

ARTICLE SERIES

LAW FIRMS AS TARGETS FOR HACKERS – RISKS AND THE WAY FORWARD

FEBRUARY 2021



word write. Welcome

```
height: auto;
width: auto;
padding: 10px;
border: 1px solid #ccc;
border-bottom: 2px solid #ccc;
```



```
443100...
110423...
110431...
us12...
435...
other...
"smart...
abled", "father...
,ooseong_test_gro...
"athersdayus" enabled...
red_wall_story_funnel" collect...
aggregated_engagemen...
interstitial
```



INTRODUCTION

CKED

...img?x=...&y=...&w=...&h=...&...jpg



INTRODUCTION

The growth in technology has led to a sudden shift in the storage of information from physical storage systems to online storage platforms. Individuals and organisations are now beginning to save their information online and the reasons for this development are not farfetched.

Amongst several advantages, online storage of information appears safer compared to traditional methods, as such information stored online cannot be wrecked by environmental hazards such as fire or natural disasters including storms and earthquakes.

Furthermore, it makes such information easily accessible for those that are entitled to access them. The outbreak of COVID-19 has also encouraged and facilitated an increase in the online storage of information by individuals and organisations. This is mainly as the various lockdown orders halted the movement of goods and persons and as a result, several organisations and businesses have had to work and operate remotely. To be able to access relevant data and work effectively, while working remotely, these organisations have had to adopt several digital means of storing its relevant data.

However, the storage of information through online and digital means does not occur without some challenges. Indeed, with the increase in online and digital storage of information, cyber-attacks and data breaches by cybercriminals are now a very common phenomenon in the world today. And these cyber-attacks mainly occur without the knowledge of their victims. Additionally, the cybercriminals either utilise these access and information they get, for their personal use or sell them to other persons who may be in need of them. For example, threat intel firm, Group-IB reports that the sales of access to compromised corporate networks grew fourfold in 2020.[1] It therefore appears that the sale of access gained by cybercriminals to the data of some corporate organisations and entities have become a lucrative venture.

[1]Network hacking and ransomware fueling global cybercrime surge by John Leyden (accessible via <https://portswigger.net/daily-swig/network-hacking-and-ransomware-fueling-global-cybercrime-surge>)



THE PECULIARITIES OF THE LEGAL SECTOR

THE PECULIARITIES OF THE LEGAL SECTOR

In Nigeria, the legal sector is not left out of the odious ventures of these cybercriminals as law firms are a vital part of society. First, they have in their possession and control, commercially sensitive and privileged information, as almost all sectors in the country involve the services of lawyers in their operations and transactions. These transactions have given Nigerian lawyers and law firms access to salient and privileged information of these business entities that they work for.

The information with law firms that are attractive to hackers include intellectual property information (such as trade secrets, patents, industrial design and copyrights), corporate financial reports of clients, financial details (including account access information), confidential and privileged business information of both the law firms and their clients, relevant information relating to their clients' criminal activities, personally identifiable information (PII) of both law firms and clients, proprietary software codes, the personal health information of individual clients, emails and other forms of correspondences.

Ironically, despite the potential cyber threats being posed by cybercriminals and the tendency for law firms to be targets, there appears to be the narrow-minded belief that law firms are hardly targeted or that if such threats exist, then they are problems of the magic circle or top-tier law firms. However, in reality, small law firms and sole practitioners have become vulnerable targets of cybercriminals. As a matter of fact, the issue of cyber breach and attack of law firms was raised in a 2020 ABA Legal Technology Survey Report that revealed the percentage of law firms experiencing a known security breach stood at 29% in 2020.

Furthermore, DLA Piper, a multinational law firm with solid expertise in cyber-security was also hit by the popular Notpetya Ransomware attack. This should serve as sufficient warning for both law firms and lawyers, on the issue of cyber-attacks and data breaches. Consequently, the need to establish protocols, procedures, policies and precautions that guarantee cyber hygiene for both lawyers (involved in sole practitionership) and law firms cannot be overemphasised.

TYPES OF CYBER THREATS/BREACHES

TYPES OF CYBER THREATS/BREACHES

It is salient for these law firms to have an idea of the possible cybersecurity risks that they are highly susceptible to. Though cyber breaches can occur in various forms, the ones that commonly affects law firms include:

1. Ransomware

It is a type of malware from cryptovirology. It threatens to release and publish its victim's data or block access to it in perpetuity unless a certain sum is paid. It is quite common and infected DLA Piper's system in June 2017.[2]

2. Virus

A virus uses written codes that it replicates. It also attempts to spread from one device to another by attaching itself to a host program.

3. Worm

It is a standalone and self-malicious program that replicates itself in order to spread to other programs.

4. Malware

A software that is intentionally designed or formulated to damage, disrupt or gain unauthorized access to a device. It is often utilised by hackers to compromise information systems.

