Infusion Lawyers

Your Partner in Innovation

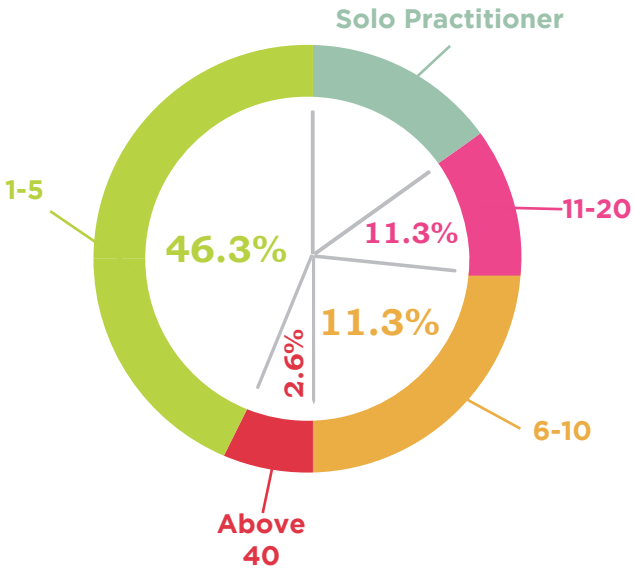
CYBER SECURITY FOR LAWYERS AND LAW FIRMS: TACKLING CYBER RISKS AND DATA BREACHES.

METHODOLOGY

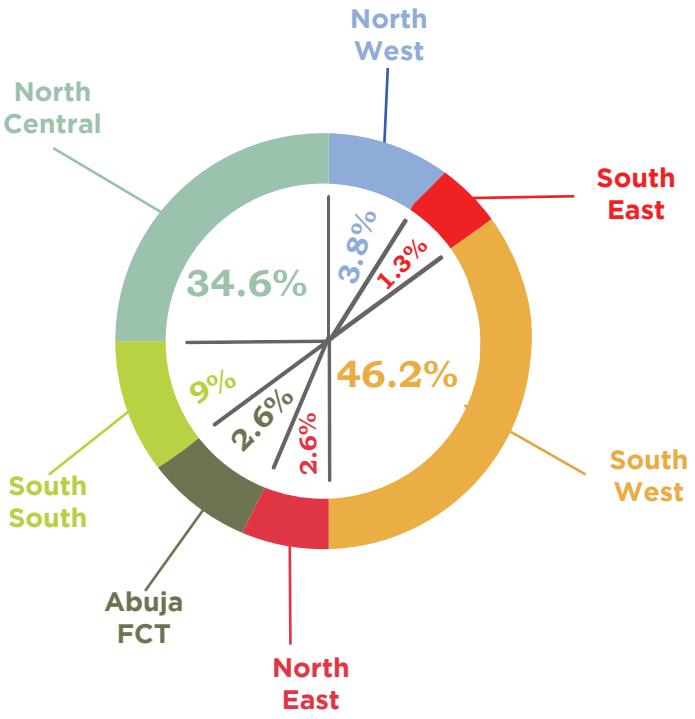
This is a study on Nigerian law firm's cybersecurity and data protection hygiene. The data represented in this study is a compilation of data by the author and gathered through an online anonymized survey. The data points were specifically selected to accurately reflect both the cybersecurity threats and current efforts taken by Nigerian lawyers and law firms to limit the risks of cyber exposure or breach. In the course of compiling this report, the author surveyed and assessed over 200 Nigerian lawyers located in Nigeria and having a full-time practice in Nigeria. The purpose of this study is to create awareness in the Nigeria legal community of the risk of data breaches and the need for data protection.

Keywords:
Law Firms, Lawyers, Cybersecurity, Data Breach, Cyber-attack, Policies.

