka File System Access Control)

People in law firms perform a broad range of work with their computers. This also means that they need different access levels to for different programs. Segmenting access, or trimming access to the minimum required level, can reduce user-introduced problems.

For example: only accounting staff should have access to accounting files and only HR staff should have access to HR documents.

However, firm leaders should be careful not to trim access *too thin* because people may start feeling that they are not trusted. This can lead to a loss of energy and enthusiasm, which in turn leads to lower performing personnel.

Choosing the Right Equipment

There are three primary factors to consider when purchasing equipment:

1) the quality of the equipment,
2) there is reliable and prompt support from the manufacturer
3) that it can be correctly configured by qualified IT staff to suit your specific needs.

[6] According to the 2009 VMware Survey, published in *The Benefits of Virtualization for Small and Medium Businesses*, **62%** of the surveyed businesses lost a significant amount of clients due to downtime caused by accidents, disasters or emergencies. **92%** of respondents say it would take them up to three days to recover applications and data, but if servers are destroyed in a disaster it could take as long as a week or even longer to obtain new hardware and restore all systems.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

Firewalls

A firewall acts as a protective shield for computers. As the name implies, it separates the inside world of a firm (the intranet) from the outside world (the internet). Its purpose is to protect the firm's computers from unauthorized access from the outside world, thus preventing malicious actions. A firewall can be fine-tuned, so that it allows certain kind of access while blocking other kinds of access.

These devices can be hardware or software-based which is important when considering that members of the firm may have to reach their 'inside world' files while working from the 'outside world'. Before deciding whether to use a software firewall or a hardware firewall, consult with an experienced IT professional.

Remote Access for Home and Traveling Users

Even if the firm's computer network is set up and configured correctly, allowing people access to their office computers from their home computers can introduce a broad range of vulnerabilities.

Two of the greatest vulnerabilities are[7]:

1) Accessing the office from an unsecured Internet connection.
2) Accessing the office from a public or unsecured device.

Fortunately there are some fairly simple solutions:

1) Only allow access to the firm through via Virtual Private Network (VPN)[8]
2) Rather than working on the home/hotel computer, access your firm's terminal server[9] via a secure VPN (above).
3) Avoid streaming material directly from the web.
   Instead download the material to the hard disk of your computer and play it from there
4) Install the most up-to-date antivirus software and the latest security patches.

Accessing the Office Network from Mobile Devices

In many cases lawyers and support staff can use their mobile devices to access their office computers. This also increases the probability of security breaches.

The most common security threat from mobile devices is when they are lost or stolen. Unfortunately due to their small size mobile devices can easily be lost or stolen. According to the IDC market research firm, computer manufacturers have reported that **2,000** Mobile devices are stolen worldwide on a daily basis.

Most users use handheld devices to access company emails and open attachments, and when those devices get lost or stolen, thieves will have access to sensitive, potential confidential information. One small measure of protection is to password protect every device.

Currently the most secure handheld device is a BlackBerry that is connected to a BlackBerry Enterprise Server (aka BES). If such a device is lost or stolen, the device can be 'wiped' and it can be disabled remotely from the BES.

Although they are extremely convenient and easy to use, USB memory sticks they are also easy to lose. Their security varies from model to model. Most cheap USB memory sticks are 100% unprotected, while others provide some security in the form of software or hardware encryption.

User Education and Training

The business world seems to be split over user IT education. Many people think it's a luxury; while others think it's vital for everyone to have a rudimentary understanding of IT security.

A basic level of knowledge is necessary to make sure that lawyers and staff members do not cause inadvertent harm to their

[7] *Hidden Dangers in the Mobile Worker Jungle* by Blue Coat, leader in Application Delivery Networks (ADN)

[8] A virtual private network (VPN) is a computer network that uses a public telecommunication infrastructure, like the Internet , to provide remote offices or individual users with secure access to their firms' networks.

[9] A terminal server is a hardware device that connects terminals (PCs, printers, and other devices) with a common connection point to a local or wide area network (LAN or WAN).

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

computers. For instance, one of the main causes of malicious software infection is that people blindly click on links contained in email messages from seemingly reliable sources. And that simple click can initiate an avalanche of nasty events.

Another benefit of IT education is that users will develop a respect for technology, and apply that respect as their use of computer equipment.

