JURISK!

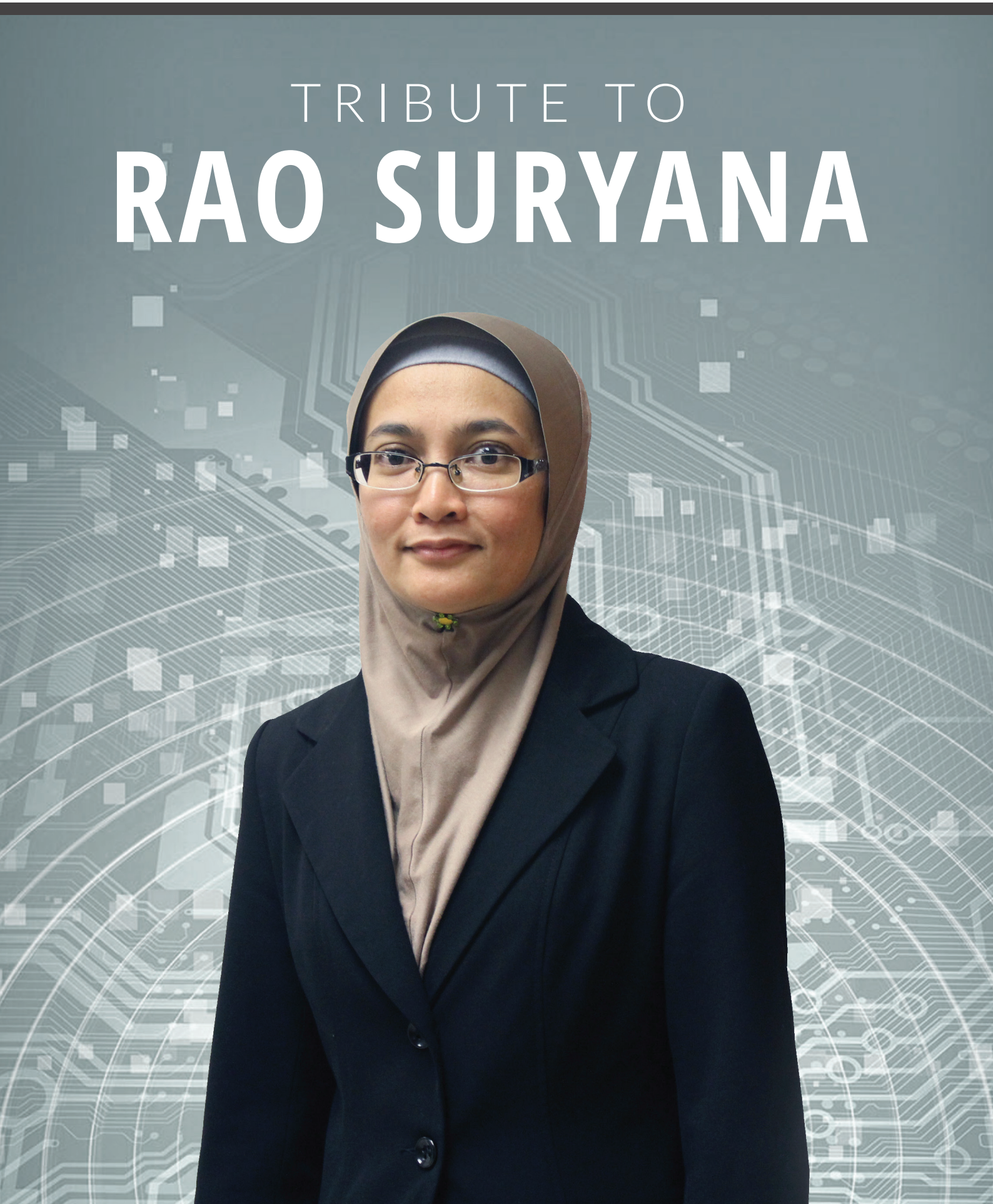
December 2016 Volume 12 Issue 2

Risk Management Newsletter

A biannual publication of Professional Indemnity Insurance Committee, Bar Council Malaysia

TRIBUTE TO

RAO SURYANA



Content

Inside this issue ...

Happy New Year!

