LAWTECH

The Law Technology Magazine

Issue 4 | August 2015

Win an iPad

see page 15 for details...

Insights from Law + Tech experts

Are smartphones a business threat?

Disaster avoidance for free

Improve your client relationships

LexisNexis®

REGULARS

BETTERBUSINESS

CASESTUDY

ITSYSTEMS

LEGALTECHNOLOGY

OPINION

ARJUNMEDIA

MD/Publisher: Partha Goswami
partha@lawtechmagazine.com
Editor: David Tebbutt
david@lawtechmagazine.com
Design: Dominic Kershaw
dominic@lawtechmagazine.com

The views expressed in the articles and technical papers are those of the authors and are not endorsed by the publishers.

The author and publisher, and its officers and employees, do not accept any liability for any errors that may have occurred, or for any reliance on their contents.

All trademarks and brand names are respected within our publication. However, the publishers accept no responsibility for any inadvertent misuse that may occur.

ISSN 2055-6608

Printed by Buxton Press Limited,
Palace Road, Buxton, Derbyshire
SK17 6AE

Arjun Media
26 St Thomas Place,
Cambridge Business Park,
Ely,
Cambridgeshire
CB7 4EX
Tel: 01353-644-056

Our contributors

Once again, our contributors have worked hard to deliver interesting and lively copy with barely a sales pitch in sight. The vendor contributors are, of course, writing for Lawtech largely to show off their knowledge and professionalism in the hope that they'll get on your radar and, maybe one day, you'll take a serious look at their websites. The law firm employees will have mixed motivations. Maybe it's for the sheer pleasure of sharing their insights. Or it might be to put themselves 'out there' and increase their visibility among their peers in the legal profession.

The magazine and website

It would be impossible to make every article interesting to every reader but we hope you find LawTech interesting enough to make you want to continue reading it. Don't forget we also have a website which carries, on average, two interesting news stories a week. Sometimes we comment but, mostly, we leave the interpretation to you.

This is similar to the way we create each magazine. We often provide articles on the same subject but taken from different perspectives. This month you'll find we've done three 'disaster' articles that range from avoidance to recovery. We also have a few points of view on Bring Your Own Device (BYOD). One of them, although written by one person, takes two points of view in an imagined email conversation between the practice head and a long-standing employee.

Win yourself an iPad mini 2

You may be interested to note that we're giving away an iPad mini 2 to print magazine subscribers who are willing to spare a few minutes to tell us what they think of LawTech magazine - good or bad, it doesn't affect your chances of winning. It also asks if you'd like to write for us. We love case studies and insights from knowledgeable people in law firms. We'll give you as much help as you need to make your story shine.

Why not hop over to **page 15** to learn how you might win that iPad and, maybe, become one of our writers?

David Tebbutt
Editor – LawTech magazine

Our pick of the LawTech website's news stories since the last issue

Will 3D visual aids come to UK courtrooms?

A Canadian company, Courtroom 3D Evidence (C3DE), wondered if our readers would be interested in its service. Our answer is, "Yes, but probably not how you'd hoped." It seems unlikely that many, if any, LawTech readers would seek a consulting service from Canada. On the other hand, it is breaking new ground with its 3D printed evidence for use in the courtroom.

A former poverty law lawyer, Natalka Falcomer (pictured), frequently witnessed the failure for lawyers and 'experts' to clearly convey their arguments or the facts of their case to the judge or jury. 3D visual aids, according to C3DE, "play a critical role in removing ambiguity and ensuring that juries and judges make decisions based on 'fact' and not 'gut'."

In criminal or negligence cases, these could be 3D replicas of wounds, for example. This is a step forward from conventional visual aids which are, themselves, already better at conveying information than the written or spoken word.

Could this be an opportunity for a UK legal technology consultancy?

www.c3de.net

Goodbye Ogden tables

Anyone involved in personal injury and fatal accident cases will be familiar with the 'Ogden' tables which help calculate the lump sum compensation due. What they may not know about is piCalculator from Rebmark Legal Solutions which saves shedloads of work for clinical negligence and personal injury lawyers and delivers the most complete and accurate schedule of loss. It's in our news because Eclipse has just announced its integration with Proclaim.

According to Rebmark, "You enter detailed information about your client, we do the rest, calculating interest and multipliers. No more Ogden Tables. No more maths." And you can keep updating the information from the first meeting with the client to the court appearance.

The working documents are securely stored and continuously backed-up in an ISO 27001 data centre, accessed through the cloud by encrypted communications with authorised users. The system outputs a Word document which can be saved to your case management system. You can also customise it with your firm's styles.

www.picalculator.co.uk
www.eclipselegal.co.uk

Encryption: Letter to President Obama

We all know how important it is to keep our secrets secret through encryption. Governments would prefer some kind of 'back door' access to encrypted communications and documents. Here's a letter from two prominent hi-tech industry groups to President Obama and other leading members of his administration on June 8. The outcome of the US deliberations will have world-wide repercussions, not least on us in the UK. The letter states the case clearly, so no further comment from LawTech is needed:

Dear President Obama,

The undersigned associations, representing a wide range of companies in the technology sector, write in connection with encryption technologies that companies incorporate into their products and services. This correspondence is intended to provide clarity on our position and to help develop a framework for further dialogue. We also take this opportunity to point out the global implications of certain policy measures relating to encryption.

We are opposed to any policy actions or measures that would undermine encryption as an available and effective tool. As you know, encryption helps to secure many aspects of our daily lives. Encryption is an essential asset of the global digital infrastructure, enabling security and confidentiality for transactions as well as assurances to individuals that their communications are private and information is protected. For example, the rapid growth in online commerce would not have happened but for consumers' trust that their payment information is secure. Consumer trust in digital products and services is an essential component enabling continued economic growth of the online marketplace.

Accordingly, we urge you not to pursue any policy or proposal that would require or encourage companies to weaken these technologies, including the weakening of encryption or creating encryption "work-arounds." We appreciate that, where appropriate, law enforcement has the legitimate need for certain information to combat crime and threats. However, mandating the weakening of encryption or encryption "work-arounds" is not the way to address this need. Doing so would compromise the security of ICT products and services, rendering them more vulnerable to attacks and would erode consumers' trust in the products and services they rely on for protecting their information.

In addition to these security and trust concerns, the U.S. policy position on encryption will send a signal to the rest of the world. Should the U.S. government require companies to weaken encryption technology, such requirements will legitimize similar efforts by foreign governments. This would threaten the global marketplace as well as deprive individuals of certain liberties.

We are committed to finding pathways forward that preserve security, privacy, and innovation. We know the issue at hand is extremely complex, with implications both domestically and internationally. We hope that by being clear in defining the nature of the problem and our position we can contribute to the current dialogue. We look forward to continuing this discussion with your administration.

Sincerely,

Information Technology Industry Council
www.itic.org
Software & Information Industry Association www.siia.net

2015
GLOBAL THREAT
INTELLIGENCE
REPORT

Are security threats exaggerated?

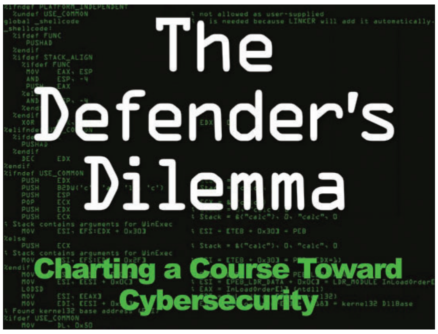
We hear all the time about the valuable information held by law firms and the attractive amounts of money being transferred between them. It stands to reason that law firms must, therefore, be prime targets for cybercriminals. But, do you know what? According to NTT's Global Threat Intelligence Resource Centre, you're by no means a prime target. At least, you weren't in 2014.

Breaking out the UK figures from the six billion malware-specific attacks in 2014 that the research analysed, law firms will be hit by just seven in every hundred thousand attacks in the UK. That's 0.007 percent. Public sector is far more likely to be hit, at 39 percent or insurance at 13 percent.

With regard to types of attack, SQL injection is twice as likely to happen in the UK or Norway than anywhere else in the world. The world average is 26 percent, the UK is 60 percent and Norway 58. By comparison, the US and Sweden were 19 per cent, France and Germany 12 per cent, and the Netherlands 10 per cent. Make of that what you will.

Does 0.007 percent mean you don't have to worry? Probably not. It will be a growing figure. But perhaps it's okay to be slightly less worried today than you were yesterday. But even one breach is enough to set you on the road to disaster.

www.nttcomsecurity.com


The Defender's Dilemma
Charting a Course Toward Cybersecurity

Cyberbreaches: disclose or not?

We fear that 'cybersecurity' and 'LawTech' are the modern equivalents of 'wolf' and 'Peter'. It's easy to glaze over and say, "There they go again." And, if you're a smallish firm with limited resources, who can blame you? After all, serious detection and countermeasures are probably beyond your budget and needs. Note the word, 'probably'. What if you're digitally connected to other, larger and better protected, organisations? Might you not be a tempting entry point for an attacker? All it would take is a stupid click on a dodgy link in an email or the insertion of a thumbdrive you found by your car. It may be that staff education is all you can afford, on top of the usual antivirus/antimalware protections, but it would be a heck of a lot better than nothing at all.

The RAND Corporation has just published a report called *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. I won't entirely spoil the punchline of this 162-page document Trey Ford takes a refreshing point of view which we think is worth sharing. He's a Global Security Strategist at Rapid7, a security data and analytics software and services company. He notes that Chief Information Security Officers (CISOs) are, "tasked with protecting brand loyalty." While this might sound like, "cover up", Ford actually believes the opposite is true. He says that, "The trust of partners and customers is built over time, but can be lost in a moment. The CISO preserves that trust by working in concert with IT, Operations, Legal, PR, and Marketing." That takes care of the internals, but then it's what happens next that matters.

He says, "Breach response and disclosure can go in one of two very different directions - losing face, or investing in relationships. I believe a meaningful, coordinated, and honest response to a breach is an investment in corporate partnerships and customer relationships." adding, "Transparency, thorough follow-up, and deliberate communication will forge meaningful brand loyalty in the long run."

With regard to the upcoming mandatory breach disclosure, he says, "Customers, stockholders, and partners do not expect perfection - they expect an honest partner working hard to preserve their trust. I think mandatory breach disclosure could help preserve the public trust and be a key step in maturing the cybersecurity profession."

www.rand.org
www.rapid7.com

Bundle, annotate and share disparate documents

Document Workspace lets you assemble 'workspaces' from all manner of existing documents, even if you don't have the original software.