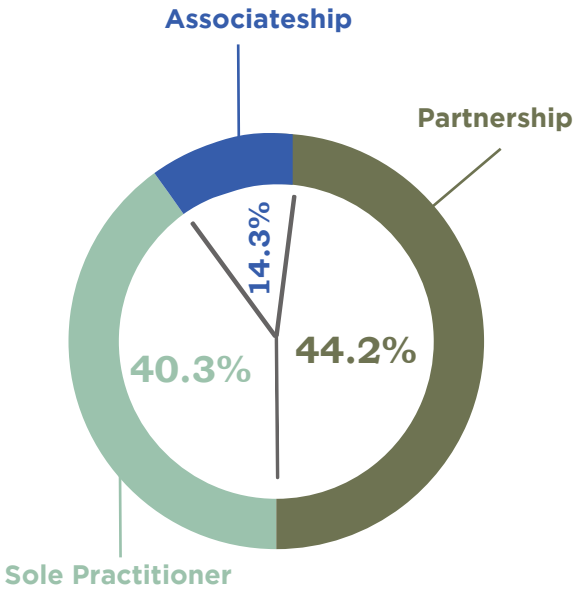
Law firms represented by Size



Location of Law firms



Types of Law Firms



Some Key Findings

- 71 percent of firms do not have formally documented cyber-security policies.
- 10 percent of firms strictly implement their cyber-security policies.
- 87 percent of lawyers use their personal laptops, phones, thumb drives, apps and emails for work-related purposes instead of the firm's approved devices, apps and emails.
- 72.3 of firms do not see cybersecurity as a major challenge.
- 90 percent of firms do not have existing cyber-insurance coverage in the event of a data breach.
- 74 percent of lawyers have never changed passwords to their official email addresses.
- 62 percent of lawyers open attached documents from unknown sources.
- 90 percent of firms do not have a dedicated IT department that ensures data security.
- Most firms lack the awareness or the right infrastructure to effectively protect their clients' data, thereby making them vulnerable and unprepared to tackle data breach.

INTRODUCTION

Cyber-attacks and data breaches have become a thing of concern to every individual and organization. With more data being stored online, the threat that cybercriminals pose has never been greater. We wake up every day reading newspaper headlines or seeing and hearing news about data breaches around the world. It can happen to anyone and any type of organization. These data breaches are occurring at an increasingly alarming rate with most victims blissfully ignorant about a breach. It is safe to conclude that these data breaches cut across every sector and;

The Nigerian legal sector is also not left out from the prying eyes of cybercriminals. Nigerian law firms are a vital component of Nigerian businesses, having in their control and possession personal, business-sensitive, and commercially-sensitive information[1]. This makes them an attractive target for cybercriminals. As lawyers, we should not be misled into believing that data breaches are only a problem for others and not law firms. More dangerous is the belief that your law firm is well protected from any forms of data breaches, or that it is a concern for the top tier law firms in Nigeria. Small law firms and solo lawyers are also becoming constantly vulnerable to all forms of data breaches. Lawyers operating small law practices and solo lawyers should not take comfort in the illusion that they are too small to be victims of cyber-attacks. It-won't-happen-to-me mentality is overly misguided. If DLA Piper[2], a multinational firm that has touted its expertise in cybersecurity, was hit by NonPetya, and as reported by ABA Journal[3] of 6 major law firms that have been hit by cyber-attacks, you or your law firm could be next.

[1]DLA Piper statement on malware attack. https://www.dlapiper.com/de/germany/news/2017/06/dla-piper malware-statement. Retrieved February 9, 2019
Julie Sobowale, 6 Major Law Firm Hack in Recent Hinstroy. www.abajournal.com/magazine/article/law_firm_hacking_historyReterive 10, 2019
[2]Symantec Internet Security Threat Report Volume 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. Retrieved February 9, 2019
[3]Natasha Turak, The next 9/11 will be a cyberattack, security expert warns, https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html. Retrieved February 9, 2019.

WHY ARE LAW FIRMS THE NEW TARGET FOR CYBER-CRIMINALS?

It is no news that the vast majority of Nigerian lawyers and law firms are not highly sophisticated in the use of technology. This makes it easy for hackers to have unauthorized access to clients' sensitive information. The following reasons are why law firms have now become a suitable target and treasure trove for hackers:

1. Nearly every industry in the country, large and small, works or has something to do with a law firm in at least one capacity or the other. In doing so, Nigerian law firms have in their custody and control, sensitive and valuable client information. Essentially, today's law firms have become a vault of sensitive and valuable information such as:

- Client's intellectual property such as trade secret, copyright, and information regarding prospective business deals;
- Litigation tactics and strategy;
- Clients confidential business information;
- Attorney-client privileged legally privileged information and communications;
- Clients personally identifiable information (PII);
- Clients financial details and account access information;
- Clients personal health information;
- Corporate financial reports;
- Proprietary software code;
- Emails and other communications with clients.

All the above-listed information are incredibly valuable on the black market.

2. Secondly, Nigerian law firms and its lawyers are ill-prepared as far as facing these evolving threats are concerned. Despite growing cyber-security threats, majority of law firms and lawyers still lack the proper and requisite awareness, knowledge, policies, procedures, and precautions to establish a proper individual or organizational cyber hygiene and defense.

