Wolters Kluwer

When you have to be right

Cyber Security: a crash course for Law Firms

Learn in this free eBook why Cyber Security will be your problem and cost you money if you don't undertake a bullet-proof security program

Brought to you by Wolters Kluwer

Cyber Security as global scale phenomenon

The huge scandal over the leak of 11.5 million documents from the tax haven Panama and the thousands of global law firms – big and small – that everyday are at risk of being hacked in an attempt to uncover confidential information, put an uncomfortable spotlight on law firms and their data security programs.

While the **Panama Papers** scandal has grabbed headlines around the world, **average cyber-attacks** and everyday data breaches are less talked about but can potentially be equally **devastating**: intellectual property and commercially sensitive information can be very attractive to hackers and, if stolen or lost by unsecure user behavior, can cost quite a lot to your clients in terms of ideas loss and innovation cannibalism.

If you are delegating all your legal firm's data protection strategic decisions to **external IT consultants**, but you want to go the extra mile and be sure you are leveraging the best technology to protect your data from cyberattacks (as well as from natural disasters and unsafe user behaviours), here are some notions that, as client-oriented Lawyer, you absolutely need to know.

Cyber Security by the numbers

Before we dive deep into how to apply a Top Security Program, let's have a closer look at the top data loss cause: Cyber crime is becoming a global phenomenon with implications for the economies across the world.

$ 2.1 trillion

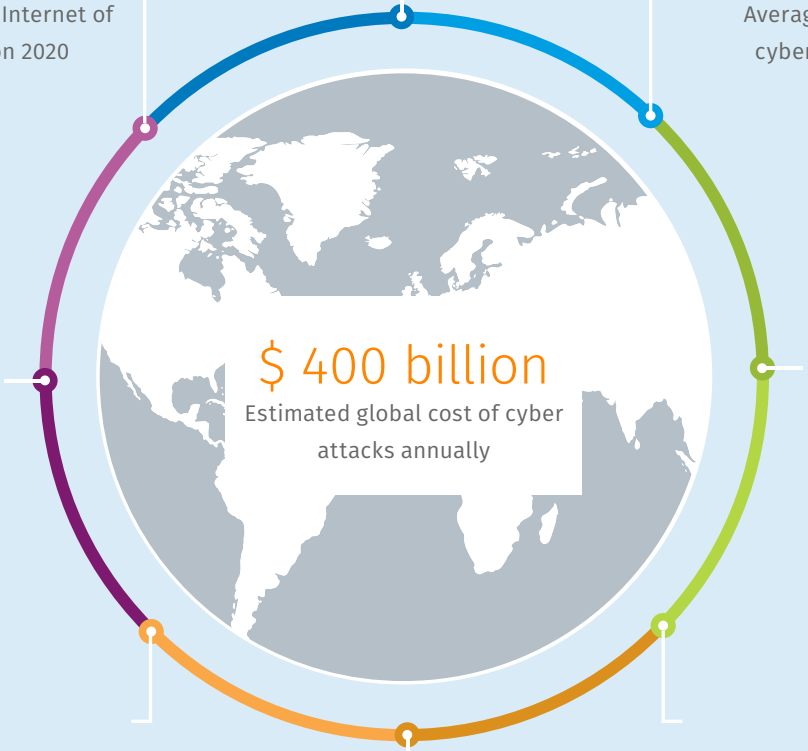
Projected global cost of cyber attacks in 2019

$ 29 billion

Projected market size of the Internet of Things security market on 2020

80-90 million

Average annual amount of cyber security incidents



$ 400 billion

Estimated global cost of cyber attacks annually

$ 179 billion

Projected market size of the global cyber security market in 2020

65%

Percentage of employees that admit to using the same password across business applications

$ 75 billion

Market size in the global cyber security market in 2015

65%

Percentage of business decision makers that believe they will suffer a data breach in the future