You can combine edit and annotate documents from over a hundred different formats. It keeps a connection to your source documents such as web pages, images, text files, spreadsheets and presentations. This helps you check for updates and reminds you of its provenance. You can share and publish your workspace in a variety of popular formats.

The company behind Document Workspace is Global Graphics Software whose other software is used to print more than 80 percent of the world's newspapers.

You can download a 15-day free trial of Document Workspace for Windows 7 or 8. After that, it costs $49.95 or the local equivalent.

www.gdocinspired.com/products/document-workspace

LAW FIRM EXPLOITS SOCIAL MEDIA

How social media transformed Pini Franco's reach

By Claire Trévien, Social Media and Marketing Manager at Passle

Pini Franco LLP is a boutique full service law firm that serves UK and European clients. Although based in the City, its ethos is to provide specialist legal expertise without the extra cost or pretentiousness often associated with such firms.

Previously, Pini Franco's marketing comprised a quarterly e-newsletter of four articles. This took a lot of time and energy from the small firm, which didn't have a marketing team to facilitate this. It sent the newsletter to its client base without using a dedicated provider such as MailChimp, so it received no statistics to monitor the success of this tactic.

Only one of the firm's partners had a Twitter account, which he used irregularly, while the firm itself had no presence on Linkedin. It's safe to say that, prior to the creation of a dedicated marketing resource in November 2014, Pini Franco found it difficult to have a strong online presence.

The social push

The principal objectives of the social push were to Increase the online presence of the firm, to showcase its expertise on legal issues, to compete with the bigger firms and to get meaningful feedback.

In the first four months after signing up with Passle, Pini Franco created 199 posts to demonstrate its knowledge and expertise. That's ten times what it used to manage in a whole year with its newsletter.

Passle's research into the top 200 UK law firms showed that the average lawyer creates just 0.51 knowledge pieces per year. Pini Franco, with its team of six partners, has created 33 knowledge pieces per lawyer in four months. If it continues at this rate, it will create 99 knowledge pieces per lawyer per year!

Domenic Pini, Partner at Pini Franco, explains, "Social media was kept under lock and key, Passle was the key to getting content out." Using Passle has encouraged the firm to explore social media; it now has a Linkedin company page while the named partners regularly use Twitter.

How Pini Franco has met its objectives

1. It has increased the online presence of the firm. By creating 199 knowledge pieces on Passle and sharing them widely on social media, Pini Franco has substantially increased its online presence. Its posts have attracted over 6000 views since starting, thanks to their publication on the website.

2. It has showcased the firm's expertise on legal issues. One of its most popular posts was Domenic Pini's Je Suis Charlie and the Public Order Act 1986. This post demonstrated exactly how the Pini Franco team has been able to showcase their expertise while still being able to focus on their day jobs.

In this particular piece, Domenic Pini quoted an article from Reuters on the Charlie Hebdo attacks in Paris. The Reuters article talks about the importance of freedom of speech but Domenic explains that, had the satirical newspaper printed the images in the UK, it would have been illegal under Section 4A of The Criminal Justice and Order Act. This is not something a non-expert would know and it gives a new spin on a news piece.

This post is not content for content's sake. It is characteristic of Pini Franco's output; each of its experts regularly comments on the news, providing relevant, timely, and innovative knowledge pieces suitable for their target audience.

3. Pini Franco is able to compete with the bigger firms. If this boutique firm – without the additional resources of big firms – continues at the same rate, it will create more knowledge pieces than all but 11 of the UK's top 200 law firms. When you break down how many knowledge pieces per lawyer Pini Franco has created to date, it would already easily rank first in the top 200 UK law firms.

4. The firm now gets feedback. By using Twitter, Linkedin and Passle, Pini Franco has access to statistics it didn't have previously. Passle gives it a day-to-day breakdown of statistics, both for the individual and the company, which allows it to see which posts proved most popular and adapt its approach accordingly.

Quite apart from the hard objectives mentioned above, Pini Franco has been able to show its knowledge of social media. Previously, its online presence really suffered through lack of resources. Now, with all this content, it has something relevant to share with its communities through social channels, such as Twitter and Linkedin, all of which have helped build its online presence.

The knowledge pieces provide a key way for a law firm to establish itself as a powerhouse of thought leadership.

By increasing the number of these pieces it produces, Pini Franco has opened itself to more business opportunities and generated more traffic to its website.

Conclusion

Using Passle has not only demonstrated Pini Franco's knowledge but it has also allowed it to get into the habit of reacting quickly to everyday events. The firm has undoubtedly made significant strides in promoting its brand through content marketing and social media marketing, developing the way in which it relates to the outside world. The way in which it approached content marketing demonstrates innovative and original thinking and applying its knowledge to the news instantly.

About the author

Claire Trévien is Social Media and Marketing Manager at Passle which provides a content marketing platform for professional services firms. Passle recently won the Supplier Innovation Awards at the Legal Innovation Awards.

home.passle.net
www.pinifranco.com

TECHNOLOGY TRANSPARENCY

How to improve the law firm/client relationship

By Nicholas d'Adhemar, CEO at Apperio Solutions

The traditional law firm client relationship has remained relatively unchanged for decades. Law firms have managed to keep much of what they do and how they operate a mystery to the client. Clients often do not understand the time and work that goes into the deliverables they request. And, despite regular conversations between both parties, fees and invoices can remain a taboo subject that is avoided until the last possible moment.

Communication problems

Like any relationship, a lack of communication can lead to misunderstandings. In a law firm/client context, this is frequently played out when the time comes to pay the bill. In fact, 74 percent of the businesses that use the Apperio legal spend tracking platform previously reported having regular invoice disputes with their law firms. Nine times out of ten this was purely down to poor communication between the partner and their client.

The pitfalls that arise from a lack of transparency are not just isolated to a law firm's clients but also to the law firms themselves. One top ten UK law firm, with a £1.4bn turnover, estimated that it wrote off almost £100m in fees due to poor communication in the previous financial year. It is not just the financial impact that matters, the impact that it can have on the client relationship is equally, if not more, important.

Why this has been the status quo?

The industry has remained resistant to transparency for a number of reasons. It's true to say that some law firms do not want the client to see fee breakdowns. This could be because clients might take fees out of context (if a deal was frontloaded with work) or it could simply be that the client relationship partner wants to be able to sanitise anything before the client sees it. It is also possible the law firm has been inflating bills and doesn't want the client to know.

> "It is one of the main factors that leads to client churn"

This misalignment of information has reached a point where some clients will refuse, as a matter of principle, to pay the amount on the first invoice. They expect to be able to beat up their law firm to write off in the region of 20 percent. It has almost become a game whereby law firms know this will happen so they price this discount into their opening invoice.

The benefits of transparency to a business

The benefits of transparency to businesses are obvious. Regular updates on fee information and matter progress gives the businesses accurate information which enables them to effectively budget and plan.

Additionally, transparency enables businesses to proactively monitor deals as they progress and gives them the ability to identify something before it becomes a problem. This concept of proactive management rather than reactive at the point of invoice is key. It removes the element of surprise and is, frankly, smart business.

The benefits of transparency to a law firm

The benefits of transparency are as important to the law firm as they are to their clients. The single biggest complaint from clients of City law firms relates to their lack of transparency over fees. In fact, it is one of the main factors that leads to client churn. Keeping clients regularly informed will lead to happier and more understanding clients, as well as building greater trust into the relationship. Happier clients spend more money, which in turn benefits the law firm.

The flip side to sharing pre-invoice information with a client is that it actually leads to greater cost recovery for law firms. As clients are able to manage matters as they progress, they are also able to see fees as they are recorded and equate that directly to the value that they receive. The net result is that clients will pay a greater proportion of the bills they receive.

How technology can make this happen

Clients don't have the time or inclination to chase all of their lawyers to keep them regularly updated on fees. Lawyers would have to spend considerable time contacting each one of their clients on daily/weekly basis and informing them where they are on fees. The ever-advancing nature of technology means that this transparency is only a platform away. The use of technology can automate this process, plugging directly into the law firms' time recording systems, normalising it and then feeding it back to a client dashboard. A task that may have taken weeks for a large business to conduct previously is achieved in an instant.

You won't be surprised to learn that my company provides exactly such a platform. It allows businesses to view, manage and analyse legal spend in real time. We believe that we are at the forefront of a revolution in legal practice transparency. It's going to be hard for many firms to accept that this is good practice. Sadly, as more and more law firms become more transparent, those that refuse will be left behind.

About the author
Nicholas d'Adhemar is the founder and CEO of Apperio. He spent six years working as a lawyer and three years as a client. He built his business on the realisation that the fewer fee-related surprises, the happier the client.

www.apperio.com

IMPROVE COURT BUNDLING FOR 'FREE'

Disaster avoidance for lawyers and courts through e-bundling

By Tim Long, CEO at Zylpha

Justice Secretary Michael Gove's seemingly heartfelt desire to reform the legal system has had much press coverage lately. He claims that significant reform is required to eliminate the unfairness of what he sees as a two-tier legal system; which treats the poorest far less well than the richest. While many would point the finger at the previous administration's machinations with Legal Aid for this 'unacceptable' status quo, Gove focuses his ire on the need to reform process and efficiency instead.

Before one dismisses this out of hand though he may, in this respect, have a point. Making the case for reform initially of the Criminal Court system, the Justice Secretary condemned the "human cost" of the "waste and efficiency" in the current legal system. In his view, far too many cases are now derailed by poor administration, which causes prisoners to arrive late at court. He also criticises the insufficient use of modern technology such as video and even worse the perennial scourge of missing paperwork. In a strongly worded statement, he recently added. "It is the poorest in our society who are disproportionately the victims of crime, and who find themselves at the mercy of this creaking and dysfunctional system."

Importantly, he went on to opine that prosecutions should be brought more efficiently and that information should exchanged by secure email or conference calls "rather than in a series of hearings". He also felt that evidence needed be served "in a timely and effective way". In his view the introduction of innovation would resolve these issues. Justice Secretary Gove also added that such innovations must be "implemented with all speed".

Mr. Gove's comments echoed views expressed in a similar vein by senior judge Lord Justice Leveson that criminal justice in England and Wales needs far-ranging reform to increase efficiency and therein to lower costs. Innovation does also seem to be one of the trending clarion calls at Practice level.

But where's the money?

In response to the Justice Secretary's comments, a rather back-footed legal system has retaliated with the time-honoured implication that most things are possible if the money is there to fund them. The debate in the press since has descended into a rather messy debacle as to whether the Treasury might be able to stump up the estimated £700 million to introduce the reforms.