Why Is Cyber Security So Important And Why Should Lawyers And Law Firms Be Concerned?

According to a 2016 report by Symantec, the threat of email hacking and malware is growing. Between 2014 and 2015, the amount of new malware grew from 317 million to 431 million. Crypto-ransomware attacks rose from 269,000 to 362,000. Web attacks also grew in the same timeframe from 493,000 per day to 1.1 million per day[4].

Therefore, the need for Nigerian law firms to pay more attention tocybersecurity is perhaps even more vital than boosting profitability and expanding clientele. With law firms in control and possession of clients' sensitive and valuable information, they have an arduous task to keep this information safe and secured from unauthorized access. The law firm's cyber hygiene forms part of the big picture when it comes to providing excellent, efficient service and peace of mind to clients. The risk of a cyber-attack should not be ignored because there are no expectations that these trends will reverse anytime soon[5]. Law firms will need to take proactive action to ensure that they protect their clients and themselves as much as possible by taking a number of steps to protect their firms and their client database.

If law firms are not able to safeguard thesensitive and valuable information in their custody, control, and possession, they are definitely leaving their doors open for possible cyber-attacks. And when this happens, not only will the firm's reputation be damaged, such law firm or lawyer could also face legal action for not putting in place reasonable steps to prevent the data breach resulting in clients' sensitive and valuable data ending up in wrong hands. The core of the law firm's business, integrity and livelihood will also be negatively impacted; downtime and billable hours will be lost; files will be lost, destroyed, or otherwise corrupted; a huge amount of money will be spent on recovering from the data breach; and the lawyer might lose his or her practice license.

[4] Natasha Turak, The next 9/11 will be a cyberattack, security expert warns, https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html. Retrieved February 9, 2019.
[5] Barney Thompson, DLA Piper still struggling with Petyacyber-attack, https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895. Retrieved February 9, 2019.

What Kind Of Threats Do Law Firms Face?

Having shown above why Nigerian law firms are targets of cybercriminals, it is vital that the legal community have a good idea about the various shapes the cybersecurity risks and threats they face take. These cybersecurity risks and threats are constantly evolving in the global landscape. However the shape they take, any of these threats can cause irreparable damage to a law firm. Some of thethreats faced by law firms are:

a. Malware or malicious software: this is hostile or intrusive software which is employed by cyber-criminals to compromise information systems and network. These include viruses, worms, Trojan horse, ransomware, spyware, adware, scareware, and other variants of malicious software programs. Malware can take the form of executable code, script, active content and other variations of software.

b. Ransomware: This type of malware locks down a computer and threatens to shut down the system unless a ransom is paid. This is what infected the DLA Piper system in June 2017[6].

c. Virus: A virus uses code written with the express intention of replicating itself. A virus attempts to spread from one electronic device to another electronic device by attaching itself to a host program[7].

d. Worms: Worm uses self-propagating malicious code that can automatically distribute itself from one computer to another through network connections[8].

e. Trojan horse: This is a program that appears useful or harmless but which contains hidden code designed to exploit or damage the system on which it runs. This type of malware discretely creates backdoors which allow hackers or other malware to enter your system .

f. Spyware: Just as the name suggests, spyware is software used to spy on you. This includes recording your keystrokes to learn your passwords or secretly using your camera to watch you[9].

g. Phishing attacks: This is an attempt to obtain sensitive information or gain unauthorized access to client information or funds by masquerading as a trustworthy source via email[10].

h. Website Vulnerabilities: Cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, as website administrators fail to secure their websites. Nearly 75 percent of all legitimate websites have unpatched vulnerabilities[11].

[6]TLP White, An Introduction to Malware. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/An-introduction-to-malware.pdf Retrieved February 9, 2019.
[7] https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html. Retrieved February 9, 2019.
[8]Kunkun Wang, Xiaoyu Chen, YeshengXu. A Brief Study of Trojan. https://cdn.ttgtmedia.com/searchSecurity/downloads/Malware_Ch06.pdf Retrieved February 9, 2019.
[9]Daniel Jonasson, Johan Sigholm, What is Spyware. https://pdfs.semanticscholar.org/5779/5aaa5fbbd931b21ab7c11b83b6e305ce35cd.pdf Retrieved February 9, 2019.
[10]National Cyber Security Centre. Phishing Attacks: Defending your organisation. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Phishing%20Attacks%20-%20Defending%20Your%20Organisation.pdf Retrieved February 9, 2019. S. Zanero Ph.D. Student, Politecnico di Milano T.U. CTO & Co-Founder, Secure Network S.r.l. Automatic Detection of Web Application Security Flaws. https://www.blackhat.com/presentations/bh-europe-05/bh-eu-05-zanero.pdf Retrieved February 9, 2019.
[11]Rules of Professional Conduct for Lawyers 2007. Rule 14(1) & 19(1) & (4)