70%

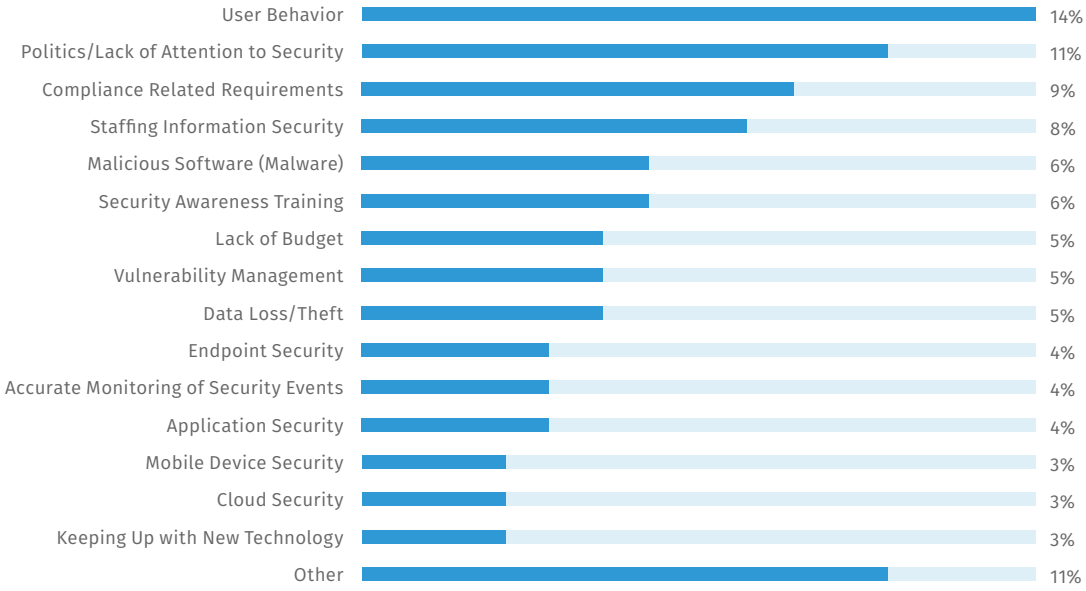
Percentage of cyber attacks that go undetected

Source: expandedramblings.com
Link: http://expandedramblings.com/index.php/cybersecurity-statistics/4/

The internal data security threats in a Law Firm

But external attacks are not the only threat: according to **Legaltech News**, "probably 80% of the intrusions we see are the results of employee carelessness". **NetWatcher** recently published an interesting analysis on the top causes of data loss in both companies and law firms: user behavior and internal poor security hygiene are among the top internal security pain points.

TOP INTERNAL SECURITY PAIN POINTS



NetWatcher Legal eBook | Cyber Security 101:A A ResourceGuide for Lawyers
Source: 451 Research | 451alliance.com/Portals/5/2015reports/121615_security_report/121615_security_report.pdf

Poor **internal data security policies** and the growing phenomenon of cyber attacks can be a lethal combination and inflict a fatal blow to any corporation and law firms.

And it's not only huge corporations that risk to be attacked. According to **Imperva** smaller organizations will continue to fall prey in larger numbers as much as larger ones. If not even more.

This is becoming a problem of huge proportions and data breaches at law firms today are indeed on the rise. Furthermore, beyond the risk of a hacking incident, law firms are vulnerable to data breaches from within: think of a lost or stolen laptop or of internal staff misappropriating or misusing confidential client data.

In order to defend their data, law firms need to invest in security. Only those in a position to guarantee their data security will earn a strong reputation of excellence and will continue to be recognized among the best to work with by General Counsel, who will choose them to take care of their business. Furthermore, implementing adequate data security is not only a sound business practice, but also a legal and ethical duty for a lawyer.

Top 10 actions for a Top Security Program

Most firms already rely on competent external IT consultants and employ common security tools such as firewalls rule sets, network security systems, spam-filters and virus scanners. The latter are essential measures a law firm should not live without, but are by no means sufficient. Law firms should establish a **true culture of security** and **data protection** among lawyers and staff members by establishing **strong policies and protocols** but also by empowering them with knowledge and tools. Find out now if your law firm is vulnerable to cyber-attacks or poor user behavior and what needs to be done to prevent data breaches and loss.

1. Are your servers secure enough?

If you want to sleep at night and be certain that data are properly secured against hackers and other threats, you should think of a cloud-based solution: **in the cloud** your data reside far away from any environmental disaster, protected from external instusions and automatically backed up 24/7. If you opt for this solution, ask for evidence of third-party security certifications.

