TRAVELERS

TRAVELERS CYBER BULLETIN OCTOBER/NOVEMBER 2019

Cyber-attacks are becoming increasingly common in the legal industry, with the law society reporting that one in three law firms suffered a cyber-attack at least once a week in 2018. The legal sector is a desirable target for cyber-attacks due to the vast amount of sensitive information stored, which is valuable for criminal activity, and due to the involvement in numerous financial transactions.

Solicitors Regulation Authority: Cybercrime Rise

In 2016/17, the Solicitors Regulation Authority (SRA) reported that cybercrime had resulted in over £11million of client money being stolen and predicted a continuous increase in cybercrime reports. By 2018/19, statistics showed that cybercrime against law firms has **increased by 52%** in the past few years. Such crimes include email modification fraud, phishing and malware. The effects of cyber-attacks can be detrimental, resulting in data breaches, theft of funds and reputational damage.

The SRA provide scam alerts for the public which help to inform them when choosing and using legal services. The scam alerts provide information on recent and relevant frauds where scammers imitate solicitors or law firms. Almost all the cybercrime reporting involves some form of forgery. This is used as a means of deceiving employees, rather than explicit hacking of a firm's systems.

(https://www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/)

(https://www.sra.org.uk/consumers/scam-alerts/)

Fake Website and Emails Scam

A fake website and email were set up misusing the name of a genuine law firm and a genuine solicitor. The scam, reported in late May 2019, involved an email which claimed to be from the law firm and was sent to an organisation in which the law firm has legitimate business with. The email included a loan agreement contract which requested the receiving party to sign and pay a $1,500 execution fee. The Solicitor's name was used to sign off the email and a fake email was used.

The scam was extremely sophisticated, replicating the original website and using genuine information, whilst adding fraudulent elements such as emails, solicitors and contact numbers. The scammers used a similar email domain to the company's, however added 'ltd' at the end. See example: **"Solicitor@LawFirm.com"** which is extremely similar to the fake email used in this scam, **"Solicitor@LawFirmLtd.com"**.

(https://www.sra.org.uk/consumers/scam-alerts/2019/may/abk-solicitos/)

This type of impersonation is increasingly common, and our intelligence shows that some scammers have gone as far as taking personal photos – selfies – with genuine company executives and using the images to convince victims they are representatives of the firm/individual and can trusted.

IN ASSOCIATION WITH

xcyber®

THE HUMAN SIDE OF CYBER

Exploiting Heightened Awareness: Cyber Protection Rackets

Impersonation of law firms as an increasing trend has also led to cottage-industry cybercrime – such as fraudulent domain name registration services.

Recent intelligence shows that a least one major, global law firm has been conned by a fraudulent China-based registrar, which purports to offer domain-name brand protection within China and Hong Kong.

Such domain registrars typically target brand managers at firms through direct engagement, especially where the target firm has recently been beleaguered by clone firms misusing their brand elsewhere. The brand manager's understandable hyper-sensitivity to further clone firms is exploited by such groups. We have noted providing spurious claims of identifying 'cybersquatting' activity in China and adjusting their marketing to purport to alert law firms to the activity and offer 'protection' from it.

Similarly, arguably legitimate - but otherwise dubious - Chinese registrar 'protection rackets' have been noted that do actually offer domain name registration services, albeit at grossly inflated rates, and in doing so avoid the scrutiny the completely fraudulent enterprises attract – where no services are offered, and the criminal intent is more obvious.

> *Comment:* Cybersquatting is the practice of registering names, especially well-known company or brand names, as Internet domains, in the hope of reselling them at a profit or using them in criminal activity.

Human Error Still Dominates

Human interaction plays a vital role in cybercrime within the legal industry. Human vulnerabilities can often expose a firm to cybercrime, where attackers can exploit human errors to launch successful attacks. Cyber criminals often target individuals rather than infrastructures as it primarily yields more effective results. Techniques include phishing, business email compromise, and impersonation scams which prey on human nature.

About 60% of data breaches that occurred between January 1 and June 20, 2019 were the result of human error, according to a recent Egress report. Of those incidents;

- 43% were due to incorrect disclosure
- 20% were caused by posting or faxing data to the wrong recipient
- 18% were due to failing to use the Bcc function or emailing data to the wrong recipient
- 5% were caused by providing data in response to a phishing attack

Psychological vulnerabilities can impact human error. Cognitive biases contribute to poor judgement or mistakes in decision-making. Such biases include time pressures on decisions, decision fatigue and bounded rationality. Cyber criminals can use social power and take advantage of these cognitive vulnerabilities and tailor attacks to them. For example, attacks which have a time pressure or appear to be from a higher level of authority put pressure on an individual to complete a task quickly and without hesitation. Another example is administrating the attack in the afternoon when employees are tired and lean towards 'easier' decisions or miss 'warning' signs.