To me this required investment is where the story ceases to make sense. Much of the technology required to automate the court process is already available and its introduction would revolutionise the current cost structures in play – saving huge sums and dramatically improving efficiency in the process. It would also eliminate the abject frustrations of lost paperwork and other major data breaches from mishandled documents. Potentially, therefore, the enormous savings available from automating the current paper-based systems are so great that it could very likely fund all aspects of the reform required.

So let's look at where these potentially enormous cost savings can be found. Well, with the exception of the Supreme Court and a couple of other trailblazers, most of the UK court system still insists on receiving legal document bundles in paper. Document bundles are of course at the heart of the current UK court process. Incidentally, this is also the same in the coroner's sector where inquest bundles also need to be submitted in paper.

By contrast, in advance of going to court, the majority of practices are now moving to both electronic document bundling and secure electronic communication as a matter of best-practice. This is also the case with the legal services departments of many local authorities. For example, the combined group - South London Legal Partnership - now uses such electronic document technology for services relating to four London boroughs: Richmond, Kingston, Merton and Sutton. The same group is currently involved in a very successful pilot with the West London Family Court to examine the use of e-bundles in Family Hearings.

With Electronic bundling the time taken to create, maintain, paginate and amend complex document bundles is reduced from hours to minutes. These bundles can be hearing and trial bundles, Instructions To Counsel, Case Management Conferences, witness statement exhibits, client reports, board reports and more. Effectively then, cost-laden paper-based processes that once took several hours to manage can now take just a few minutes to effect.

While this enormous time reduction facilitates serious cost savings, this is not the end of it. The costs and environmental impact of literally millions of printed pages are also saved, as are the physical costs of filing, storage and courier charges too. However, as things stand with the current court system, all the bundles prepared by practices electronically have then to be recreated as paper files for the court, which subsequently has to manage

their handling and storage.

So, with all this in mind, I'm convinced that the available savings from the court system moving to electronic documentation would more than fund the cost of all the technology required for reform. Indeed it would simply be an extension of what is already being used in practices and legal services departments. Such document technology can also be tied in with other relevant systems too, such as identity verification and also electronic signatures. In short, the courts would get a comprehensive document technology solution covering all major bases and yet it would be a solution that could potentially pay for itself.

Additional benefits

Apart from cost savings though, one of the other key benefits of electronic bundling is the ability to transfer documents securely online. This negates the risk of highly embarrassing data breaches by mishandled or misplaced paperwork. Traditionally, people have only thought of data security as an IT issue with the internal IT team responsible for dealing with it. Their remit revolves around maintaining the latest security systems and procedures. Countering the threats of DNS attacks and other topical threats such as Crypto-locker or Watering Holes are always going to be their main focus of their work. As a result we are comfortable leaving all our security and IT risk issues to them alone.

> "it would be a solution that could potentially pay for itself "

However, the real impact of security risks is much further-reaching than solely an organisation's IT security systems. Indeed, the greatest security threat is nothing to do with incoming viruses and the like. No, the greatest threat to security is also an organisation's greatest asset – the people that it employs.

Human security breaches

In truth, the highest profile, most inexcusable security breaches are also sadly the most human. This is especially true where sensitive legal or financial information is involved. And it is a sorry list of disasters concerning missing paperwork that can befall people. According to Michael Gove, this is as true in the UK court system as anywhere else. The missing paperwork to which he refers has not vanished – it is of course simply not where it should be and that is proving seriously disruptive. Worse still, as it's missing how can we be sure it's not fallen into the wrong hands?

I remember the BBC News reporting that 'discs containing information from three of the UK's most sensitive inquiries went missing after being put in the post.' The material related to inquiries into the role of the police in the deaths of three men, Mark Duggan, Azelle Rodney and Robert Hamill. The Government said it took the loss "extremely seriously."

One always hopes of course that such events are isolated incidents. However, accidental data loss is apparently currently pretty common. According to the latest statistics from the ICO (Information Commissioners Office) in spring 2015, the accidental loss or theft of paperwork was the third largest type of incident recorded. This is despite the threat of sobering financial penalties from the ICO which, for the record, handles over 14,000 cases annually while fielding over a quarter of a million calls on their helplines.

There is little doubt that the problem is just as common across all sectors too – from central and local government right through to commercial interests and now apparently the courts too. However, for obvious reasons it is, as mentioned, financial and legal data, which is particularly important to protect and often most at risk. Just as in the commercial world where Board Reports are highly confidential and often need to be protected from being leaked, so too is the loss of case files or settlement figures relevant to a court case. The loss of these could, for example, seriously damage the reputation of a practice or legal services department. It could even disrupt the hearing or trial itself.

To me, meeting the Gove criteria starts with a realisation that paper-based information is all too easily, and all too frequently, mislaid on its way to court or even once there. Understandably, this explains the frustration felt by the Justice Secretary, not to mention the judiciary itself. However, by moving to a culture where courts only receive and store sensitive data electronically and then communicate it via secure delivery systems, the risks of such disruption are greatly diminished. If essential highly confidential data is only communicated electronically via secure auditable means to secure court-approved locations, then it can't be left for all to see in a court anteroom or found later in a taxi.

We have answers already

As mentioned such systems already exist and are ready to forward secure electronic document bundles. Indeed the lead already taken by the more innovative practices in the legal sector, along with some local authority lawyers, is likely to point the way ahead for the courts. Not only are such systems able to deliver cost savings, efficiencies and enhanced security but they would also be relatively quick and easy to deploy, thereby meeting Mr. Gove's "need for speed". The main challenge thwarting their introduction is to persuade the courts that, on this point, Mr. Gove does have a case and that it doesn't require breaking the Treasury's bank to transform the best-practice of the court systems along these lines. Whether they would do this willingly and give up their claim for £700 million before pressing the automation button is yet to be seen, though one can only hope that the decisions taken represent 'sound judgments'.

About the author
Tim Long is a qualified solicitor with 20 years of IT experience. He started Zylpha in 2006 to exploit the potential of technology to transform repetitive tasks in legal practices. His clients include local authorities and law firms with over 300 active users.

www.zylpha.com

SOCIAL MEDIA: TRADEMARK THREATS

Could your clients' reputations be damaged by social media fakery?

By Haydn Simpson, Commercial Director, Western Europe at NetNames

In the not-too-distant past, intellectual property lawyers' main focus was to register trademarks and monitor for infringements in traditional media, which would then be actioned in individual jurisdictions. However, in recent years, trademark law professionals have been adapting their approach to meet the host of new challenges presented by technology, social media and the internet.

With its estimated 4.67 billion pages at the time of writing, the internet is vast, relatively unregulated and does not fall under any single jurisdiction. The requirements for protecting trademarks have significantly changed and both brand owners and their legal counsels have been updating their strategies accordingly. The internet is proving to be particularly challenging for brands battling against fraudsters. Social media platforms have changed the way consumers and brand interact, but at the same time, cyber criminals now have an array of new opportunities to defraud brands and their customers. So what does this new brand protection landscape look like, and how can lawyers best advise their clients in this space?

An evolving dark side

It is no secret that social media platforms can provide brands with a powerful new way of marketing their products and services on an unprecedented scale. Figures revealed earlier this year by Statistica showed that social media giant Facebook has over one billion registered profiles, while the microblogging platform Twitter has 288 million monthly active users.

> “new opportunities to defraud brands and their customers”

Social media provides brands with a powerful way of reaching out and engaging with consumers to generate brand awareness and boost marketing and sales efforts. However, with new opportunity comes new risk; just as leading brands can use these channels to target customers, unscrupulous cyber criminals can try to do the same.

The growth of the internet has fuelled the ability for fraudsters to deceive consumers with unauthorised websites and fake social media profiles that infringe on a brand's intellectual property. These criminals often use copyrighted logos and exploit the features of social media platforms to allow them to create a familiar 'branded' 'environment that helps to gain the consumer's trust. At this stage, unsuspecting consumers are often lured out of the social media environment and redirected to a third-party site where counterfeit or fraudulent activity takes place.

Unsurprisingly, this abuse of trust can have serious consequences for brands – not just to revenues, but to reputation too. Indeed, research conducted for NetNames' *Internet 2020* report found that 78 percent of internet users would shun a brand if they found themselves on a bogus website purporting to be that brand.

Unfortunately, these threats are not going away any time soon. Last month, UK police seized 6.2 million doses of illicit medicines in a global operation targeting counterfeit pharmaceuticals promoted on social media. The initiative was led by the Medicines and Healthcare products Regulatory Agency (MHRA), who worked with Facebook and Twitter to close social media profiles selling and advertising the fake substances. Nearly 1,400 websites selling illegal drugs were also shut down, and raids took place that uncovered £15 million worth of counterfeit drugs and medical devices.

While high-profile crackdowns like these are certainly welcome, businesses cannot rely on the authorities alone to tackle the fraudsters. Brands and their lawyers must recognise the constant evolution of online channels and how these changes affect authorised and unauthorised online activities.

Advising brands on a profile update

The exponential growth of social media platforms means that most brands have some catching up to do in terms of monitoring and enforcement strategies to beat the fraudsters. While most businesses are willing to embrace new online channels and routes to market for sales, they must also address the risks and threats posed by fraudsters.

Even though sites like Facebook and Twitter have processes in place to deal with intellectual property violations and suspicious advertisements, brands must also remain vigilant and help to identify any fraudulent profiles. This is true even if businesses do not choose to directly engage with social media platforms for marketing purposes themselves, as fraudsters can still exploit them there.

Now more than ever, it is vital for brands to have a robust, proactive strategy in place to protect themselves and their customers. IP lawyers must also help their clients to implement a proactive brand protection strategy that will enable them to protect vital revenues and reputation from cyber criminals, especially on new and unregulated platforms.

The responsibility to protect consumers lies with the brand or trademark owner and their advisers to monitor the internet, to detect infringements and to issue enforcement notices. It can be relatively simple to do this, but many brands are not considering the consequences and reacting to these new challenges, which is exactly why legal guidance in this area is so crucial. Understanding this new 'social' brand protection landscape is therefore key for intellectual property lawyers who wish to safeguard their clients' brands.

About the author

Haydn Simpson is Commercial Director Western Europe at NetNames, a global online brand protection specialist. He's led the company's growth in brand protection for the past eight years, following senior sales roles in domain name management and internet advertising.

www.netnames.com

SECURITY: GET YOUR BOARD ON BOARD

How to achieve board level support for an effective cyber security strategy

By Adrian Woolfe, Freelance Technical Writer

The number of security breaches in the UK has continued to increase, with 90 percent of large companies reporting breaches, up from 81 percent last year, according to the 2015 Information Security Breaches Survey, conducted by the UK government and PwC. Furthermore, the cost to businesses has more than doubled in the past year. The 'starting costs' for a major security breach at a large organisation rose to an average £1.46m – up from £600,000 in 2014, while smaller firms can expect to pay £310,000 – up from £115,000.