5. Spyware

It is a software that enables its user spy on other computers. It enables its user to obtain covert information about the activities and actions of other computers. It does this by simply transmitting data in a covert manner, from their hard drive.

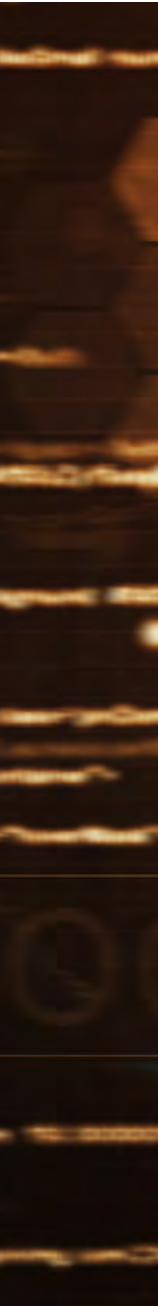
6. Trojan Horse

A type of malware that often confuses computer users of its true intention. It usually appears useful or even harmless. However, it contains hidden codes designed to exploit or damage any device which it runs on.

7. Phising Attacks

This is a type of social engineering that disguises as a trustworthy entity in an electronic communication (mainly by mail), in order to steal user data, including login credentials and credit card numbers.


[2] DLA Piper set to sue insurer over Notpetya Claim: Report (published on infosecurity-magazine.com)



It operates in such a way that it dupes its victims into opening an email, instant message or text message, just to get relevant data from the user.

Other factors that can also contribute to cyber breaches include:

- External and internal threats (such as recklessness of certain members of staff).
- Website vulnerabilities
- Security issues with cloud systems
- Security issues with other third-party providers
- Weak password management
- Utilization of outdated technology
- The activities of Hacktivists.



In the second part of this article, we will be looking at ethical issues that may arise following a breach, particularly with regards to the provisions of the Rules of Professional Conduct (“RPC”) and providing recommendations that can be adopted to forestall breaches.

**THE IMPORTANCE OF
CYBER HYGIENE TO
LAW FIRMS AND LAWYERS**



THE IMPORTANCE OF CYBER HYGIENE TO LAW FIRMS AND LAWYERS

According to a recent report, email malware creation increases by 26% year over year, with about a million malware threats created every day[3]. Additionally, between 2014 and 2015, the number of new malwares that emerged grew from 317 million to 431 million. By 2016, a breach of more than 11 million confidential and privileged documents which included emails, databases, files, PDFs and thousands of text documents, occurred as a result of an attack on Mossack Fonseca law firm. Based on the reports released by security researchers, there were multiple reasons for the success of the attack.

These reasons included external-facing servers running outdated software while missing critical security updates. This suggests that the Mossack Fonseca law firm did not have adequate cyber hygiene protocols and procedures as there was a clear lack of visibility across the firm, as well as missing patches and vulnerabilities including poor network segmentation.

This clearly indicates that the worst cyber breach is often a result of poor cybersecurity. [4]

To this end, law firms and lawyers need to pay more attention to their cybersecurity. With the growing rate of cyber breaches, law firms cannot afford to be careless with the information of their clients within their possession. Procedures and protocols must be established by these law firms to ensure cyber hygiene.

For the purpose of clarity, cyber hygiene underscores a successful incident and threat management program that keeps computer systems up to date, promotes full visibility and guarantees data protection.

It includes a range of procedures and protocols that helps to maintain best practices in keeping sensitive data safe from external attacks. It also helps to ensure compliance with the latest security standards.[5]If a proper cyber hygiene procedure is not put in place, then the valuable and sensitive information in the possession of these law firms may be tampered with by cybercriminals.

[3]5 Facts on Email Security Threats inc 2021 (published on Mailbird Blog).

[4]Law firms as prime targets for hackers: 7 Steps to reducing cyber risks by Aniket Bhardwaj, Charlse River Associates (Published on Lexology).

[5] Ibid.

This will affect the integrity of the firm and may also result in some legal actions being taken against the law firm.

Additionally, ethical issues may also arise, particularly with regards to the provisions of the Rules of Professional Conduct (“RPC”) which vests with legal practitioners in Nigeria, an ethical and professional obligation to make sure that valuable and sensitive information of clients are protected from unauthorised access and they are kept confidential[6].The provisions of Rule 19 (1) – (3) of the RPC is clearly to the effect that a lawyer has a duty to ensure that whatever information that is disclosed to him by his client, is not divulged to another person, except:

- with the consent of the client (upon full disclosure to them);
- where such lawyer is required to disclose any relevant information on grounds of law or by an order of the court;
- where the intention of the client is to commit a crime and a disclosure of such information is necessary to prevent the commission of such crime;

- Where such disclosure is necessary for the lawyer to establish or collect his fee; or
- Where such disclosure is necessary to defend himself or his employees and associates against an accusation of wrongful conduct.