2. Did you implement a strong password policy?

A strong and common password policy is the first important step a law firm needs to take to protect sensitive data. It should be at least 12/15 characters long, contain upper and lower cases and a combination of letters, numbers and symbols. Forcing users to **change passwords periodically** and not allowing them to use the same one more than once is also a strong best practice.

3. Are your data encrypted?

Are you sure that your data are correctly encrypted, and hence protected from interception, when transferred between your computer and another one (a cloud-based server, for example)? You should ask for **evidence of data transmission being encrypted** with a 2048-bit PKI Certificate and certified by a third-party security auditing provider.

4. Are you protecting your data from fire, floods and other disasters?

There are good two ways to protect your data from fire and other disasters:
You can store your data on fireproof external drives. They are extremely robust and can offer protection from water and fire. They are not infallible but can offer good protection.
You can store your data in the cloud. This way if your laptop is lost or stolen or your building is severely damaged, your data will be stored real-time on a remote server.

5. Are you protecting your data when connecting outside of your firm?

Strong internal wireless protocols should be installed. When working outside of own law firm's premises, however, lawyers must exercise caution: free networks (in restaurants, at the airport, in stores) are not secure and should always be avoided. Alternatively, you should rely on a **trusted, cloud-based legal practice management system** that stores, protects and synchronizes all your data real-time through any device, anywhere.

6. Are your external personal devices secure?

Many law firms today have "Bring Your Own Device" policies that enable staff members and lawyers to access the firm's network and download sensitive data onto their own devices. Everyday sensitive legal data move across the firm's network, through emails, dropbox and external devices. Firms should regulate the use of and gain ultimate control on such devices: remote location-tracking application, automatic data-deletion software, data encryption and password protection measures will do the trick. Or, in order to be in total control of your data, **you should consider adopting a cloud-based data management system** that synchronizes all your communications, email threads and documents across the different devices in use in your firm, inside as well as outside your network.

7. Are your computer clients secure enough?

Though cloud computing can guarantee data security, you need to ensure that your desktops and laptops are **properly protected with an antivirus, a firewall and the latest operating system and web browser security updates**.

8. Did you already obtain a cyber risk insurance?

Law firms should consider **cyber liability insurance** for the value of risk (damage, disruption, etc.) that cannot be mitigated. This could make the difference between a law firm surviving the potentially devastating financial impact of a data breach and one succumbing.

9. How reliable are your current IT and security consultants?

Law firms need to create a **cyber-aware culture across their entire organization**, including third-party vendors: even the latter can be a vulnerable point of attack. If you are leaning on outsourced IT and security management services to host, manage, maintain and support your network, servers, desktops and applications, you should consider protecting your firm through written confidentiality agreements when vendors are storing, transporting or analyzing sensitive client information. Strict user-level permission protocols should also be observed.

10. How well-trained is your legal staff?

Security is everybody's direct responsibility. Lawyers as well as non-legal staff members should be all regularly trained on **basic confidentiality matters**, the **evolution** of **cybersecurity trends** and **best practices**. They should also be instructed on the policies and practices the firm expects them to follow on a daily basis. Periodic training sessions should be conducted.

Legal Professional Cyber security is Top of Mind for Wolters Kluwer

In the legal industry, **security of information is paramount**. If you don't know from where to start to **manage your law firm's workflow** in total, you should start considering to adopt a **cloud-based end-to-end practice-management software tool** that gives lawyers access to all their clients' files, anywhere, at any time, creating a flexible and secure virtual office in the cloud.

Your vendors should be true experts in data protection and cyber-security but also be knowledgeable with the specific needs and procedures of a Law Firm. You should consider choosing a **partner** that knows your work, your issues and your goals. Entrust a reliable and specialized partner with your data protection, security and staff training matters. Lawyers should spend their time in being lawyers.

Wolters Kluwer customers rely on us to support their efforts to be responsive to these types of issues in a myriad of ways.

If you want to find out more about Wolters Kluwer cloud-based Legal Solutions, visit our website: kleos.wolterskluwer.com