(https://www.egress.com/en-US/news/ico-data-breaches-foi-2019)

(https://www.darkreading.com/threat-intelligence/how-cybercriminals-exploit-simple-human-mistakes/d/d-id/1335847)

> *Comment:* Social power is the influence or change of an individual's beliefs, behaviour and emotions due to actions of another individual.

Friday Afternoon Fraud

A conveyancing scam is a type of email modification fraud which includes criminals falsifying emails between a law firm and a client. This is often achieved after the criminal has gained illegal access to either the firm's or the client's email server, setting up inbox rules to divert certain messages to a hidden folder that the criminal has created. Access can be gained either through a breach into the firm's or the client's email server, or the use of insecure wi-fi. The main aim of the attack is to manipulate, or use information gained from such emails, to change bank details so that money is transferred into the hacker's account. Conveyancing is an extremely tempting target for cyber criminals due to the large sums of money involved, as well as the remote nature of transactions. Conveyancing has become one of the highest risk areas of law, with roughly £10million a year lost to email modification fraud.

In April 2019, Woodfords Solicitors lost more than £600,000 in a conveyancing scam. Fraudsters set up a fake email account impersonating a client and requesting a transfer of funds to be made from the solicitors to a chosen a bank account. The fraudster's email was only one letter different to the victim's legitimate email.

Conveyancing scams are commonly referred to as 'Friday afternoon fraud' due to them normally occurring just before the weekend, often a particularly busy day for completion of conveyancing contracts. This is also partly due to staff often not fully concentrating, as well as businesses being closed for the weekend and any unusual activity not being detected until a few days later. Due to the rise in conveyancing scams, both firms and clients should work together to mitigate and reduce the threat of an attack. This can be achieved through not using public Wi-Fi, using confirmation techniques such as call-back, transferring low sums to confirm bank accounts or password protection.

(https://www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/how-to-identify-a-cyber-attack/friday-afternoon-fraud/)

(https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams)

Vulnerabilities When Working Remotely

Research indicates that despite law firms being one of the most attractive targets for cyber criminals, they don't always protect themselves accordingly. Results from a 2018 survey demonstrated that 70% of people globally work remotely at least once a week. However, over a quarter of the businesses analysed fail to prepare basic security precautions and do not restrict access to files for employees working remotely.

The legal profession now has workers who frequently work remotely or take work home. In order to do this, employees often email necessary documents to their personal or home accounts. This poses as a major risk as it can leave data completely exposed with no protection. Working remotely, on a mobile phone or laptop can present other risks, particularly when public or insecure Wi-Fi connections are being used. Insecure Wi-Fi connections are easier to hack due to the open connection often being unencrypted and vulnerable. The 2018 Mobile Security Report reported that 62% of Wi-Fi related security incidents occurred in cafes and coffee shops. Despite this, legal industry investigations demonstrate that free, insecure Wi-Fi in cafes, bars and hotels are used by around one third of employees.

As a nation, the way we work has dramatically evolved and businesses must adapt its cyber security and training to reflect current lifestyles. Simple precautions such as user education, use of Virtual Private Networks, mutlti-factor authentication and enforced updating/ patching regimes for remote users can significantly reduce risk.

(https://www.lawyer-monthly.com/2018/09/hackers-took-11-million-from-law-firms-last-year-time-to-take-action/)

(https://www.todaysconveyancer.co.uk/main-news/legal-firms-vulnerable-cyber-attacks-working-remotely/)

Artificial Intelligence Audio Fraud

Social engineering attacks are on the rise, with various methods being used to successfully defraud companies. In March, fraudsters used an artificial intelligence-based voice generating software to impersonate a CEO and request a fraudulent transfer of $243,000. The CEO of a UK based company was tricked into transferring the funds to a 'Hungarian supplier' under the orders of who he believed to be the CEO of the firm's German parent company. The fraudster's slight German accent and voice patterns resulted in the targeted CEO not rendering any suspicion of the request. The funds were then transferred from Hungary to Mexico and other locations and have yet to be recovered. To reduce the risk of economic and reputational fallout from such attacks, companies must safeguard themselves by implementing a verification system before transferring funds. Such techniques can include email confirmation or 'call back'.