No sector has been immune from the targeted attacks. Cyber criminals and hacktivists have certainly become more sophisticated but the primary source of targeted attack still comes from foreign states seeking political, economic, commercial or intelligence information.

The Head of Threat Intelligence at Context Information Security noted, "We know from our own experience at Context that legal firms all over the world have been targeted by attackers, in most cases seeking sensitive data belonging to their clients. A few firms that have suffered security compromises have been named publicly, while many others have been informed by government sources and an even greater number are likely to remain unaware of the security breaches on their networks."

Security in law firms

Most large legal firms have a specialist security team and achieve the security basics very well. Some conduct more proactive threat detection to identify threats that anti-virus and other traditional security products may not find. But how does an IT department understand what data is attractive to an attacker and protect it effectively? How should firms translate IT security risks into business process change?

Law firms need a cybersecurity strategy that involves stakeholders from across the business and not just IT. The strategy must have board level buy-in and be actioned within every department. The five key steps are:

- Brief the Board on the cyber threats to your business
- Understand incident detection and response capabilities
- Gather threat intelligence and evidence of network compromise
- Talk about cyber attacks with peers and clients
- Set and understand goals while working towards a strategy

The Board must understand that cyber attacks represent a real risk to the company's data and that threat actors exist who are motivated to carry out these attacks. A successful outcome for this first step is recognition and a commitment to exploratory work.

Briefing the Board is not a step to be undertaken lightly; Board members will require the right information delivered in the right way to guide them. It may help to bring in an external specialist, either a recognised industry or government expert. The UK agencies responsible for cyber security are CESG, the Information Assurance arm of GCHQ, and CPNI, the Centre for the Protection of National Infrastructure, and they are responsible for accrediting companies to provide cyber incident response services through the Cyber Incident Response (CIR) scheme.

Establish the need

Your briefing should describe the threat landscape, cover industry case studies and target data as well as discussing possible courses of action. This is not a technical briefing because the problem is a business issue and not an IT issue. There is no place for fear, uncertainty and doubt anymore; this is not about scaremongering, but about presenting information clearly and setting out risks.

In many organisations, a gap analysis exercise is the first step towards being able to provide a picture of how well prepared the organisation is to detect and respond to, or protect against, incidents. Usually carried out by a third party, a gap analysis will identify security weaknesses, compare the organisation against industry best practice and provide a series of prioritised

"The problem is a business issue and not an IT issue" recommendations for improving defences.

Some law firms carry out gap analysis exercises regularly to chart progress and one of our clients even makes the results available to its clients in order to show a high level of awareness and the actions taken to safeguard data.

The next phase is to seek the Board's support for further work to establish whether or not the organisation's defences have been breached. Detection of compromise can take different forms and each provider will have its own way of tackling the problem. One of the key decisions to make is whether to adopt a consultative approach or a managed service? A consultative approach will be more tailored to the firm's needs, but requires effort and involvement. Managed service providers will remove that effort but often come at a premium.

There are three main sources of evidence: log, host and network. Log data, assuming it is collected and reliable, allows investigators to look back and try to find known signatures of attack. Examining hosts can reveal traces of malware either historic, current and active, or dormant. Network data is potentially the richest seam and allows for recording an attack in progress through monitoring all data entering and leaving an organisation to the internet.

> "A consultative approach or a managed service?"

Detection engagement rarely finds nothing and organisations will often accept some level of compromise. For the Board to take notice, the output of the exercise must be a summary of a detailed investigation, looking not just at malware, but potential business impact, whether incidents were avoidable, the true cost of the incident and remediation, and of course, whether data was, or could have been lost.

Transparency

If the data most at risk belongs to clients, the Board will have to take some tough decisions around assessing impact and whether to inform clients

The next step is one of the most uncomfortable for any organisation to take: opening up to others about the issues and what has been done about them. There are a number of ways to approach this: industry security forums, bi-lateral contacts in other firms, or wider cybersecurity gatherings. You can be sure that every other company in the legal industry is facing the same problems, so this is a real opportunity to share, learn and perhaps even lead.

Your cyber security strategy

The first four steps are intended to give firms an understanding of the real risks and threats so they can take an informed decision on action. In some cases, the answer may be 'nothing at all' and this can be a valid approach if the decision makers have the relevant information and are prepared to accept the level of risk presented. In most cases, the issue is placed on the risk register and a Board member oversees work across the business to remedy the shortcomings.

A cyber security strategy has different strands. These should include:

- Regular/ongoing detection and response exercises to mitigate/reduce impact
- Ongoing risk and threat assessments and identifying projects or clients likely to raise the risk of attacks and protecting that data from the outset
- Network hardening measures and increased visibility of evidence sources along the so-called 'Kill Chain' – a set of steps an attacker must work through from network reconnaissance to the exfiltration of data – for aiding investigations when breaches occur
- Engagement with clients, others in the legal sector and government to talk about the issues
- Working with HR to increase staff education and awareness
- A capability to deal with cyber attacks in a 'Business As Usual' fashion
- An intelligence gathering strategy.

Conclusion

Law firms, like other data aggregators or third party service providers with access to sensitive data, will sooner or later lose business if they do not identify and mitigate cyber risks. Reputational damage in the aftermath of an attack is one aspect, but another is clients seeking assurances that their data is safe while in the hands of their lawyers. Financial penalties for data loss may also have a serious impact as regulators and governments seek to punish this type of breach. As client organisations significantly improve the security of their networks, law firms must ensure they do not become the weak link in the protection of data.

About the author

Adrian Woolfe is a freelance writer specialising in high technology. He writes about digital communications, cloud infrastructure and the business use of technology. He acknowledges the help given by Context Information Security when preparing this article.

www.contextis.com

LexisNexis® Enterprise Solutions

Creating enduring and valuable relationships with your clients is all about delivering excellent service at a competitive price whilst ensuring efficiency and profitability for your firm. To do this you need the right technology; built to adapt to changing competitive legal markets, delivered by an industry expert.

LexisNexis Enterprise Solutions offers powerful software built with legal market expertise to help you get ahead – and stay ahead.

- **LexisOne™** - Enterprise resource planning
- **Lexis® InterAction®** - Client relationship management
- **Lexis® Visualfiles™** - Legal workflow and case management

Contact Us

For more information, please contact us:

salesinfo@lexisnexis.co.uk
+44 (0) 113 226 2065
www.lexisnexis.co.uk/enterprisesolutions

Follow us on Twitter
@LexisNexisES

LexisNexis®

Enterprise Solutions

DEALING WITH BYOD POLICY FEARS

What happened when a lawyer suddenly received a BYOD policy document

By Matt Lancaster, Director at Pracctice and Chairman of the LSSA

A law firm recently emailed its employees a Bring-Your-Own-Device policy document. It comprised a simple overview page covering the main dos and don'ts and some more technical pages which helped users with specific machine and software issues. One of the lawyers, an old hand, took this document as a personal affront. We thought you might like to read the (email) conversation between him and the senior partner.

We've been logging in from phones, tablets and laptops for ages. Why are you suddenly getting twitchy?

The reason for the BYOD policy is to protect both the company and the employees from falling foul of data protection or confidentiality policies. Logging into our company systems via your own device such as phone, laptop, tablet or computer is absolutely fine as long as it's done in a secure and considered manner; hence the policy! Most of our systems reside in secure data centres provided by our suppliers so accessing these remotely, providing you are not saving your credentials in the web browser, is as secure as using the software from our offices. Ensuring we all adhere to the policy will mitigate the risk of any data being lost, stolen or used inappropriately.

It's sometimes much easier to use a thumb drive to take work home or on the road. Are you really planning to stop me?

Yes, absolutely. Thumb drives are such a security issue that we will not allow the use of these in our organisation. Saving your data to a thumb drive means that sensitive data is on a small device that can easily be lost which of course creates huge concerns with regard to security. Furthermore, data stored on thumb drives is rarely encrypted which means that, once lost, the data is readily available to anyone who wishes to use it. Viruses can also be easily transferred using thumb drives and, while we would never suggest this would be done on purpose, the risk is such that our policy prohibits their use.

When you intend to work from home, please ensure your data is uploaded to our web-based practice management system which is accessible from anywhere but ensures the data resides in the safety and security of our software supplier's data centre. Should any information be downloaded to your local device then you must ensure that it is deleted and all traces removed when you have finished working with it. This will minimise the risk of people accessing your local machine and having access to sensitive or confidential work materials. Ideally you will never download any information to your local device. However, we accept that in some circumstance this may be necessary and therefore our policy provides instructions on how to manage that.

Will I be able to use whatever software I like? After all, I've bought the machines.

Not quite. Software is licenced differently for corporate and personal use and therefore any software you use to perform your work must be licenced accordingly. Please contact our IT department to discuss your particular requirement so that we can ensure the software you intend to use is appropriately licenced. Our BYOD policy covers this area in some depth.

Are you going to clog up my machine with company software? Will it work on my Android phone, iPad and Lenovo Windows 7 laptop?

As we use web-based systems we won't clog up your machine or alter any settings since nothing will be installed on the device itself. That's the joy of work with true web-based systems. You will simply be accessing our systems through an Internet browser just as you do in the office rather than working on systems that are installed on your machine - think of accessing Linked in, Facebook or BBC news. As you are accessing systems that are hosted and distributed as webpages it will work on any device.

I really don't want the company to be able to rummage around my personal data or be able to seize control of my devices.

As you are connecting to our services through a web browser and not installing corporate applications locally we would not require access to your local device. Furthermore, as I mentioned above, we would never want you to store anything locally on your machine and if you do it must be deleted immediately after you've finished with it.

If you expect me to do work out of hours, you can't stop me doing private stuff at work.

Well, this is a separate issue from bringing your own device. I wouldn't expect you to work outside of your contracted hours but you may of course if you wish. While you are at work, I would expect you to focus on work, as I would hope is your desire!? Okay, a bit harsh, but it's a question of using your common sense.

I mean, really, don't you trust me? Have I ever let you down? Why should I start now?

There is no issue of trust, in fact the opposite, you have access to our systems from wherever you are and on your own device because we trust you. It is our responsibility to mitigate any potential risks and the BYOD policy is aimed to do that to keep our data safe and secure.

I hope the above helps address your concerns. I know the BYOD policy document is heavy-going in places, but all the broad principles are laid out on the first page. Most people will never need to read beyond that.

[If you're wondering why Matt Lancaster's submitted someone else's email instead of writing his own article, the truth is that this is actually his own creation. – Ed.]