... we take a look at some of the issues of cybercrime that law firms have encountered. Fraudsters and threats are not only in the form of physical entities. If you are an Internet user — either having an email account, browsing the Internet or storing files in a cloud storage system — and were not cautious when you were online, you can be a victim of cybercrime. You can read about and take heed of the applicable notifications made to the Professional Indemnity Insurance ("PII") Scheme, some of which are shared in this issue as case studies.

There is no definite or best way to protect you or your law firm against cyberthreats, but undertaking some basic steps — especially if you have yet to do so — will help reduce the risk. We have included tips on protecting, among others, your identity online, email account, and password.

This issue is dedicated to Rao Suryana bt Abdul Rahman, our PII Committee member since 2009, who passed away in November 2016. She was a sole proprietor of a small firm, and benefitted from using technology in running her practice, especially when she was on the road.

We have also included tips for small firms and new start-ups, on maximising the use of technology, and hope that these will be helpful.

We hope you enjoy this issue of *Jurisk!* If you have any feedback, thoughts or ideas that you would like to have featured in *Jurisk!*, or even about the PII Scheme in general, please contact us at the PII and Risk Management Department. You can find our contact details on the last page of the publication.

Happy reading!

The *Jurisk!* Team

Chairperson's Message

DON'T FALL VICTIM TO CYBER CRIME

Happy New Year and Best Wishes!

We are ushering in the New Year and let us hope that 2017 will be better, kinder and more fruitful to all of us!

In these difficult times, we have to be more vigilant, prudent, risk averse and more diligent in our practice.

Practising law in this day and age is becoming increasingly challenging. Not only do lawyers have to keep up with changes in the law and its procedures, deal with escalating competition and an even more demanding clientele, we must also keep up with the rapid changes of modern times.

With the economic downturn, lawyers normally end up at the tail end of client disappointment and more likely to end up with law suits for all kind of things ie negligence, loss, failure to attend to matters etc.

The number of malpractice suit against lawyers are on the increase and we would therefore caution members to be vigilant in their practice and office administration.

Keeping accounts in order, having check and balance mechanisms in place and keeping a close eye on staff would greatly reduce your risks.

Please ensure that you have checklists in place for conveyancing matters. It will greatly assist you when there is a malpractice suit and your PII cover is invoked. If you have used a checklist in the conduct of the file, then the conveyancing Base Excess most likely would not apply to you and therefore you don't have to fork out a higher base excess.

The other area of concern is partnership dishonesty. It is distressing to listen to members being put in a very difficult financial position which many are not able to recover from wayward partners. There is not much any insurance policy can do for dishonesty. The primary aim and cover of the policy is for negligence.

Although there is a basic cover for partnership dishonesty for the innocent partners, it is capped at RM350,000 or the firm's mandatory limit whichever is the lowest. A firm's Base Excess also differs when there is dishonesty of partner. We would strongly urge members to take stock, re-examine their partnership arrangement with regard to client and office account management. We have in past issues provided some guidelines on what are the key areas that need to be addressed.

We also need to take stock of the advent of the internet and the new threats and challenges that it brings with it.

While it has made our lives easier and much more comfortable than ever, it does come with its own set of risks. In the past, the Scheme has had to deal with actual, human fraudsters – living, breathing beings who brazenly walked into our offices, having found deceitful ways to fraudulently cheat and embezzle millions from our firms. These days however, these very same fraudsters have now become faceless entities hiding behind computers, with abilities and know-how to cause much, much more harm than ever before.

We should be vigilant than we have ever been in our daily work, especially when cyber-crimes are now on the rise. The Scheme has been receiving notifications from Firms who have been victims of cyber-crimes but we believe the numbers could be much more than actually reported, and we also believe that crimes of these nature will only grow bigger each year.

If you do not know where to start, begin here, with this Issue of *Jurisk!* And to be honest, none of us here are experts in the field of cyber-crime, but hopefully the articles we have in this issue can be a jump-off point for you and your Firm to develop your own cyber-security initiatives.

Increase of Insurance Premiums

As you may already know, there is an increase of RM50 per lawyer in the 2017; premium payable for the 2017 PII Renewal is RM1,190 per lawyer. The PII Committee were not able to hold off the increase this year – caused predominantly by a substantial surge in the claims experience in the PII Scheme.

A surge in claims as well as the claims' values directly increases the costs that is involved to maintain and manage the claims – these costs are directly borne by the Insurers. Realistically speaking, to reduce these costs that Insurers face, we must bring down the number of claims.