As mentioned previously, information technology continues to advance at a rapid rate, and it is to everyone's benefit to learn the basics. Education will not fully eliminate computer or security problems, but it will certainly reduce the magnitude of the issue. Also, good user education is preventive medicine, and simple preventive action is a lot cheaper than remedial action. It is also important to develop a "preventive mindset", which will help people to take the right action when facing potential security incidents.

Systems Problem Track: Reducing or Cutting Preventive Maintenance

The method by which a law firm chooses to maintain its IT equipment can make a significant impact on the maintenance budget.

Many law firms choose the "Run to Failure" (RTF) approach. This means using IT equipment until something breaks down and requires a break-fix service. This stems from the "If it ain't broke, don't fix it!" mentality which has sadly become the norm.

The potential damage of the Y2K issue should have reminded everyone that when IT systems are neglected, they can cause serious problems. Fortunately, the fear stemming from Y2K issue was so great that most companies took *some* action, with the net result being that most of the predicted disasters didn't occur.

Apart from the Y2K issue, something sinister is going on in the background. That something is continually accelerating changes in every area of information technology. Unfortunately, unlike the Y2K problem, most law firms are not prepared to adopt or embrace this rapid change in technology.

So, How Can You Be Ready?

Just as law can be practised either in a proactive, "How do I prevent this lawsuit?" or reactive, "See you in court!" way, so can technology.

Many law firms choose to eliminate preventive maintenance altogether and focus on the "Run To Failure" method. This is because they believe proper prevention is too costly and also because they perceive it as too much of an interruption in their daily operations. The ironic part of this is that lawyers will often chastise their clients by saying:

"You know, you could have prevented this."

A joint Rotman-TELUS study[10] on Canadian IT security practices show major differences in the average annual losses organizations suffer, depending on whether they are public companies, private companies, or part of the public sector. The study focused on a one-year period between 2008 and 2009.

> IT security breaches at Canadian firms with over 100 employees increased by 97%. The average number of breaches also rose by 276%: from 3 per company in 2008 to 11.3 per company in 2009. In private companies, the cost of security breaches increased by 174% over that same period.
>
> The storage of sensitive information makes government offices the number one target for attacks, but some private sector industries are also desirable. Law firms belong in this sector.
>
> The authors of the study point out that the overall economic situation plays a major role in how safely companies handle data. Specifically, during lean times, budgets get cut and many law firms replace preventive measures with the old "Run to Failure" (RTF) approach.
>
> Some good news is that the appearance of increased security breaches is partially due to the fact that more attempts are recognized and reported as breaches.
>
> While firms can do their best to protect themselves against breaches from the outside; inside breaches is the fastest-rising category. Unauthorized access to information by employees increased by 112%. Proprietary information theft increased by 75%, and the theft of mobile devices increased by 58%.

Three major impacts to of security breaches are:

[10] Ibid.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

1. Damage to the firm's brand and reputation.
2. Lost productivity due to disruption
3. Lost clients.

To this list we can also add what Warren Buffett called "The biggest cost of all": *Opportunity cost*.

There are five major concerns that incite Canadian law firms to implement *prevention-based* security programs.

1. A disclosure or loss of confidential data.
2. Compliance with Canadian regulations and legislation.
3. Securing business continuity and disaster recovery.
4. A loss of strategic corporate information.
5. Compliance with firm-wide security policies.

One of the major problems in enacting preventative security is that many law firm partners don't fully understand the implications of security threats. Therefore they struggle with changing their perception to regard IT security as a competitive advantage. It is imperative that law firms view IT security in one of these two ways:

1. To comply with government regulations or professional standards.
2. To demonstrate to their clients that the firm takes lawyer-client confidentiality very seriously.

Another problem is that many IT solutions and IT solutions providers originate from or are based the USA. Despite being our neighbour, the IT threat can manifest itself in slightly different forms. It's unwise to think that just because something is a perfect solution in the USA that it will be the perfect solution in Canada.