About the author

Matthew Lancaster is Chairman of the LSSA and Sales and Marketing Director of Pracctice Ltd, the company behind the Osprey Legal Cloud. He has worked in the legal industry for 25 years and specifically within the legal software industry for 16 years.

www.ospreylegalcloud.co.uk

EU DATA PRIVACY IN THE CLOUD

What cloud users need to know about EU data privacy rules

By Willy Leichter, Global Director Cloud Security at CipherCloud

Data privacy regulations in the European Union (EU) are among the most stringent in the world and can deter companies that operate in the region from maximising the benefits of cloud adoption. In order to send data into the cloud, firms need to understand the regulations in play and the measures required to achieve compliance.

This is evidenced in CipherCloud's *Cloud Data Security Report*, which examines related strategies of organisations in 12 vertical markets. It found that 64 percent of organisations worldwide name 'compliance and standards' as the top reason for protecting cloud-bound information.

What are the data privacy rules?

The shift in legal landscape in the EU and growing awareness of privacy and data protection issues have led companies to consider additional protection for moving sensitive data into cloud applications. This would then put the Data Protection Directive, the cornerstone EU data legislation, into play.

Application of the legal principles in the directive gives rise to a number of regulatory requirements. When businesses decide to go to the cloud, one of the requirements is for the cloud customer to take appropriate measures in order to protect the data, taking into account the cost, risk level and classification of the data being processed. Companies must also assess whether their cloud providers offer sufficient guarantees in respect to technical and organisational measures, and this (together with certain liability provisions) must be laid out in a contract.

What are the cloud security standards?

The issue of data security is a top concern for companies from a legal, commercial and operational perspective. This is particularly true when data qualifies as sensitive. Securing that data becomes an important issue because companies do not want business critical or personally identifiable information to be subject to data breaches, hacking or other unauthorised access.

Given its importance, the European Commission has listed a key action point (in *Unleashing the Potential of Cloud Computing in Europe*) of setting up security standards and adopting certification schemes. It has resulted in the establishment by the European Telecommunications Standards Institute (ETSI)'s *Cloud Standards Coordination* report, which provides an overview of ongoing standardisation initiatives in cloud security. Related to this framework, the European Union Agency for Network and Information Security (ENISA) cites International Organisation for Standardisation (ISO) and PCI Data Security Standards among existing cloud computing certification schemes for cloud customers guidance. [https://resilience.enisa.europa.eu/cloud-computing-certification]

Should you grant government and law enforcement access? The Snowden revelations and massive data breaches have placed prevention of data surveillance high on the enterprise agenda. Companies operating in the EU must be aware of data privacy and residency considerations that apply to transferring personal information to parties outside of the European Economic Area. Additionally, companies holding such data pertaining to EU citizens must also contend with the possibility of unwanted access by national and foreign government agencies.

A recent example is the US court ruling that US jurisdiction, and with it, access to data, applied to data Microsoft was storing on servers in Ireland. Though Microsoft is appealing the ruling, the case reveals the uncertainty of data jurisdiction in the cloud and the plausibility of unwanted government intrusion.

How can you get high level security compliance?

Even in cases where the use of cloud-based services is considered to fall under the scope of data protection laws, encryption and tokenisation (a code represents sensitive data, which never leaves your premises) solutions can help achieve compliance on a number of legal requirements. In fact, the CipherCloud report also found that the majority of organisations with a cloud security deployment centred their data protection efforts on encryption (81 percent) followed by tokenisation (19 percent).

Both encryption and tokenisation can offer a high level of compliance for the security of personal data through local storage of encryption keys (or token mapping tables) and a granular and layered approach to securing sensitive data. In addition, these techniques can complement local storage offered by cloud providers in addressing cross-border transference of data outside of the EEA, and can help organisations to carry out privacy impact analyses of cloud providers.

With regards to personal data, organisations should be aware that the legal requirements do not apply if they are sending sufficiently secured personal data (that cannot link to, or single out an individual) to a cloud service provider. If one argues that encryption or tokenisation make the data effectively anonymous, the data processed in the cloud is no longer personal data. Where the rules on the processing of personal data still apply, encryption and tokenisation techniques can nonetheless increase the level of legal compliance.

Essentially, a sufficient level of encryption or tokenisation of data before sending it to the cloud could avoid the legal barriers created by data protection laws. For stricter regulations, such solutions can still offer substantial benefits for achieving legal compliance from a data protection point of view. When implemented properly, they can also offer a high level of compliance from the perspective of general security requirements and protection against unwanted access to the data.

About the author

Willy Leichter leads CipherCloud's efforts to evangelise new models for cloud security, creating product requirements and market positioning. He's held marketing and product management positions in the US and Europe, at CipherCloud, Axway, Websense, Tumbleweed Communications, and Secure Computing (McAfee).

www.ciphercloud.com

NEW WAYS TO FILE FOREIGN PATENTS

How cloud-based platforms simplify foreign filing

By Justin Simpson, Founder of inovia

The past decade has witnessed a significant increase in specialist IP service providers that focus on a certain area of the patent system, one being foreign filing. While outsourcing a service like annuities has been common for decades, only in the past 12 years has there been an emergence of foreign filing platforms that completely streamline and simplify the once complicated and time-consuming part of the patent process.

In many cases, Intellectual Property professionals have been hesitant to alter their filing strategies as the industry is historically slow to change its ways. However, times and attitudes are changing with regard to foreign filing practices. With the emergence of service providers, what was once a lengthy and costly process is now a simple administrative task. Providers now offer cloud-based solutions for their clients, which in turn increases transparency and efficiency, a goal that all companies and law firms seek to achieve in 2015.

The international patenting steps involved in the Patent Cooperation Treaty (PCT) and European patent process can be very costly if protection is sought in multiple countries. Prior to the arrival of specialist IP platforms, applicants used their local counsel to handle all of their foreign filing needs. With the emergence of streamlined filing systems, this is now unnecessary and considered a more old-fashioned approach.

“Cloud-based solutions increase transparency and efficiency”

After filing a PCT application, entering the national stage requires filling out the proper forms, submitting the necessary documents and coordinating with foreign associates. Since no substantive work is involved, a patent attorney offers limited value when handling this part of the process. In fact, a paralegal or administrator within the firm generally takes care of it.

Over the past twelve years we (at inovia) have established a network of professional and top-quality attorneys in over 135 countries and negotiated fixed rates with those agents by virtue of the significant volume of work sent each year. After all, service providers like us do not eliminate the need for a patent attorney, because the substantive prosecution after filing overseas still needs expert input. We simply help in this one area of the patent process to save our clients time and money.

Which countries are interested in these services?

According to our annual survey, *The 2015 Global Patent & IP Trends Indicator* – now in its sixth year – foreign patent filing is on the rise in Brazil, Russia, India, and China (also known as the BRIC countries). In this research, we surveyed companies and universities based in North America and Europe. Organisations surveyed spanned industries and ranged from small enterprises filing a single patent family to multinationals filing more than 100 patent families in 2014. All survey participants are involved in the IP strategy and patent filing activity of their organisation with job functions ranging from patent manager, to general counsel and up to executive leadership positions.

As in previous years, respondents were also asked to rank the importance of certain jurisdictions in their 10-year foreign filing strategies. For the second consecutive year, Europe was rated as the most important destination, with China and Japan following closely behind respectively.

83 percent of the survey respondents filed into the BRIC countries jurisdictions for the first time within the last five years, with the remaining applicants not willing to file there in the near future. Those interested in filing into BRIC countries noted that they were seeking fast and affordable services that used cloud-based solutions they could easily access online. While five years ago these destinations were considered unreliable and unnecessary for most seeking patent protection, the growing technology sectors and business expansion opportunities in these jurisdictions now appear attractive for corporations and inventors looking to protect their IP rights in 2015.

Many respondents from the survey also noted they were looking for cost effective solutions that would help stretch their patent budgets as far as possible. Companies and inventors have been working on reduced budgets since the economic downturn. While patent budgets have improved since 2010 (only 31 percent of respondents were working on a reduced IP budget in 2014 compared to nearly two-thirds of respondents 5 years ago), applicants were still adamant about keeping filing costs down while receiving the same quality of work.

Only 35 percent of respondents noted they would file into fewer countries to save money. More applicants were willing to turn to service providers and make up the cost difference that way rather than sacrifice the number of destinations to file into. The attitudes of IP applicants are changing with more individuals and companies taking control of their foreign filing. A growing number of respondents from the annual survey reported that they plan to save on foreign filing costs by shifting their work from attorneys to non-law firm providers.

With the emergence of these foreign filing providers, including inovia, it’s undeniable that the IP landscape has evolved dramatically in the past twelve years. Companies and law firms are looking to save money and time, while improving internal efficiencies. Now is a good time for all firms to consider aligning with an IP platform and be a part of these changing times.

About the author

Justin Simpson, BSc LLB, invented the inovia technology platform in 2000 and founded the company in 2002. Previously, he was a software specialist patent attorney for Australian attorney firms including Allens Arthur Robinson and Shelston IP.

www.inovia.com

MANAGING SMARTPHONE RISKS

How to tackle the dangers that lurk in the business use of personal smartphones

By Phil Beckett, Partner at Proven Legal Technologies

Many businesses are still unaware of the risks involved with employees using their own smartphones for work purposes. The truth is that even 'wiped' smartphones can retain a lot more information than their owners realise, from call and web browser history, to photographs and files.

To illustrate this point, here at Proven Legal Technologies, we bought four randomly selected second-hand smartphones from eBay, two of which had removable memory cards – all from UK-based personal sellers.

The content was forensically analysed, revealing a surprising amount of information about previous use, some of which had not been wiped and some that was retrievable despite having been deleted. We retrieved information about 1,392 calls, all but one of which had been deleted. We also traced 442 SMS/MMS messages and 616 third-party application messages – such as those from Facebook and Twitter.

We also found 749 audio files and 727 pieces of location data, with 2,967 other files, such as system files, of which 1,531 had been deleted. We discovered a further 474 pieces of information from the web browser, such as browser history, bookmarks, searches and cookies.

These discoveries come as an increasing number of people now own smartphones, changing their device on average every two years and storing more information on them than ever. From Facebook, Twitter and LinkedIn, to WhatsApp messages, emails, texts, browser history and personal notes, a wealth of information about that person and their employer's business can be gleaned from each handset as it is sold on. This poses a potential risk to the security of the business and its intellectual property.

BYOD boom should be considered

It is important to consider these results in the context of Bring Your Own Device (BYOD) schemes, which are becoming more popular, as employers grow savvy to the benefits of allowing staff to use their own smartphones, tablets and laptops both on site and remotely.

However, while such schemes may offer flexibility, it is important to consider the security implications of having vast amounts of confidential data about your business stored on your employees' phones. If an employee were to sell on his or her phone, how much of your company's information would still be stored on the handset, whether deleted or not?