Apart from the targeted and specialized attack mentioned above, data breach of law firm's confidential and sensitive information can also occur through other means such as:

- Insider threat in the form of a negligent or rouge staff or lawyer who has complete access to the firm's sensitive and valuable information. Such rogue might sell, misuse or manhandle vital information obtained through this means;
- External threats: This could be in form of competitors or a foreign government interested in disrupting the law firm's legal operations, steal information or who are interested in espionage;
- Loss of an unsecured laptop or mobile device;
- Visiting questionable websites;
- Communications over unsecured and public networks;
- Downloading unapproved software onto the law firm's computer network or onto a mobile device, which connects to a repository of confidential firm information;
- Security issues with third-party providers and cloud system;
- Hacktivists;
- Weak or non-existent password management being weak or non-existent;
- Use of outdated technology e.g. Microsoft Windows XP.

Ethical and Legal Responsibilities of Lawyers and Law Firms.

Lawyers can no longer afford to treat cybersecurity as an afterthought. Rather than being reactive, lawyers must learn to be more proactive. Lawyers have an ethical and professional obligation to ensure that clients' sensitive and valuable information is protected from unauthorized access. The ethical standards for ensuring lawyers and law firms protect and maintain the confidentiality of clients' information is provided in Rule 14(1) and 19(1) & (4) of the Rules of Professional Conduct for lawyers 2007 . It states as follows:

> *19(1) Except as provided under sub-rule (3) of this rule, all oral or written communications made by a client to his lawyer in the normal course of professional employment are privileged.*
>
> *(4) A lawyer shall exercise reasonable care to prevent his employees' associates and other services are utilized by him from disclosing or using confidences or secret of a client, but a lawyer may reveal the information allowed by sub-rule (3) through his employee.*

A close reading of the above rules shows that a lawyer must act competently in protecting the confidentiality of its client's information. A lawyer's duties of confidentiality and competence require that he or she takes appropriate steps in ensuring that the use of technology in conjunction with client's representation is not subject to undue risk or unauthorized disclosure.

WHAT CAN LAW FIRMS DO?

Now that we are aware that cyber-criminals are interested in having access to the sensitive and valuable data law firms have in its possession and control, we have the responsibility of combating these threats. Here are a few recommended mechanisms or actions which can be applied in combating cyber breaches in Nigerian law firms:

a. Employer and Employee Awareness Training, and Education: Cybersecurity awareness training and education help firms' staff and lawyers understand the ethical and professional responsibilities they have in ensuring data protection .They also need to be vigilant. These training should be conducted periodically and should be mandatory for all. (It is within the human nature the possibility of reverting to our old habits that may put data security at risk.)

b. Keeping Hardware and Software up to Date: It is important to update the law firm's hardware and ensure it is running on the latest software version. These updates keep your network and devices safe from vulnerabilities.

c. Encryption of all portable devices and valuable data: They say encryption is the acid test of seriousness. All hardware's including mobile devices that contain the firm's valuable data and confidential information should be encrypted every time data is transmitted into or outside of the firm. Ensure that lawyers and other staff do not leave workstations unattended without locking devices.

d. Password Policy and Multi-factor authentication: Firms should have a policy that mandates lawyers and other staff to change passwords after a certain period of time and such password should contain characterizations consisting of numbers, letters, and special characters. Lawyers and other staff should be encouraged to use at least a two-factor authentication password.

e. Law firms must have up-to-date and clearly written cybersecurity policies and backup procedure: Law Firm's cybersecurity policies should be documented, accessible, understood and implemented by all employees. These policies should be reviewed, maintained and revised on a periodic basis and should be updated at least once annually to stay on top of technology best practices. Some of these policies are incidence response, computer use, password policies, backup procedures etc.

f. Conduct regular vulnerability and penetration testing: This determines the weakness in the law firm's application (software), infrastructure (hardware) and people in order to ensure that the controls and policies put in place are implemented and effective. Vulnerability and penetration testing should be done on an annual basis.

g. Have a cyber-liability insurance policy: A proper cybersecurity insurance policy should include reimbursement for investigation, business loss, required notification and credit monitoring to clients, legal expenses, cost of extortion and cover human error where possible.

h. Hiring the right cybersecurity personnel: Have a cybersecurity personnel who will be responsible for establishing and maintaining a comprehensive cybersecurity vision and strategy for your law firm. They will to enforce policy formulation and implementation. This will help ensure that valuable assets, technologies, and systems are adequately protected.

