RepKnight

Securing the Law Firm:
Dark Web footprint analysis of 500 UK legal firms

> Has *your* data already left the building?

January 2018

Executive Summary

Legal firms have access to some of the most sensitive data imaginable about their clients – whether corporate or private. And just like any other company, they hold personal information about their employees, such as home address, contact details, bank account numbers and pension information.

But just how secure is the average law firm? Using our BreachAlert platform, we analysed the dark web footprints of domains belonging to the top 500 law firms in the UK, and quickly discovered details of more than 1 million hacked, leaked or stolen credentials being circulated online – that's an average of 2,000 email addresses per firm.

> **The top 500 UK legal firms have more than 1 million credentials exposed online**
>
> *RepKnight, January 2018*

The vast majority of these credentials were exposed through "third party breaches" – a data breach from another website or system unconnected to the law firm, where their employees have signed up using their work email address. These breaches are not the fault of the law firm, and there's no suggestion that the firm's networks have been hacked.

The key findings from our analysis were as follows:

- 620 domains belonging to 500 different law firms were profiled
- Every single law firm had at least 1 credential exposed
- A total of 1.16 million credentials were discovered in data breaches available on the Dark Web, and dump / paste sites.
- More than half of these credentials had been posted in the last 6 months

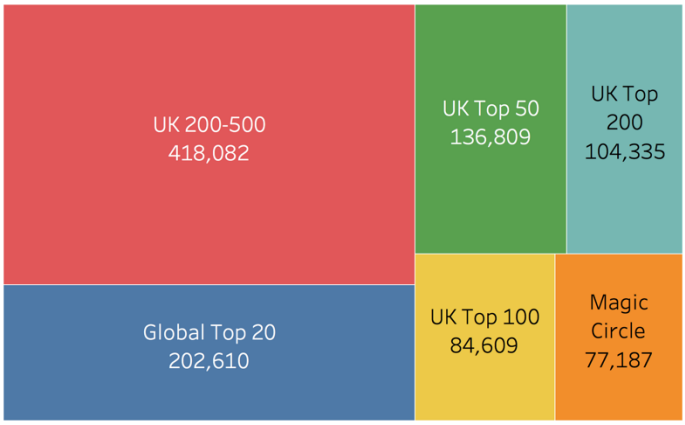

Figure 1 - Number of breached credentials by tier of firm

- More than 80% of the breached credentials also had an associated password – often in cleartext.

With many law firms publishing contact email addresses for their partners and staff on their website, it's relatively easy for spammers and cybercriminals to get an email address. Every exposed email address puts that member of staff at significant risk of phishing attacks and impersonation attempts, as well as the constant plague of spam and malware.

However, almost 800,000 of the 1M+ breached credentials we found also contained passwords. These are often visible as plaintext, or hashed values which are easily cracked online.

This puts those staff – and the law firm's network – at significant risk from "credential stuffing" attacks, where bots are used to repeatedly try the same username and password on multiple sites.

Perhaps more serious are "spear phishing" attacks or identity fraud, where those credentials are used as part of a targeted cyberattack on that individual.

Keeping watch outside the firewall

Most firms quite rightly spend the majority of their time - and IT budgets - worrying about the security of their in-house networks. At RepKnight, we have a different perspective: we think you should be looking after your data, not just your network.

Breaches happen, and they're an unfortunate fact of life. RepKnight's BreachAlert platform continuously monitors the Dark Web, data breach sites, and hundreds of paste and dump sites used by cybercriminals to exchange leaked, hacked or stolen data.

By keeping watch for your data outside the firewall, and instantly alerting you if it's posted online, it's like having a "burglar alarm" for your data. Dark Web monitoring provides valuable peace of mind for your company, staff and clients, and is a key element of any GDPR compliance strategy.

So how does the average law firm score? We decided to find out.

Profiling the top 500 UK law firms

To start with, we focused on the simplest search type: looking for email addresses matching corporate email domains.