In this uncertain and bleak economy, when every other costs of living seem to be escalating, it can become attractive to law firms to take shortcuts here and there, to skip vital steps in procedures, and to overcharge clients, but these are how mistakes are made and this will lead your Firm down a very dark rabbit hole if unethical practices do not cease.

We must continue giving our clients the very best and the most professional experience we can so that they walk away happy and fulfilled. Unhappy clients are trigger-happy clients – do not give them any reason to sue you or your law firm.

The Lexon Project

Bar Council has appointed Lexon Insurance Pte Ltd, a captive insurer providing primary layer professional indemnity insurance to Queensland solicitors in private practice as Bar Council's risk management consultant. Lexon will train Bar Council's dedicated staff on risk management and thereafter assist in developing effective risk management programmes for us. The consultancy role also includes a review of the claims data, training staff on data collection and ongoing support on risk management.

The consultation for lawyers will help the Bar understand the process of establishing the roots of claims affecting Members and to develop appropriate risk management programmes to effectively address the issues surrounding claims and risk management. Bulk of the consultation and training will be in the first six months of the project with an option for ongoing support for subsequent years at the end of the consultancy period.

Have your Firm Reviewed

The *Risk Aware!* Review initiative that was kick-started in 2016 is still ongoing, and we hope to reach more Firms in 2017. Our aim for conducting the review individually on Firms is to gauge how far they have gone in their risk management initiatives, for example, what steps and procedures they have, are these procedures adhered to by all in the Firm, and is there a monitor within the Firm to ensure compliance?

The review will also be able to pinpoint areas of weaknesses and highlight avoidable areas exposed to risks. Using the information gathered during the review, our Team will be able to put forth recommendation that the Firm can follow. The PII Committee highly recommends that every Firm open its doors for us to help you. At present, our priority are Firms outside of the Klang Valley especially smaller to medium sized firms.

The Committee is once again proud to have served Members of the Malaysian Bar for yet another year, and we look forward to doing the same, only bigger and better, in 2017.

As always, if you have any thoughts, comments or feedback you can contact me directly at any of the contact information provided below. You could forward them directly to the PII and Risk Management Department – their contact details are on the last page of this Issue.

Thank you, and we wish you all the best for 2017.

Ragunath Kesavan
Chairperson
PII Committee
Email: ragunath@kesavan.com.my
Telephone: 03-2095 2299

CYBER ATTACK! ARE YOU READY?

In this day and age of technology, it's important to be up to date with technology's latest developments and perils to be prepared. If you're using any of the following:

mobile devices, laptop, desktop, tablet, email account, web browser etc

This issue of Jurisk! will help you get started.

Are You Online...?

You decide what information you reveal, when, why, and to whom!

Tips on password

- Passwords should be difficult for others to guess.
- Don't use the same password for every account.
- Create passwords which are long, unique and use a mix of random numbers, and lower and upper case letters.
- Change passwords regularly and don't share them.

Spotting Fake Emails

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email is sent from a completely different address or a free webmail address.
- The email does not use your proper name, but uses a non-specific greeting like "Dear Customer" or "Dear Winner".
- A sense of urgency; eg the threat that unless you act immediately your account may be closed or someone's livelihood endangered.
- A name of a prominent organisation with a forged or fake website link.
- A request for personal information such as user name, password or bank details.
- The email contains spelling and grammatical errors.
- The email indicates you were expecting an email from the sender.
- The entire text of the email is contained within an image rather than the usual text format, which contains an embedded hyperlink to a bogus site.