It is important to identify the threats you could face to, ultimately, minimise the risks.

Well-documented means well-prepared

First, businesses need to treat confidential information as confidential. It may sound obvious, but organisations should ensure that only those with a legitimate need can access this material, and also make sure this access is logged and recorded. If you do have a BYOD or smartphone policy, it should be clear and well-documented. It should describe exactly what individuals are permitted to do with the firm's data and devices. It's also important to define what constitutes an offence; for example, taking documents out to access at home.

Data that is removed from the company domain is harder to monitor so, if you would prefer employees not to do this, include this in your policy. Likewise, you should ensure that confidential information is not shared or discussed via other messaging forms.

Employees should be made aware of these policies and given appropriate training so that they understand the importance of risk management and intellectual property.

Businesses should also establish their right to audit or delete any sensitive information as necessary, for anyone who is allowed to come into a workplace and use a personal device to log onto the office system. This will give firms the right to periodically audit the employee's device and permanently delete company data.

If you do decide to give a foreign device access to the corporate network, think about how 'deep' you want it to go. The access parameters within which employees can operate should be considered and set out clearly, and could vary between their different devices. In addition, firms must take steps to protect their data by implementing robust firewalls, anti-virus software and encryption methods to minimise risks.

Some solutions on the market enable smartphones to be internally segregated to block interaction between the personal and corporate side. This could help overcome the risk associated with users flicking between business and social apps and accidentally or deliberately sharing sensitive information.

Not all bad news

While the legacy of data left on a smartphone can be seen as a risk, it also presents an opportunity. A 'wiped' handset could still offer a large amount of crucial information to any company carrying out an investigation – following a security breach, for example.

Experienced forensic teams will always need to determine an individual's pattern of behaviour, so no devices should be overlooked, as they examine all relevant sources, connections and activity. Their role will be to identify all available software platforms and data sources as well as workplace activity patterns such as emails, file transfer history, cloud access and internet history databases. Social media profiles and traces of Skype and video calls will also be important.

By implementing procedures like these – and ensuring that employees are fully signed up to them – firms will be in a much stronger position to protect themselves and their data.

About the author

Phil Beckett is a Partner at corporate forensic investigation and e-disclosure firm, Proven Legal Technologies. Previously, he led Navigant Consulting's European Forensic Technology practice for seven years. He's a qualified fraud examiner and recognised court expert in digital evidence.

www.provenlegal.com

INTRODUCING ENTERPRISE RESOURCE PLANNING

Our decision to switch from traditional practice management systems to ERP

By Mike Giles, Finance Director at Fieldfisher

We recently took the decision to adopt an enterprise resource planning (ERP) system. The plan is to replace multiple business systems with LexisOne, an integrated suite of applications, which includes all the core business capabilities we need as a law firm – general ledger and legal accounting; matter planning; time, travel and expense processing; billing; procurement; purchase; business intelligence and asset management; and human resource management. In doing so, we hope to become a highly efficient business operation (of course) but, more importantly, the approach will deliver value to our clients too.

It's not a decision we took lightly – there is a strong business rationale behind it. Technology projects such as this are demanding, painstaking, expensive and business critical, so we've done a great deal of research and evaluation to ensure that our system selection is appropriate, future proof and practical.

> "We have separate HR and financial systems and it is difficult to link them"

The time is right

We had got to a point where our existing practice management software was no longer delivering what we need as a business. Regardless of whether we stayed with our current technology provider, a complete new software installation was required. Therefore, it made sense to evaluate the alternative systems on the market and to select the one that was the best fit for our firm.

As we began exploring options, it became evident that for our business today (and in view of how the legal marketplace is rapidly changing) a practice management system would only partly meet our requirements. We are a people-led business, but currently have separate HR and financial systems and it is difficult to link them. Traditional practice management software systems don't provide the seamless and reliable interfaces between these two vital functions and we need the capability to undertake head count management, staff budgeting and workload planning – in addition to profit & loss related proficiency.

Removing the integration headache

Like most law firms, we use a number of standalone technology systems for customer relationship management, human resource management and financials alongside the Microsoft Office suite for day to day document production and management. Although they can be linked, it is not easy to fully integrate them and it's never seamless. It's a constant challenge to maintain multiple solutions and that leads to increased cost of ownership of technology.

From a user standpoint, the look and feel of the alternative proprietary systems is very different. A Microsoft Outlook style interface suits our people very well, it is simple and intuitive and makes our system feel 'joined up'.

A step change

The key justification though for our decision to adopt an ERP approach is that it allows us to re-examine the way we conduct our business. It brings us as close to starting with a clean sheet of paper as is realistically possible.

The last time we changed our core technology system was 12-13 years ago. A lot has happened during this time – the legal landscape has changed dramatically as has our business. We've grown from a single office in London to an international firm with a presence in Brussels, Düsseldorf, Hamburg, Manchester, Munich, Silicon Valley, Paris and Shanghai. Today, we have over 400 lawyers and 160 partners. The current practice management system was configured for that single office firm and the way it operated. Along the way, we expanded its use, but never really looked at how we were developing our business processes. While we have made those processes work thus far, we've reached a stage where a step change is required if we are to achieve our growth aspirations.

We need to question everything we do and how we do it in order to ascertain the most effective and efficient way of doing business. I do not buy into the deep-rooted belief that the legal business is 'different'. Like other businesses, we need to adopt best practice in our approach to pricing, matter management, resource planning and so on. To do so, we need access to a rich source of real-time data and management information. This will allow us to be creative and innovative when new business opportunities present themselves while working smarter and in a more client-focussed way so that continuous process improvement becomes standard.

Funds aren't unlimited at Fieldfisher, so we've taken a hard look at our firm and invested in ERP because, after looking at the capabilities and commercial benefits the approach offers, it makes business sense.

Technology sits at the heart of our firm and we are recognised for our legal expertise in IT industry. Our investment in ERP via LexisOne is proof that we believe in what we do, we dare to be different and our approach delivers benefits to the firm and to our clients.

About the author
Mike Giles is the finance director at Fieldfisher and has over 25 years experience in working in professional services organisations, including 16 years working in law firms.

www.fieldfisher.com

BYOD IN THE LEGAL ARENA

Wise words on a successful BYOD implementation

By Matt Torrens, Director at SproutIT

You're probably familiar with the concept but, just in case you're not, Bring-Your-Own-Device: Noun – "the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes". Now we just need to understand why BYOD remains a hot topic, particularly in Legal.

Somewhat unusually, barristers found themselves in a BYOD environment long before anyone coined the phrase. Despite using a conventional, shared and centralised computer network, most barristers still provide their own computers and mobile devices. In most cases however, and certainly until more recently, the notion of a formal BYOD policy or any type of mobile device management was fanciful. Indeed, attitudes towards data security as a whole still have a long way to mature. For the purpose of this paper, solicitors provide a more useful focal point for a BYOD discussion.

How can Legal IT benefit from BYOD?

Software & Apps – Automatically and centrally provision authorised apps to authorised devices.
Device Management – Enforce user-authentication policies, disallow jailbroken devices and block the installation of undesirable applications.
Inventory Management – Map device use by employee as well as device location. Control use rights, based on geographical location, or alert/wipe when a device leaves a defined geographical boundary.
Security Management – Automated device audit to ensure only compliant devices are enrolled; blocking non-compliant devices from the network. The best Mobile Device Management (MDM) solutions manage secure Wi-Fi enrolment, access to internal data stores and deliver a secure browser – often all accessed by micro-VPN.
Encryption – MDM systems can be configured to allow only devices that support suitable encryption technology and the best MDM tools deliver their own securely-contained environment, within the device.
Share & Sync – Policy-based secure synchronisation of corporate data across all enrolled devices. Edit (even while offline) and share documents with clients, co-counsel and others, and receive real-time workflow notifications.

What does BYOD mean for data security?

Separation of work and personal data. It's very important that an MDM solution offers the ability to securely separate form (client) data from personal data on the same device. This 'compartmentalised' zone should be FIPS encrypted and include suitable access security – e.g. centrally managed PIN requirements. This separation of data is all the more important on tablets and suchlike (e.g. iPad) which are often used as shared devices, with friends and family.

The findings of ILTA's *2012 Technology Survey* found that 65 percent of law firms do not track mobile device use. These law firms have no real clue as to how this mobile data is accessed or processed, nor where it is stored. Importantly, the chain of custody for e-disclosure purposes will be largely compromised.

Company Policy

You'll need one! Some items to consider within the policy may include:

- Productivity concerns – using a personal device for business activities could encourage personal use in business time.
- Determine who owns the data and intellectual copyright to the data on the device, particularly if the device is not properly partitioned to split work and personal data.
- Rogue employees or people who leave your organisation. Be sure you have a documented process to wipe the partitioned section of their device or, if there is a need to wipe the whole device, make sure you (and they!) understand what personal data may be lost and who is responsible for that.
- Determine whether 'photographs' are seen as personal or corporate. Most BYOD policy templates rule photographs as personal – but how often do employees use the camera function to capture corporate data? A lot. Photos of whiteboards, business info, evidence collection etc. Such is the quality of smartphone cameras today, that a photo now often replaces a scan or photocopy.
- Once the policy is in place and defined, it is very important to communicate it and to offer training. There's nothing worse than remote wiping a device, and someone's wedding photos, and then hearing the employee had no idea the BYOD policy existed.
- Often the policies will be drafted heavily in the company's favour. While there is a need to mandate some rules and process, businesses should be mindful of their employees and seek a suitable balance.
- Device usage and purchase costs. The question of who foots the bill has long been a barrier to adoption for BYOD in business. Why should the employee purchase and maintain a device, which is often used for business and to make a profit for their employer? Conversely, why should your employer provide you with a work device that you gleefully use to call your wife or place a bet on the football?
- Many companies now offer to foot the purchase of the employee's device, repayable over 2-3 years. While helpful, this raises an issue of financial obligations should the employee leave employment within that period.
- In America, carriers now have technology which, with compatible MDM solutions, can split a device's data usage bill between work and personal use. In the future, voice calls are likely to be able to be split as well. This push was largely designed to protect the rights of the employee in a BYOD environment. Great. But it won't be long before businesses utilise the same technology to re-charge employees for the personal use of their corporate devices.

What about the employees?

So, you've got your smart, new MDM solution and the new company policy is hot off the press. The employer is happy, but let's spare a thought for the foot soldiers; after all, they are your greatest asset. Aren't they?