We compiled a list of 500 UK law firms from a variety of sources, including the "Magic Circle", the global Top 20 list from Law360, the UK Top 200 from TheLawyer.com, and our friends at i4business. We then categorised each company according to their tier: Magic Circle, Global Top 20, UK Top 50/100/200, and the rest. Finally, we created a list of 620 domain names belonging to those 500 companies, and ran them through our BreachAlert Dark Web monitoring platform.

The results were surprising – in a few minutes we quickly discovered details of more than 1 million hacked, leaked or stolen credentials being circulated online – that's an average of 2,000 email addresses per firm.

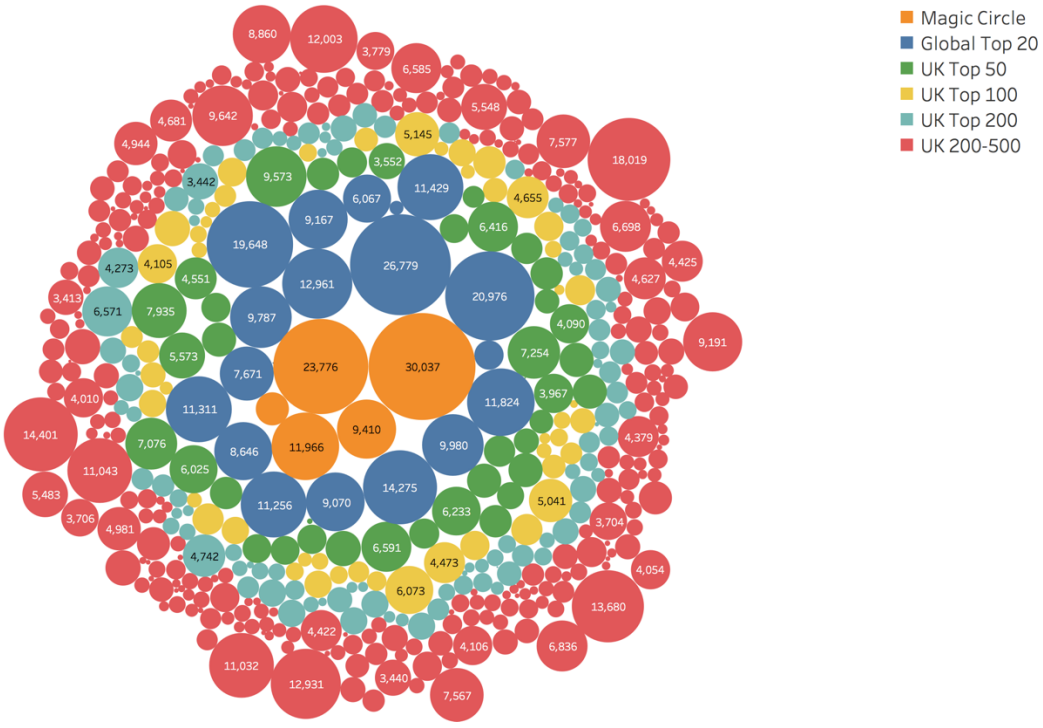

Figure 2 - Number of exposed credentials by firm

Not your fault, but still your problem

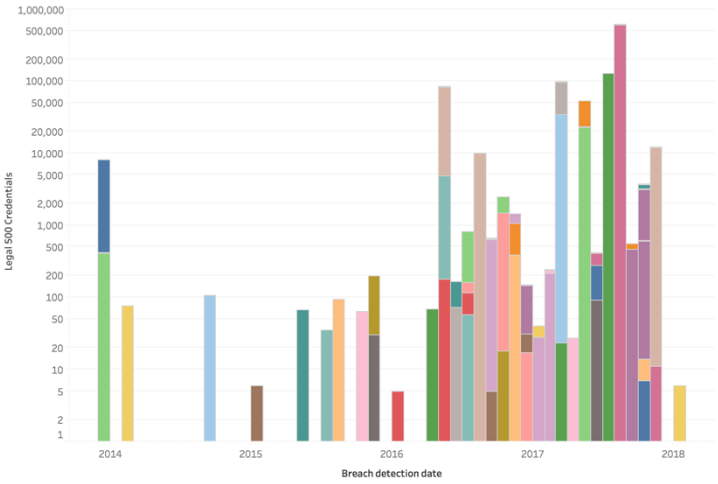

Figure 3 - Breaches featuring top 500 law firms

The vast majority of these credentials were exposed through "third party breaches" – a data breach from another website or system unconnected to the law firm, where their employees have signed up using their work email address.