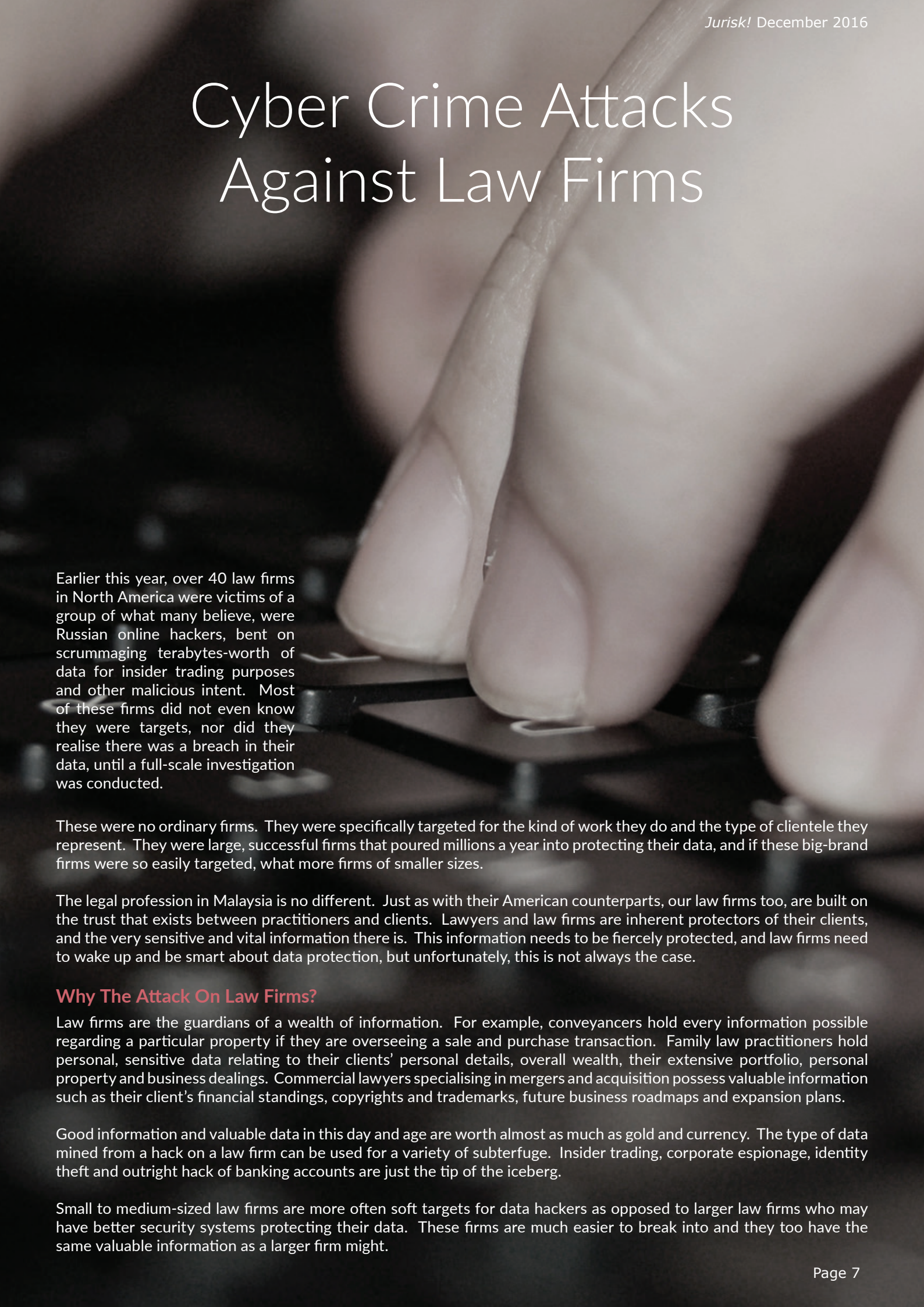
Do

- Use anti-virus.
- Keep your software updated.
- Ensure that the link label and web address tallies before clicking on it.
- Ensure that data transmissions are made over secured sites.
- Think before sharing information over social networks.
- Be cautious of public Wifi.
- Lock your gadgets with a passcode.
- Consider wiping out data on a gadget remotely if it is lost.
- Control how information is disclosed as many hacks do not involve hi-tech methods.
- Take time to check that you have the correct email address.
- Do online search.
- Turn on firewall.
- Make sure the link is secure before entering payment card details on a website.
- Be conscious of web security.
- Ensure email settings have the requisite security settings, such as encryption of emails.
- Check "From" field when you receive or before sending an email.

Don't

- Click on unsolicited pop-ups, unknown emails, email attachments.
- Click on a link you did not expect to receive.
- Provide information on the website that may open.
- Click on links you are unfamiliar with.
- Use the same passwords for different websites.
- Disclose information unless you're sure of its intended purpose.
- Accept social media invitation if in doubt.
- Store credit card details online.
- Reveal your username and password to anyone.
- Reply to spammer or the sender, for any reason.