Clearly, the above exceptions provided for under the RPC does not cover cyberattacks/breach. The inference drawn from this is that a lawyer may be liable under the RPC for any cyber or data breach that affects his clients’ information.

[6] Rule 14 and Rule 19 of the Rules of Professional Conduct.

**POSSIBLE STEPS THAT CAN
BE TAKEN BY
LAW FIRMS TO ENSURE
CYBER HYGIENE**



POSSIBLE STEPS THAT CAN BE TAKEN BY LAW FIRMS TO ENSURE CYBER HYGIENE

The following steps can be taken by lawyers and law firms to ensure cyber hygiene and prevent any further cyber or data breach.

- Law firms should routinely identify items such as unmanaged laptops, servers and desktops.
- Engage in regular awareness and training of its employees on cyber security and cyber hygiene in general.
- Carefully address any system updates and operating-system-specific updates[7].
- Initiate a regular change of password policy and multi-factor authentication.
- Adequately identify unencrypted valuable and sensitive data and adhere to the required
- industry security compliance program.
- Develop a security system that adequately addresses insider threats.
- Scrutinise hardware and firmware updates for the purpose of identifying security risks and priorities.

- Obtain cyber insurance policies for future cyber liabilities.
- Establish and frequently update cybersecurity policies.
- Carry out regular penetration and vulnerability test on the various software and hardware being utilized by the firm, to determine their cyber strengths, overtime.

[7] Ibid.

sword write Welcome

```
height: auto;  
width: auto;  
padding: 10px 0;  
border-bottom: 2px solid #f00;
```



CONCLUSION



CONCLUSION

As earlier noted, cyber hygiene in Nigerian law firms is now more than ever, imperative. Law firms must begin to take steps to secure information that are stored online and offline. An understanding of the responsibilities vested with a lawyer to protect and keep confidential, information of clients, is sufficient for a lawyer to be proactive and take the necessary steps to avoid any cyber breach. Lawyers must also understand that they are not in any way immune from the activities of cybercriminals. In fact, they appear to be one of the most vulnerable targets of these cybercriminals.

Hence, law firms must begin to establish and maintain policies that guarantee and promote cyber hygiene. These firms must consider educating and enlightening their employees on cybersecurity. Apart from the steps recommended in this article, Nigerian law firms must also look forward to other ways, in which their data will be secured. Similarly, the services of experts and consultants should also be acquired by these law firms where necessary.

Though some of these measures may be expensive, it is better to expend resources ensuring the safety of the information of their clients, than to spend on any resultant legal action or liability that may be incurred as a result of a cyber breach.

ÆLEX



Raphael Irenen
(Associate, AELEX)

For further information, please contact:



Davidson Oturu
(doturu@aelex.com)



Frances Obiago
(fobiago@aelex.com)



Florence Bola-Balogun
(fbola-balogun@aelex.com)



Oyeyosola Diya
(odiya@aelex.com)



Opeyemi Adeleke
(oadeleke@aelex.com)



Kehinde Takuro
(ktakuro@aelex.com)

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed [here](#). You can also visit our website at www.aelex.com to learn more about our firm and its services.

COPYRIGHT: All rights reserved. No part of the publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior permission in writing of ÆLEX or as expressly permitted by law.

DISCLAIMER: This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.

CONTACT DETAILS

LAGOS, NIGERIA

4th Floor,
Marble House
1, Kingsway Road, Falomo
P. O. Box 52901, Ikoyi
Lagos, Nigeria

Telephone: (+ 234 1) 2793367; 2793368
4736296, 4617321-3;
Facsimile: (+ 234 1) 2692072; 4617092
E-mail: lagos@aelex.com

PORT HARCOURT, NIGERIA

2nd Floor,
Right Wing UPDC Building
26, Aba Road
P.O. Box 12636, Port Harcourt
Rivers State, Nigeria

Telephone: (+234 84) 464514, 464515
574628, 574636
Facsimile: (+234 84) 464516, 574628
E-mail: portharcourt@aelex.com

ABUJA, NIGERIA

4th Floor,
Adamawa Plaza
1st Avenue, Off Shehu Shagari Way
Central Business Area
FCT Abuja, Nigeria

Telephone: (+234 9) 8704187, 6723568,
07098808416
Facsimile: (+234 9) 5230276
E-mail: abuja@aelex.com

ACCRA, GHANA

7th Floor, Suite B701
The Octagon
Accra Central, Accra
P.M.B 72, Cantonment Accra, Ghana

Telephone: (+233-302) 224828, 224845-6
Facsimile: (+233-302) 224824
E-mail: accra@aelex.com