- Solutions should be broadly self-service; some employees bring a lot of devices!
- The traditional nine-to-five working day no longer applies and BYOD can mean the working clock is reset forever. Be careful not to over-burden employees with a consideration that they are always available and working, thanks to your BYOD environment.
- A Cisco survey reported that productivity and staff job satisfaction increase within a BYOD environment. It's probably true to say that employees prefer the flexibility of single device use but the success of BYOD, from the employee perspective, hinges on a properly crafted BYOD policy that clearly addresses data segregation and ownership, programme funding for device procurement as well as device replacement in the case of damage/loss.

What next?

BYOD is one of those revolutions that has passed some companies by, particularly in Legal. Personal device use is happening within firms, without their knowledge and certainly without clear policies or security. BYOD won't go away any time soon and, in fact, its adoption will only accelerate; we communicate electronically more than ever before and from a variety of devices.

If you already have a BYOD policy then review it now and regularly – there are likely to be technical advances that you should be considering. If you don't yet have one; panic. Then breathe. Then engage an expert to help you create the policies, build the network security and implement the most suitable MDM solution for your business. Gartner reports that 25% of employers in the US now mandate their employees to use personal devices for work and that 84% of legal professionals admit to accessing company data from a personal device, regardless of corporate policy. It's time to empower your workforce and protect your client data, along with your own brand reputation, by embracing BYOD. But to avoid data leaks and to stay on the right side of the Information Commissioner, a well thought out BYOD policy and solution design might just be a good idea.

About the author

Matt Torrens, Legal IT expert and entrepreneur, has been providing secure, innovative, outsourced IT services to professional service firms for over 20 years. He co-owns SproutIT, a specialist in the legal industry and now the leading supplier of IT strategy and service to Barristers' Chambers.

www.sproutit.co.uk

DISASTER. WHAT DISASTER?

Good planning means you won't get caught short

By Nigel Wright, Managing Director of Converge Technology Specialists

When fires raged underground in Holborn in London in April this year, few businesses were prepared for the impact this would have. The London Chambers of Commerce estimated the cost to have been in the region of £40m.

None of the buildings caught fire and, thankfully, no one was hurt, but electricity and gas services were cut as the underground fires took 36 hours to control; 5,000 people were evacuated for safety reasons; shops, courts, offices, theatres, hotels and restaurants stayed shut until power was restored; and the main Holborn road reopened some weeks later, allowing businesses to eventually begin to return to normal. An underground electricity fault turned out to be the cause of the London fires. But businesses needed cutting-edge technology to respond to and deal with the challenge of such widespread business interruption.

Preparation is everything

Companies operating on the Cloud would have come through with a distinct and competitive advantage. They were able to pick up where competitors left off as staff were able to work remotely and on systems that were fully updated and worked in real time. All that staff required was a PC or laptop – and they could work from anywhere. In those crucial 36 hours, business continuity plans were well and truly tested. The virtual office and business as usual became a reality for the organised and prepared, despite the very challenging circumstances.

> “Business as usual became a reality”

Putting this into perspective, a law firm with 50 fee earners, charging £150 per hour on a 5-hour fee charging day would have lost £187,500 based on a 5-day downtime.

We have worked with clients in situations that would make the blood of most managing partners run cold: a junior member of a client’s IT team deleted their virtual server; and another suffered potential business outage due to an air conditioning unit leaking into their office. Perhaps the most likely threat to firms is a computer virus wiping out records or rendering their IT useless. This was the case for one firm affected by the Cryptolocker virus. Luckily for them, a disaster recovery plan was in place (via continuous backup) and the firm was able to return to a point an hour before the virus hit, and get fully up and running within a matter of hours, thus ensuring business continuity.

How would your business have coped in the same conditions? Would you have been able to pick up, dust off and crack on, or would you have had to shut down, put in a claim for loss of earnings and work out how you were going to get back to business as usual?

A duty of care

Of course, law firms are required to provide a duty of care to clients, with a proven business continuity plan in place that outlines how they will continue to trade should the worst happen. It’s a requirement in the Solicitors Regulatory Authority’s code of conduct.

The SRA stipulates that all law firms must:

- Provide a proper standard of service to clients;
- Behave in a way that maintains the trust the public places in firms and in the provision of legal services;
- Comply with legal and regulatory obligations and dealing with regulators and ombudsmen in an open, timely and co-operative manner;
- Run a business or carry out roles in the business effectively and in accordance with proper governance and sound financial and risk management principles; and
- Protect client money and assets.

Data security and protection is the top priority for UK law firms and a solid, proven and tested disaster recovery service forms part of the process of securing data. Data security breaches can warrant hefty fines, create distrust and taint reputations. It isn’t unknown for corporate clients to ask law firms to demonstrate the effectiveness of their data security and disaster recovery plan as failure results in reputational issues in the 24/7 culture we’re all now part of.

Indeed, with the SRA code adhered to, firms must also ensure they comply with data protection rules set out by the Information Commissioner’s Office, which has taken to making examples of firms that fail to protect their business with appropriate safeguards. Increasingly, Financial Conduct Authority regulations are being forced onto law firms and conveyancing firms, which are stricter than SRA rules.

Have you done enough?

But many firms erroneously believe that simply backing up documents, emails and case files is a job well done, a disaster averted, the compliance box ticked.

The process of business continuity management involves an evaluation of the potential risks that could lead to business interruption. Disaster recovery is your response to an event and also includes how you handle your clients, the media and the public at large. How you deal with disaster recovery – your ability to detect a problem, assess its impact, readiness and speed of response – will determine the overall reputational damage to your business. You may as well close down if you lose the confidence and trust of your market.

Disaster Recovery as a Service (DRaaS) is an essential component for all busy law firms focused on client needs. It replicates and hosts your physical servers through a third-party to provide immediate back-up availability in the event of a man-made or natural catastrophe. This is very useful for small to mid-size businesses that lack the necessary expertise to provision, configure and test an effective disaster recovery plan. You won’t need to invest in, or maintain, your own off-site IT disaster recovery solution as it is ‘built-in’ to your Cloud. All that you and your firm needs is an internet connection to access all your data and applications, removing the risk of downtime through local disruption and disaster, and guaranteeing a continuous level of service to clients.

Of course, outsourcing and handing over data to others introduces other very important risk assessment requirements. It is a distinct advantage to use a UK-based DRaaS provider because they will have access to UK-based data centres. These are

compliant with much better internationally recognised security standards and power back-up systems than a physical server. Many firms moving to the Cloud find that, far from adversely affecting their obligation to clients, it can underpin and guarantee delivery of that obligation, as well as providing the DRaaS that they require.

Today, more than ever, as data volumes massively increase and networks become more complicated and testing more onerous, a well thought through disaster recovery plan that considers every possible scenario is essential. Firms need to be able to robustly answer:

- How frequently do we test our disaster recovery plan?
- Is our test to destruction thorough enough?
- How well does our system stand up to threats?
- Do our people know who to reach, what to do, and when they should invoke the business continuity plan?
- Do our people know how to reach the right decision maker and raise the alarm to ensure business as usual or, at the very least, as close to business as usual?
- What do we regard as the right and affordable recovery time objective (RTO)?

But where do you start when it comes to testing systems to destruction? Law firms need to think about and plan for the following:

Test for 'worst case scenario'

An annual, all server shut down, should be the minimum test you undertake, and there is no time like the present. Your clients, panel referrers, quality standards, or management team may require it to be more often. A half-hearted test will not satisfy the above and it should not satisfy the business – always test for the worst case scenario. Consider a fire, a terrorist event, the sudden incapacity of the IT leader or key decision maker and look around you for threats to your business. It could be cybercrime and business sabotage, it could be a natural disaster such as the flooding of a river into your premises, or it could be man-made and as simple as someone spilling water onto your server or a major power cable cut during roadworks.

Include a representative test group

Junior and senior staff should be included in testing the firm's resilience to disruption, and how quickly they can return to fee earning work. Run the test during a time when it is least disruptive, such as an evening or at the weekend, but ensure the test is realistic to build confidence in your business and in your staff. Obtain feedback from staff about any lessons learned from the experience. What were the gaps in your defence? Where were the weak spots? Did everyone know what to do and how to react or respond?

Measure how quickly your firm returns to 'business as usual' – and adapt if necessary

Test how well you meet your RTO – the amount of time lost that your business can potentially sustain. If you fail to meet your RTO, look at ways to reduce it and test and test again. When disaster strikes, being able to easily open and find crucial documents can make the difference between a few hours and a few days in lost fees, as well as keeping reputations intact.

Lexcel as a Practice Management Standard and the Law Society have reacted to the growing threats to business continuity by including a useful business continuity management toolkit. The kit includes signposting to information on the Governments Cyber Essentials Scheme launched in June 2014, the ISO27000 series of International Standards on Information Security Management, and useful Law Society Practice Notes and on-line webinars.

With the right approach, a business disaster can be minimised if not diverted, reducing the impact on down time, costs and reputational damages to your business. The time to act is now.

About the author
Nigel Wright is MD and founder of Converge Technology Specialists – a provider of managed and hosted IT services and the only cloud provider dedicated to UK law firms. He's spent 18 years delivering technology services to professional firms of all sizes.

www.convergets.co.uk

DATA RECOVERY - AT THE DROP OF A HAT

How Hibberts Solicitors found itself an easy to use and effective backup and recovery system

By David Fisk, EMEA Sales Director at Quorum

Tracing its origins back to 1799, long-established legal firm Hibberts Solicitors has five offices in Cheshire and 100 employees. The firm offers a wide variety of legal services to clients in the local community, including commercial services, employment law, family and divorce law, property and agriculture.

The firm values tradition and personal service but understands these qualities need to be underpinned by the right IT systems to meet the challenges of today's legal environment. So Hibberts is constantly seeking to improve and update its services and embrace innovation and information technologies where they benefit clients.

The Challenge

The majority of the firm's IT infrastructure, which includes email, database and file servers, was based at its head office in Cheshire. All these critical services needed to be maintained and made available to staff and clients.

Hibberts previously relied on a tape and disk backup solution with a dedicated server that backed up to disk and tape every night but administration and management was time consuming. In addition, the recovery time from tape in the event of physical failure could be anything from 24 to 48 hours.

> "Gets the company back online within minutes"

With most of the infrastructure concentrated at its head office, the firm was aware of its reliance on a single location.

"We needed to take the onus off one site," said Hibberts' IT manager Chris Boundy. As the person responsible for the firm's infrastructure, he was also looking for a system that could work in the background without him having to worry about it. "I didn't want to be spending a lot of time on things that need constant supervision and work," Boundy explains. "I was looking for something that would manage itself, didn't need a lot of technical input or management and would give me the reliability and peace of mind that I could install with minimal configuration."