Cyber Crime Attacks Against Law Firms



Earlier this year, over 40 law firms in North America were victims of a group of what many believe, were Russian online hackers, bent on scrummaging terabytes-worth of data for insider trading purposes and other malicious intent. Most of these firms did not even know they were targets, nor did they realise there was a breach in their data, until a full-scale investigation was conducted.

These were no ordinary firms. They were specifically targeted for the kind of work they do and the type of clientele they represent. They were large, successful firms that poured millions a year into protecting their data, and if these big-brand firms were so easily targeted, what more firms of smaller sizes.

The legal profession in Malaysia is no different. Just as with their American counterparts, our law firms too, are built on the trust that exists between practitioners and clients. Lawyers and law firms are inherent protectors of their clients, and the very sensitive and vital information there is. This information needs to be fiercely protected, and law firms need to wake up and be smart about data protection, but unfortunately, this is not always the case.

Why The Attack On Law Firms?

Law firms are the guardians of a wealth of information. For example, conveyancers hold every information possible regarding a particular property if they are overseeing a sale and purchase transaction. Family law practitioners hold personal, sensitive data relating to their clients' personal details, overall wealth, their extensive portfolio, personal property and business dealings. Commercial lawyers specialising in mergers and acquisition possess valuable information such as their client's financial standings, copyrights and trademarks, future business roadmaps and expansion plans.

Good information and valuable data in this day and age are worth almost as much as gold and currency. The type of data mined from a hack on a law firm can be used for a variety of subterfuge. Insider trading, corporate espionage, identity theft and outright hack of banking accounts are just the tip of the iceberg.

Small to medium-sized law firms are more often soft targets for data hackers as opposed to larger law firms who may have better security systems protecting their data. These firms are much easier to break into and they too have the same valuable information as a larger firm might.

The Cost Of A Cyber Attack

The "Panama Papers" have already claimed the job of the Icelandic Prime Minister and prompted uncomfortable questions for the UK's (previous Prime Minister) David Cameron. But it should have a much wider impact.

Others named in the documents from law firm Mossack Fonseca include high profile clients around the world. Overall, 140 politicians and public officials are named, as well as more than 214,000 organisations, according to the International Consortium of Investigative Journalists[1].

The Panama Papers scandal only proved that the breaches in a law firm's data security can have a wide-casted impact – not just for its clients, but also those associated closely with its clients. If confidential data is breached and later on exposed, your clients will be left unprotected. Their personal data, business dealings, and associated business partners will be of interest to many, especially if they are public or prominent figures to begin with.

The firm too will suffer terribly as its reputation will forever be linked to the scandal and further damages will manifest in other ways; loss of current clients as they walk out the door, as well as loss of any future income in the shape of new clients.

What Can Law Firms Do?

You can choose to either continue hiding under your rock and believing you will never be preyed upon online, or you can come out from under that rock and be more vigilant against these crimes. If you think you're too small a fish, think again! These crimes don't discriminate the size of their victims, these crimes perpetuate one sole entity: the information you hold.

In 2014, US based IT security developer SOPHOS ranked Malaysia as sixth globally in terms of cybercrime threat risks, as the total cybercrime bill topped $300 million (RM1.2 billion). What does this really mean? It means that in general, Malaysians have a lackadaisical view of internet and data security. It means that law firms HAVE TO NOW BE more proactive in fiercely protecting the trust put onto them by their clients.

Sole proprietors, small and medium sized firms need to work the hardest here in finding the best-fit solution to secure data. These law firms are believed to understand that the dangers of data breach can happen, but what they lack is an understanding of how best to move forward. Hiring an "IT guy" fresh out college is no longer sufficient. Neither is adopting an Enterprise Solutions Systems as they are expensive, complicated, and just too much for small and medium sized firms.

Once you find your middle ground, develop that plan of cultivating data security on a firm-wide basis. Put your newly formed protocols and operating procedures into a readily available document for all your Partners, Legal Assistants, clerks and support staff to be able to refer to whenever. Delegate a Partner to oversee Firm's IT protocols – ensure firm-wide participation.

Footnote: [1] https://panamapapers.icij.org

Technology for Sole Proprietors & New Start-Ups

Written by Jeremiah Rais, pupil-in-chamber

The dress and vocabulary of a lawyer may seem archaic to most but that shouldn't prevent you from embracing the 21st century. While a majority of law firms will not have the resources nor the expertise to develop artificial intelligence to outperform junior lawyers and paralegals , you can still and should take small steps to replace hard work with smart work.