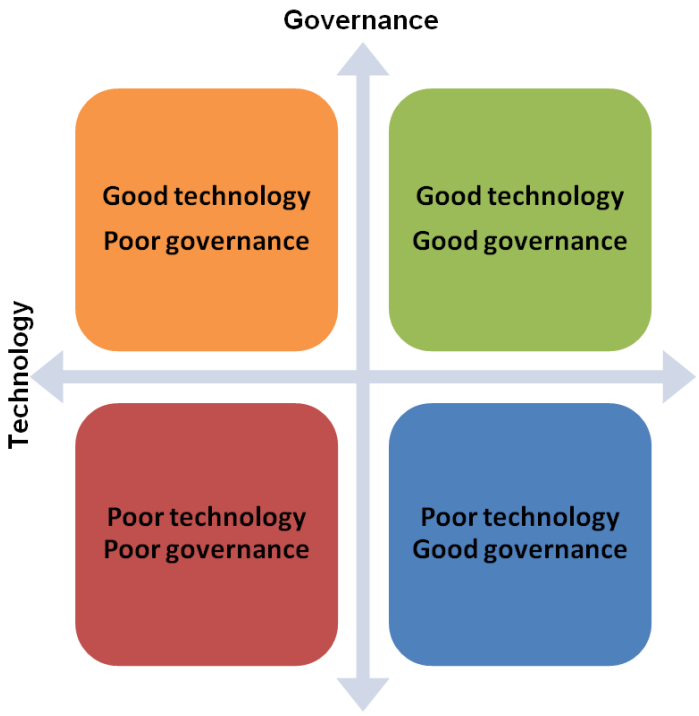

Figure 3: The effects of governance and technology

Dr. Hejazi, one of the authors of the Rotman-TELUS study, calls this calls this negligence of geographic location "A strategic error".

Canada has a different government, public healthcare and banking system from the US, thus the exchange and flow of information is drastically different.

Sadly, the average security spend is only 7% of the total IT budget. Merely spending more is not the solution, investing the right amount in the right solution can significantly reduce the probability of breaches.

The other aspect of law firm security is firm-wide governance. It is important to set up metrics at a partner level and monitor them on an ongoing basis. While IT staff will perform the monitoring, partners must be involved in the analysis of the results and initiate the appropriate action to improve upon those metrics.

The ideal situation is *good technology coupled with good governance*.

Poor technology and poor governance: These are typically overly cost-conscious firms that don't see the value of investing in good IT equipment and probably also don't spend much money on their IT staff.

Nobody is happy, and there is high staff turnover: A typical case of being reactive rather than proactive. As a result, these firms suffer from the maximum security exposure.

Poor technology and good governance: Similar to the above case, but these firms would probably pay for good IT administrators but expect them to keep their outdated equipment running.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

Again, the IT administrator can only be reactive because with outdated equipment - it's hard to be proactive. This firm will have a high turnover of IT staff

Good technology and poor governance: In this case there is usually one of two problems:

1. The firm realizes the importance of purchasing quality IT equipment but is now skimping in hiring an administrator who knows how to configure it. The equipment is not used to its full potential, which can leave security holes and decrease productivity because users are not able to utilize the technology available.

2. The firm realizes the importance of purchasing first-class IT equipment and hiring a good network administrator, but the company policies prevent the administrator from configuring the equipment the way that it is supposed to be configured.

Another case is where users are blocked from accessing certain websites because they are flagged as suspect or dangerous but partners ask administrators to remove this restriction in the firm's policy so that users can freely browse their favourite Britney Spears or even porn sites, which most probably contain viruses or malware.

Good technology and good governance: Maximum security protection. Good equipment, good IT staff, firm IT policies. Everybody is happy!!

A Few Thoughts on Passwords

For security reasons it is recommended that users change their password every 60-90 days and the password should be at least eight (8) characters long. In many cases, this policy is considered an inconvenience and partners order the network administrators to remove the password change requirement and reduce the minimum password length to *as little as three or four characters*. Short passwords make programs and data virtually unprotected from hackers with even the most basic knowledge.[11] The challenge for people trying to break passwords is the "keyspace", which is the total number of possibilities for a password based on the number of characters it uses. Expressed mathematically, this is the number of possible characters you can use - to the power of the length of the password.

Keyspace = [Complexity]$^{(\text{Password Length})}$

- *Keyspace* is the password's overall strength.
- *Complexity* is the number of keys used on the keyboard.

  This can be **26** (single-case alphabetical), **52** (upper & lower case alphabetical) or **94** (upper & lower case alphabetical and punctuation)

The chart below highlights the fact that a password's length has a bigger impact on its strength than complexity.

Technically speaking, a 16-character password that uses all 94 character and punctuation keys is **81,311,554,837,475,300,000,000,000** times as strong as a 4-character password that uses only 26 character keys.

For example: the password **R2MyNameIs:C3P0!** is 8.1×10^{25} times stronger than **fish**.