Solution

While researching the market, Hibberts came upon data recovery specialist, Quorum. Boundy contacted the vendor to test the system in his IT environment. During due diligence testing, it quickly became apparent Quorum's ease of use set it apart from other solutions on the market.

Boundy opted for two Quorum onQ appliances with a high availability device sited in its head office and another appliance as the data recovery server in a separate location.

The onQ devices keep up-to-date copies of all operating system, application and data files on the local and remote appliances. Unlike conventional backup products, they also keep ready-to-run 'recovery nodes' standing by. If any protected servers fail, the recovery node can be started with a single click and have the business running again in minutes.

The entire backup process is automatic and doesn't require any additional hardware or software, and all it takes is one click to recover data and get the company back online within minutes of a server failure. onQ's incremental updates are extremely efficient, sending only the parts of any files that have changed, storing them in its repository for point-in-time file recovery and merging those changes into the recovery nodes. The updates are so efficient that businesses can keep months of snapshots taken as little as 15 minutes apart.

Installing and deploying the appliances was simple and straightforward. The onQ devices were pre-configured with details provided by Boundy and, after a couple of two-hour training sessions, he was able to install and deploy the solution himself. "I plugged them in, powered them up and added servers that required recovery protection - It was that simple," he says.

The Benefits

The Quorum solution has helped to cut recovery time significantly for Hibberts from days with the older tape system to minutes. This represents a recovery time objective (RTO) reduction of 99.9 percent. With Quorum's recovery nodes, it can take as little as two minutes to power up a server and get it going. Under the previous system, the recovery time could be as much as two days and the recovery data could be up to 24 hours old. With Quorum, backups take place much more frequently, so any data recovered is much fresher than under the old tape-based system.

Quorum appealed to Hibberts because it was competitively priced, secure and user-friendly. Boundy has already used the onQs for file restores and to go back in time in a document's history. Looking to the future he's also exploring using the Quorum solution as a test and development environment. He explained: "At Hibberts we embrace innovation to benefit clients. Quorum fits with this motto by providing quick RTOs, protecting data and providing a snapshot of the whole system for testing."

The solution is easy to use and manage, so if Boundy is on holiday or away from the office, other managers in the firm are able to use it by logging in and clicking a few buttons. "We didn't want a highly technical solution," Boundy explained. "If I'm not there, my colleagues in the office can do the job with the Quorum solution. That was a major decision factor for us."

Summing up, Boundy said Quorum is "a fantastic tool for an IT manager. It makes my job a lot easier having it behind me."

About the author

David Fisk is EMEA Sales Director of instant disaster recovery company, Quorum. He builds excellent customer relationships through integrity, credibility and has being able to articulate business value at all management levels through to blue chip companies.

www.quorum.net www.hibberts.com

SHUT YOUR 2003 WINDOWS

How to address the threats caused by the end of Windows 2003 Server support

By Robert Rutherford, CEO of QuoStar

Microsoft Windows Server 2003

```
indows\Windows_Server_2003 >Replace
sers\Administrator>July_14th
```

support ENDED!

If you are using Windows 2003 servers, your legal firm is at risk. Simply put, for those that have yet to migrate their operating system, you need to do it. Cost saving should not be an excuse – IT security cannot be considered a luxury – it is essential, inaction has already put your law firm at great risk from dangerous and targeted cyber attacks.

As you debate whether it is worth upgrading from Windows 2003 or not, your data is at risk of being stolen. The consequences of this could be significant, causing embarrassment to the firm and also bringing threats of a regulatory compliance breaches. The expense of a fine from regulators can be heavy - EU General Data Protection legislation means that you could be fined up to two per cent of your annual turnover for a breach. In addition to your data, critical systems including email and case management can now be readily breached by a hacker or malicious code.

Understand the threats

Recently, some security vendors have been claiming that they can protect your systems despite you still running on 2003. Generally, this is not the case. Processes or people tend to be the weakest links in the security chain. Firewall protection is not enough, nor are staff and organisational protocols.

> **“Now that support has ended the number of break-ins is likely to grow ”**

The removal of Windows support (as of July 14 this year) means that 2003 servers in your legal firm are vulnerable to a wide range of threats. If your server is directly facing the internet, relying on a firewall may be ineffective as malware and zero-day threats target vulnerabilities which are not patched and your firewall may be unaware of. The lack of security patches makes the server an easy access point for hackers to access your systems. Using the internet also runs the risk of allowing malicious code to infiltrate the server and ultimately the Local Area Network (LAN) /Wide Area Network (WAN) it sits on.

Computers and other connected hardware in a LAN now also pose major problems. Regardless of whether your PCs, laptops and other servers are infected, they could still pass infections on to unprotected Windows 2003 devices. As viruses such as Flame and Stuxnet have shown, USB storage devices can also carry threats when plugged in. These mobile threats can be brought in by anyone, such as contract workers or suppliers pitching a product. Without the Window’s patches, such devices are now an even greater threat to your data security.

Now that support has ended there are likely to be a growing number of break-ins. The worst attacks will come in the next six to nine months and will then start easing off once all the soft targets have been hit.

Develop a solution

If you have not switched from your Windows 2003 server, it is critical that you start taking the following steps:

1. Keep the server from being directly connected to the internet through the use of a firewall device and keep it separate from the LAN via a Virtual Local Area Network (VLAN) at the least.
2. Do not allow any external devices to be plugged into it at all.
3. Begin planning the migration of services off the Windows 2003 server.

Make a plan

Now that support has finished, you need to create a plan that protects your services as quickly as possible. This can be an intricate and challenging job, so start planning now or bring in a consultant quickly.
Consider the following when developing your plan:

1. Will your existing hardware support the new operating systems and/or software?
2. Will your other applications work on the new operating systems and/or software?
3. Will third party application vendors support their applications on a new platform?
4. How will you overcome compatibility issues?
5. Do IT staff require training to roll-out and manage the new operating systems and/or software?
6. Will other employees need training to use the new operating systems and/or software?
7. How long will it take to test everything?
8. What resources are needed to roll out the new operating systems and/or software?
9. How long will the roll-out take?
10. What do you need to budget for? For example, you can go for a fully managed cloud option, your own private cloud option, or simply replace servers and software in your own office.

To ensure your firm remains secure and successful is dependent on how you act now. Continued inaction is putting you at the mercy of hackers, leaving you exposed the regulators, large fines and bad press. As it stands, you’ve done the equivalent of leaving your house with all its windows open; at any point someone can get in.

About the author

Robert Rutherford is Chief Executive Officer of QuoStar, a business and technical consultancy. Founded in 2005, it offers business improvement and technical consulting, outsourcing and cloud services.

www.quostar.com

MISSED CALLS ARE A THING OF THE PAST

Martyn Morgan explains the reasoning behind his firm's decision to use Moneypenny's telephone answering services

By Martyn Morgan, Senior Partner at QualitySolicitors Talbots

Talbots is a multi-disciplinary firm with seven offices across the West Midlands. In early 2014 we took a completely fresh look at the way we handled incoming telephone calls. At that time we had seven receptionists, one in each of our branches, but it was impossible for them to answer every call if they were busy `meeting and greeting' visitors or on another call. We also had no out of hours cover, other than an answering machine which we would respond to the next time we were in the office. Callers had commented that the phone would ring out at times during the day and that we weren't contactable once the office had closed. It was frustrating to realise that we were not only potentially upsetting existing clients, but also missing out on new business opportunities.

Lunchtimes, absences and holidays were an additional headache and were covered via a rota system by other staff who weren't trained receptionists. This not only affected the consistency of the responses we were giving to callers, but it essentially meant that these staff members were being pulled away from their own work. At times we would draft in temporary staff too so it was a tricky scenario to manage and we decided to set about a complete front of house overhaul.

I'd seen Moneypenny at numerous conferences and exhibitions over the years and I had heard glowing endorsements from other firms using its services. Prompted by our need to change our system, we made our approach to Moneypenny, with the realisation also in mind that we needed to address our entire culture with regard to the way we handled calls.

We took advantage of Moneypenny's no-obligation trial, to pick up any calls we weren't reaching ourselves, which highlighted just how many calls we were missing, as well as providing a host of other data. This gave us invaluable business insights around our call trends and patterns. We were immediately convinced that this was the way to go.

This new way of doing things, with Moneypenny as our telephone answering partner, meant that we would not only relieve the pressure on our own reception desks but would have the additional capability to have our calls answered professionally out of office hours, on Bank Holidays and on Sundays – effectively any time of the day or night, thanks to the novel way Moneypenny's UK receptionists dovetail with their colleagues in New Zealand, who answer night-time calls during their daytime.

We also liked the idea of setting up a brand new line, dedicated to new business enquiries which we could market in its own right and that could be handled entirely by Moneypenny. Our Moneypenny Receptionist Kate (supported by her small team of three, who also know our business well) is a legal call specialist and has seamlessly integrated with our own staff. In fact we just think of her as one of us. She has a great rapport with our team and our clients, and we know that we can speak to her anytime to ask questions or to fine tune anything.

The bar is very high in terms of client expectations. Customers expect a fast, professional response, so we have to get it right. It can seem daunting making changes, but moving away from the traditional set up is the best thing we could have done.

We now know we are capturing every call, and that's worth its weight in gold. All messages are emailed to us straight away which means we can respond to urgent enquiries any time. I was walking my dog early one Saturday morning when an email from Moneypenny popped up on my phone – we'd had a call from a client who was upset. I called her back straight away and was able to turn the situation around there and then. If I'd had to wait until Monday to pick that up on an answer machine though, the situation would have been completely different.

The Moneypenny team helps us to deliver first-rate service every time, with flexible support just when we need it. We wonder now how we ever managed without them.

About the author

Martyn Morgan is the Senior Partner, Head of Sales and Marketing and departmental Head of Residential Property at QualitySolicitors Talbots. He's also completed the New York and London Marathons and recently cycled over 500 miles from Bangkok to Phuket.

www.qualitysolicitors.com/talbots
www.moneypenny.com

Next issue of LAWTECH available November 2015

Document Assembly
Software
Employment
Regulations
Security
Outsourcing
Products
Records Management
BPM
Awards
Private Cloud
Briefing
Risk
Data Monitoring
Data
Charity
Conference
Extranets
Recovery
Cost Recovery
Data
Training
Dealrooms
Electronic Forms
Opinion
Internet
Library Management
Customers
HR Software
BYOD
Workflow
Knowledge Management

The word cloud above gives you a pretty good idea of the topics we cover and plan to cover in LawTech magazine. Each month we try to bring you an interesting mix drawn from the above. If you would like to suggest more topics, then please drop the editor a line - david@lawtechmagazine.com.

Thank you. See you in November.