Organising Your Diary

Smartphones have become as essential to us as wooden clubs were to our stone age forefathers. While smartphones do come in handy when you're trying to kill time on your commute to work, you should certainly use it to get your work organised. Most email platforms provide users with a calendar feature which can be used to organize your day and to note down key dates, whether it be to meet a prospective client or to file papers in court.

These calendars can be synchronised wirelessly to your mobile phone or tablet without you having to update the information in several places. This will allow you to be prompted of important dates no matter where you are, even in the event that a hardcopy of your diary was lost in a fire.

Don't overlook using this basic feature of your smartphone - there's a reason why PDA devices went out of fashion in the early 2010s!

Communication

Effective communication allows quicker decision-making, a key to any efficient law practice. Your law practice should consider adopting instant messaging platforms as a means for ad-hoc discussions between employees whether they are in the next room or on a different continent. Features such as document sharing and group chats will allow you to bounce ideas off each other with little hassle. The flexibility that instant messaging brings to a workplace cannot be underestimated - you may be able to minimise the need for those dreaded weekly meetings by keeping each other updated on the progress of a case from the comfort of your desk.

The messages which are sent in real time and can be accessed from most devices with internet access enables rapid means of communication and thus improves workplace efficiency. More importantly, instant messaging is a paperless record of what was said should you need to refer to it and most service providers provide end-to-end encryption, which in theory, prevents third parties from deciphering what was communicated between you and your colleagues. Many instant messaging platforms require little to no investment which makes it a viable option even for law firms with limited resources.

Footnote [1] Jane Croft, 'Legal Firms Unleash Office Automatons' Financial Times (16 May 2016) <http://www.ft.com/cms/s/0/19807d3e-1765-11e6-9d98-00386a18e39d.html#axzz4HiLoOIR6> accessed 10 August 2016

Talent Hiring

Don't miss that opportunity to hire that fledgling, young lawyer by embracing social media. Bypass headhunters and paid advertisements for that job opening at your law firm by scouting for talent on websites such as LinkedIn and JobStreet. Many young professionals today have profiles and comprehensive CVs listed on business oriented social networking websites, allowing you to find that perfect fit for your law firm even without the luxury of a Human Resources department.

While one shouldn't be quick to judge a book by its cover, a quick search of your potential employee's name or email address will likely come up with some hits and even a social media profile or two. This will allow you to gauge the person's personality and even the level of written English proficiency before the interview. Once your ideal employee is found, you may even consider conducting an interview via video conference should he be located out of town.

Legal Research

A law firm without legal resources is a non-functioning one but filling your library with practitioner texts and law reports can be a costly endeavour, especially if you're a new start up or a small firm. One way to get over this is by subscribing to an online legal database which allows you to search broad practice areas or specific databases for legal authorities from within and outside your jurisdiction depending on your needs.

Online legal databases will not only save you costs but save you the time and effort while doing legal research by essentially bringing the best law libraries in the world right to your desktop. A list of authorities that either affirm or disapprove a legal principle is just a click away without you having to leaf through numerous legal tomes. With most legal databases providing free trials for short periods of time, you should try out a variety to determine what is most suitable for your practice before purchasing a subscription.

Online Presence

A professionally designed website is key to building the credibility you need to compete against the more established names in the legal profession. With potential clients becoming more aware of their options, it is a certainty that your firm will be researched and its name will at the very least, be put through a search engine. A website with well-thought-out contents will give your clients confidence that your firm has enough stability and foresight to have an online presence.

Your website can also serve as a platform for you to air your areas of expertise and a summary of the cases you have handled to a worldwide audience. It is an excellent opportunity for you to tell potential clients why you are deserving of their trust and why you should be hired to represent them.

Aside from being an excellent marketing tool, your website will also make you more accessible to potential clients. Your website will be the first port of call when a potential client has enquiries. As it will be accessible all day and all year round, a client who has the convenience of having the details needed on your website to make an informed decision is likely to hire you over a firm that does not have an online presence. Furthermore, you can use search engine optimization basics to ensure that your website appears as a hit for certain keywords or queries and thus set you up as an authority in the eyes of the increasingly tech-savvy client.