Considering the level of increased security for your data, is it not worth overcoming your reluctance to type in a slightly longer password?

[11] *Password Size Does Matter: Length Is More Important Than Complexity When It Comes To Secure Passwords - And Here's A $100 Wager To Prove It* by Roger A. Grimes of InfoWorld: http://www.infoworld.com/d/security-central/password-size-does-matter-531

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

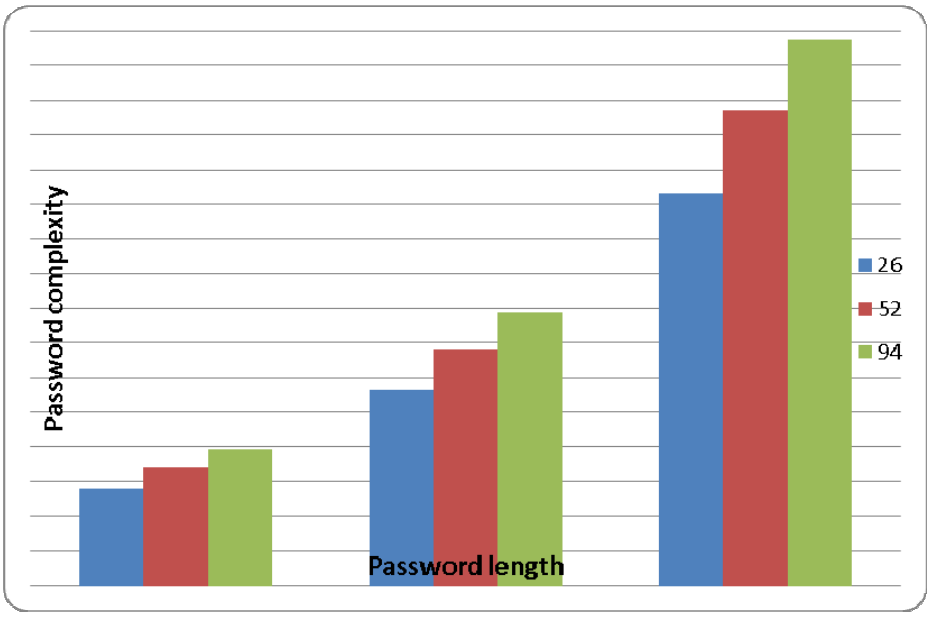

Figure 4: The difference in password strength

As shown above, if you keep the password length the same but you change the password's complexity, the overall password strength doesn't change much. Therefore, it's not complexity (the number of characters used) but the length of the password that makes the password a strong repellent for hackers.

A person who refuses to type in a few extra characters reduces the all of the firm's password effectiveness and undermines the firm's operations. When people are aware of the sensitivity of the information that they store on their computer systems, they should listen to their network administrators and happily choose to type in long passwords for their own protection.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

Conclusion

We are living in an age of tremendous technical advancements - but this comes at the price of commoditisation. Some people try to buy everything on price, like sacks of potatoes. An increase in the number of providers causes further commoditisation.

Law firms can have a very rough time distinguishing between IT service providers but when thinking of value delivered to clients, the partners have to realize that today's IT service providers need to think beyond merely "improving technology".

Actually, law firm partners have to think at three levels[12] to find valuable IT service providers such as those who offer Leadership, Relationship and Creativity wrapped around their core services.

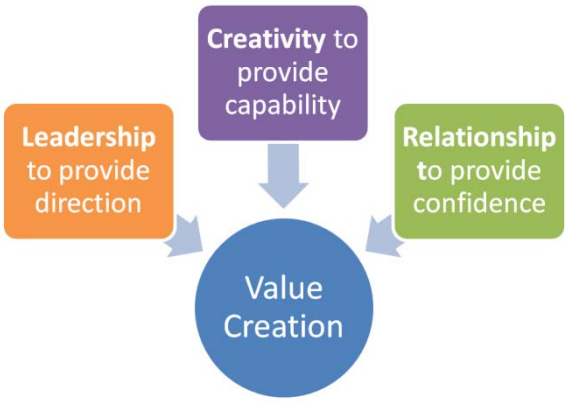

Figure 5: Performance contributors in Law firms

Leadership provides direction in a complex world. People need clarity as to where to go, but the world's complexity can cloud their visions and they lose sight of their goals. And when they lose sight of their goals they feel paralysed to move forward.