(https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/)

(https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402)

Smart Fraud via Smart Devices

A newly developed scam has occurred through fraudsters taking advantage of auto-dial features on smart devices such as the virtual assistants 'Siri' or 'Alexa'. When requesting a number for a company or service, virtual assistants look through search engines to find the number and dial it for you.

However cyber criminals have taken advantage of the fact that the majority of individuals do not corroborate these numbers. These criminals are then able to create fake contact numbers for company customer services and bump them into the top list of search results. This is often achieved through paying for adverts. As a result, when the virtual assistant locates and dial the top number, it can be the contact for the scammer rather than the desired company. Fraudsters are then able to extract personal and payment information whilst victims are under the illusion, they are communicating with a service provider.

(https://www.bbb.org/article/news-releases/20523-scam-alert-using-voice-search-use-caution-when-asking-for-auto-dial)

Similarly, our intelligence reveals that criminal networks are seeking to edit contact information contained within non-authoritative sources, such as Google Maps entries. Largely focused on financial services firms in South-East Asia at present, the scam has primarily relied upon victims looking up a local bank branch phone number on Google Maps – but dialling the number for scammers instead of the branch.

We recommend reviewing any external online presence, particularly Google Maps entries, for accuracy and where possible claiming corporate ownership of such entries.

Bitcoin Recovery by Russian Law Firm

The Moscow based law firm, Zheleznikov and Partners (ZP Legal) proclaim they can recover $2 billion bitcoin lost in the Mt.Gox hacking. Mt.Gox, a bitcoin exchange based in Tokyo, was hacked in February 2014 which resulted in bankruptcy. The hacking resulted in Mt.Gox losing around 740,000 bitcoins, valued at the equivalent of €460 million at the time.

On September 12th, ZP Legal proposed their own solution to recover about $2 billion in bitcoin on behalf of the victims of the Mt.Gox hack. The law firm claims to have identified Russian nationals who received the stolen money and plan to take legal action against such individuals.

(https://www.coinspeaker.com/zp-legal-mt-goxs-2-billion-bitcoin-hack/)

(https://www.coindesk.com/2-billion-lost-in-mt-gox-bitcoin-hack-can-be-recovered-lawyer-claims)

Island Hopping/Supply Chain

Cyber criminals are now using the increasingly popular attack technique 'Island Hopping'. Attackers infiltrate their target organisation through smaller partner companies which tend to be less secure than the larger target organisation. These smaller companies tend to have more lapses in cyber security, making it easier for attackers to gain a secure position in a connected network which allows for exploitation.

> "They're not just, say, invading your house - they're setting up shop there, so they can invade your neighbours' houses too."
>
> **Carbon Black's Chief Cybersecurity Officer**

Island hopping poses as a severe threat to organisations as it only requires one weak link in the supply chain of companies to be at risk for an attack. The legal industry has perpetual suppliers and partnered industries which can be targeted. Even one off or small partnerships can leave an organisation vulnerable, for example business card printing. Law firms may only use a company to print business cards once, but their personal data can be taken advantage of by attackers.

> *Comment:* 'Island Hopping' refers to the process of impairing an organisation's cyber defences by targeting vulnerable partner networks, rather than conducting a direct attack.

Gift of the Gifts

XCyber® routinely detect exposures of firms and/or their employees from along their supply chains. One recent, novel event saw a global law firm's top client list exposed inadvertently, due the purchase of gift baskets. In that case, the retailer's own supplier – a delivery service – were using a poorly configured data framework that ultimately revealed the full details of the firm's top clients and their contact details.

About Us

X Cyber Group Ltd (XCyber®), solve commercial problems with state-grade intelligence expertise. With management having an aggregate 200+ years of cyber experience in the British Government, the team at XCyber® have advised numerous Law Enforcement, Intelligence and Security Services across the globe on cyber strategies, including work in hostile environments.

We focus on producing intelligence-led, data-driven and evidence-based reporting which enables decision making across our clients' varying needs. Our intelligence is delivered in qualitative, narrative format, providing easy to digest and actionable information.

XCyber® are specialist in finding meaningful, lasting resolutions to complex issues. We know how to acquire the relevant information, and how to action it in a manner that is efficiently conducive to the desired aim or end-state.

xcyber®

THE HUMAN SIDE OF CYBER®

If you have found this useful and would like to receive these quarterly updates direct to your inbox please **click here** to register