These breaches are not the fault of the law firm, and there's no suggestion that the firm's networks have been hacked.

Figure 3 gives an indication of the number of different breaches, and how often they occur – multiple breaches are generally detected each month, and it can be seen that the frequency is increasing.

With many law firms publishing contact email addresses for their partners and staff on their website, it's relatively easy for spammers and cybercriminals to get hold of a corporate email address. But every exposed email address puts that employee at significant risk of phishing attacks and "CEO fraud" attempts, as well as the constant plague of spam and malware.

P@ssword1!

Almost 800,000 of the 1M+ credentials we found also contained passwords. These were usually visible as plaintext, or easily cracked hashed values.

Any exposed password – even from a third party site - puts the employee, and the law firm's network, at significant risk from "credential stuffing" attacks, where automated scripts are used to try the same username and password on multiple sites.

Perhaps more serious are "spear phishing" attacks, where those credentials can be used as part of a targeted cyberattack on that individual, or trying to use a variant of that password to access the corporate network.

Corporate emails are the easy bit

This data – which is alarming enough – represents the tip of the iceberg, and is the easiest type of data to find; it is both highly structured (an email address has a unique format) and highly correlated – we only had to search for the email domain name of the law firm.

Much of the really sensitive data in the law firm is a lot harder to search for – the individual email addresses of all your clients and employees; their home addresses, payroll and pension details – let alone unstructured text such as the

	Structured Data	Unstructured Data
Low Correlation (many search terms)	Employee home email addresses	Contracts
	Employee PII	HR files
	Bank account details	Medical Records
	Client contact details	Emails
	CRM database	Project names
Highly Correlated (few search terms)	Server IP addresses	Client names
	Corporate email addresses	Confidential documents
		Company name

Table 1 – Data categories

contents of contracts, wills and other confidential documents.

That's where an automated system like BreachAlert comes into its own – the ability to continuously monitor for a large number of search terms, and instantly alert you if any of those search terms appear online.

Watermarking and fingerprinting

For additional security, we strongly advocate adding "watermarks" to your in-house data sets – these are additional entries which can act as markers if the database is leaked. For example, you can create a fictitious client in your system, and then use their details as search terms. If their email address appears online, you have high confidence that your data may have been breached.

Data sets can also be "fingerprinted" to extract unique characteristics which identify the data as belonging to you – again, these fingerprints can be used as search terms to alert you to a possible hack or breach.

Ease of configuration

With IT security teams continually stretched, it's key to minimise the effort needed to set up and maintain each additional security system.

Because BreachAlert is monitoring outside the firewall, it's not connected to your network, and doesn't require any software to be installed. Securely cloud-hosted by RepKnight, you can easily configure BreachAlert in a few minutes from any web browser.

Summary

Most law firms have thousands of corporate credentials exposed on the Dark Web – each of which represents a possible threat vector to the company or individual. Leaks of sensitive client or employee data are far more concerning, and harder to discover – but put the company at serious risk of reputational damage and financial penalties under GDPR.

Automated Dark Web monitoring provides a simple second line of defence against data breaches, alerting you in realtime if any of your corporate data gets leaked, hacked or stolen, and requires minimal additional effort to set up.

To see how your firm scores in the Legal 500, please contact sales@repknight.com to obtain the full report.

> **Looking for your data appearing "outside the firewall" is an essential component of any GDPR compliance strategy**