Relationship provides confidence by offering unique support above and beyond simple business transactions. This relationship increases clients' confidence to do what they need to do to achieve their goals. This is where mutual trust, respect and candour play significant roles.

Creativity provides capability. IT service providers' creativity in technology must provide new business capabilities for law firms. Instead of offering better technology for technology's sake, IT companies must offer technologies that represent business advantages to their clients.

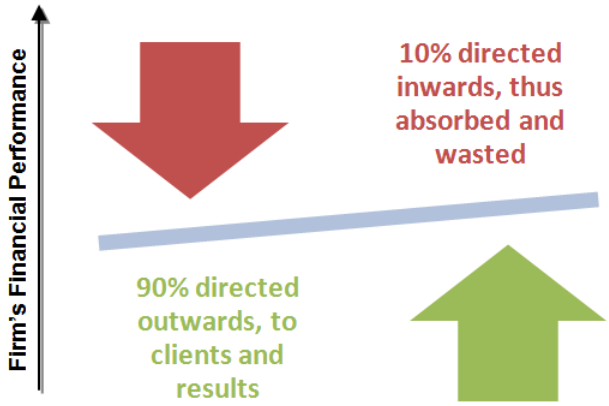

Figure 6: "Energy" inflows and outflows

After looking at what IT companies have to deliver in order to provide distinctive value to law firms, we have to look at how law firms have to integrate these new values into their operations and achieve the technically healthy law firm.[13]

In your firm, you have 100% of your people's attention, creativity, energy, enthusiasm and inspiration - basically the revenue-generating attributes. Out of this 100%, a certain percentage flows inwards and is wasted on non-essential activities like remedial servicing of your IT system.

The problem is that every percentage that flows inwards towards trivial activities cannot flow outwards towards crucial activities such as client acquisition, service delivery and deepening existing relationships - i.e. the activities that lead to new revenue, brand value and overall industry leadership.

Operating an IT system in reactive mode, using remedial action when something breaks down, is definitely inflowing energy, much of which is wasted because a little foresight could have prevented serious and costly problems.

61.1% of small- and medium-sized businesses, including law firms, regard "security enhancements" as one of their main IT

[12] Concept adapted from the works of Dan Sullivan, The Strategic Coach

[13] Adapted from *Million Dollar Consulting: The Professional's Guide to Growing a Practice* by Alan Weiss

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

initiatives for 2010, supporting the three main strategic initiatives:

1) Retaining key employees (81%), **2)** Controlling costs (81%) and **3)** Finding new clients (79%).

And while well-maintained IT systems cannot single-handedly guarantee the success of these initiatives, neglected IT systems can single-handedly destroy them by exposing law firms to the predators of cyberspace.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com

About Solid IT Solutions Inc.

About Solid IT Solutions – www.SolidITSolutions.com

Solid IT Solutions is a Vancouver-based information technology consultancy firm. As an information technology expert Heinz Deubler, founder of Solid IT Solutions, has been working with law firms, helping them to keep their operation effective, choose and install the right hardware and software for the job, perform proactive maintenance in order to keep costs down and help increase productivity by keeping downtime to a minimum.

Unique

Solid IT Solutions' uniqueness doesn't come from fancy downtown offices and, glitzy advertising campaigns and snazzy vehicles.

It's uniqueness comes from what's inside it's people's heads, between their ears and their passion for finding smart solutions to IT challenges.

A true professional knowledge firm.

Independent

Ever since its inception, Solid IT Solutions has formed and nurtured partnerships with meticulously handpicked equipment and software developers to access the best solutions for its clients. Yet, Solid IT is independent, serving, first and foremost, its clients not it's suppliers.

The final solution is always driven by clients' needs and budget. While technology is our tool, ultimately Solid IT Solutions is in the client service business, providing business solutions using technology.

Solid IT is proud of its people's ability to speak plain English which makes them welcome guests both in the boardrooms and server rooms of its clients.

Responsive

You won't find a more responsive team of qualified IT professionals who are passionate about finding smart solutions to your IT challenges.

You rely on your computers, network, and IT infrastructure to keep your business running, and to stay connected to your customers and your data.

We understand that, and work to return all client calls within two hours, and be on site in emergencies within four hours.

Qualified

Solid IT Solutions' people have multiple certifications from leading organisations like Microsoft, Cisco and Novell.

300-422 Richards Street, Vancouver BC, V6B2Z4 - Phone: 604-288-4109 - info@SolidITSolutions.com