CONCLUSION

Cyber threats are real and growing daily. For many Nigerian lawyers, law firms (big or small), or solo lawyers, cyber security is always an afterthought, and that's if we even have the time to bother about it. More attention is often directed at bringing in new clients and skyrocketing the law firm's profits margin. We still practice the habit of carrying sensitive information on insecure thumb drives, using unencrypted email on the insecure electronic device, and using unsecured shared networks. This is highly risky and not consistent with the legal client's best interest.

It's about time we started implementing sound cybersecurity and data security practices as an essential business practice for our law firms. Protecting client data as well as the firm's data should be top priority for law firms of all sizes. Whether we like it or not, we are by the very nature of our profession bestowed with the obligation of safeguarding our clients' sensitive and valuable information. Law firms that chose to ignore this and fail to devote the right attention and proper resources to protect their client's sensitive and valuable information do so at their own peril.

Yes, we were not trained in school to be aware of the evolving cybersecurity threats and data breaches. Notwithstanding, there is a growing need for us to educate ourselves about these evolving threats. This can only be achieved by making a conscious effort to educate ourselves and our colleagues about these threats and data breaches, and how we can stay protected. We also need to create plans in case of emergencies since there is no way we can perform legal tasks or provide legal services without using one form of technology or another or at least collecting personal data from their clients.

The bottom line is, if cyber-attacks are not going anywhere anytime soon—and they are not—then lawyers and law firms should also do away with their notoriously outdated, conservative and slow-to-change behavior towards cybersecurity hygiene. Beef up your security measures. Educate your employees, and communicate and report any cyber-attacks that do occur to keep everyone aware. It is legal.

REFERENCES

1. Mosadoluwa Adeleke, Cyber Security: A Critical Need for Law Firms in a Digital Age. https://www.lawyard.ng/cyber-security-a-critical-need-for-law-firms-in-a-digital-age-by-mosadoluwa-adeleke/ Retrieved February 9, 2019.

2. DLA Piper statement on malware attack. https://www.dlapiper.com/de/germany/news/2017/06/dla-piper malware-statement. Retrieved February 9, 2019.

3. Julie Sobowale, 6 Major Law Firm Hack in Recent Hinstroy. www.abajournal.com/magazine/article/law_firm_hacking_historyReterive 10, 2019.

4. Symantec Internet Security Threat Report Volume 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. Retrieved February 9, 2019.

5. Natasha Turak, The next 9/11 will be a cyberattack, security expert warns, https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html. Retrieved February 9, 2019.

6. Barney Thompson, DLA Piper still struggling with Petyacyber-attack, https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895. Retrieved February 9, 2019.

7. TLP White, An Introduction to Malware. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/An-introduction-to-malware.pdf Retrieved February 9, 2019.

8. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html. Retrieved February 9, 2019.

9. Kunkun Wang, Xiaoyu Chen, YeshengXu. A Brief Study of Trojan. https://cdn.ttgtmedia.com/searchSecurity/downloads/Malware_Ch06.pdf Retrieved February 9, 2019.

10. Daniel Jonasson, Johan Sigholm, What is Spyware. https://pdfs.semanticscholar.org/5779/5aaa5fbbd931b21ab7c11b83b6e305ce35cd.pdf Retrieved February 9, 2019.

11. National Cyber Security Centre. Phishing Attacks: Defending your organisation. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Phishing%20Attacks%20-%20Defending%20Your%20Organisation.pdf Retrieved February 9, 2019.

12. S. Zanero Ph.D. Student, Politecnico di Milano T.U. CTO & Co-Founder, Secure Network S.r.l. Automatic Detection of Web Application Security Flaws. https://www.blackhat.com/presentations/bh-europe-05/bh-eu-05-zanero.pdf Retrieved February 9, 2019.

13. Rules of Professional Conduct for Lawyers 2007. Rule 14(1) & 19(1) & (4)

Moses Malan Faya

Senior Associate

Infusion Lawyers

Your Partner in Innovation

A Virtual Intellectual property and Information Techonology law firm for the knowledge economy and the digital age

+2347038690044

malan@infusionlawyers.com

www.infusionlawyers.com