THE RANSOMWARE SCOURGE

The ransomware virus is a particularly malicious virus, that once enabled, will encrypt the data on all your computer and the computer systems that your computer is attached to, rendering it unusable. The end user will receive a message demanding a ransom paid to some unknown entity in order to get "the key" to un-encrypt your data and possibly make it usable once more.

This ransomware virus is mostly delivered through phishing emails to end users. In its early days, ransomware emails were often generic in nature, making it easier for end users to realise it was not a legitimate email, and delete it immediately. In more recent times however, these emails have evolved and now are more geared in their approach to target both the organization and the individual, making it easier for the end user to fall into its trap.

The Allure of Law Firms

Quite simply, ransomware is a malware which restricts access to information stored on a computer and demands the user of that computer to pay money in order to remove the restriction. Failure to pay the ransom money demanded will result in a permanent deletion of all encrypted files by the hackers.

Firms providing legal services are particularly attractive targets for ransomware attacks for the sole reason of storing confidential information of reputable clients they have in their computer systems. Law Firms are then forced into paying these cyber criminals merely to avoid the negative reputational consequences which arise from the failure to protect their clients' sensitive information.

How It Works?

Step 1

End user receives an innocuous looking email. These emails are generally made up of two kinds:

1. The offending email contains malicious attachments, including .pdf, .doc, .xls, and .exe file extensions. These attachments are described as something that appears legitimate, such as an invoice or electronic fax, but contain malicious code and will be triggered once it is downloaded by the user.
2. Receipt of an email that appears legitimate but contains a link to a website hosting the malware. When the user opens the malicious file or link in the phishing email, the most frequent end result is the encryption of files and folders containing business-critical information and data.

Steps 2 & 3

The malware is downloaded onto the host's computer and proceeds to encrypt all the files on its computer. Most malware also extends to encrypt files stored in the Firm's entire systems if the host computer is attached to it. Encryption of these files mean that is becomes "locked" and unusable to the Firm. The Firm will not be able to work on these files, make copies, or save backups. It is lost forever.

Step 4

The end user receives a ransom notice from the hacker providing details such as ransom amount, payment method, and deadline for payment.

Step 5

Once payment (Note: it is advised to never pay, see below) is made, the Firm will be issued a "key" code to unlock their encrypted files. These files will hopefully once again become useable to the Firm.

Never Pay The Ransom

Although it is tempting to just pay up the ransom and retrieve your information, many cyber security specialist advice not to, as more often than not, the chances of retrieving the encrypted data are almost non-existent even if you pay.

Also, when a ransom is paid just the one time, you will be attacked over and over again because you've proven once that you will pay to have your information back. The best way to protect against this type of ransomware is prevention.

Users can prevent being hit by ransomware by doing the following:

1. **Avoid clicking suspicious links**. Firms should concentrate on creating awareness and provide information to their staff to be more vigilant against these sorts of attacks. These include being able to spot the threat of ransomware via email and phishing websites.

2. **Backup important data**. If a device or system is infected, backups may be the best way to recover your critical data. At best, you will only lose a few days' worth of data. Your Firm's data must be backed up on a regular basis by a competent staff. Simply backing-up data is not enough, **as** all backed-up data must also be verified for its integrity and done so securely. Back-up data must not be connected to the same computer or network that is secured – back-up should be done into an external drive, cloud storage or a physical storage offline. Some ransomware can even go as far as locking (encrypting) cloud-based backups when systems continuously back up in real time.

3. **Double check everything.** Verify the email sender and double check the message content. See page 6 for tips on email security.

4. **Ensure your software is updated.** Make sure your that Firm's anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.

5. For more tips on guarding yourself against possible cyber threats, read the tips provided on page 6.

Case Studies

DON'T FALL VICTIM TO CYBER CRIME

Written by David Ng, Senior Manager, Malaysian Bar Scheme Department.
Jardine Lloyd Thompson Sdn Bhd

Case Study 1:

General Cyber Fraud

The law firm received instructions by email to transfer monies to a bank account purportedly belonging to its client (hereinafter referred to as "Account Bogus"). Fortunately, the firm checked and confirmed their client's instructions first by telephone and managed to avoid the scam.

The law firm believes that the fraudster intercepted the legal firm's emails by hacking into the email accounts of the legal firm and/or its client. The fraudster then posed as the client and provided instructions for the money to be transferred to Account Bogus. The fraudster also provided information believed to have been extracted from previous email correspondence between the legal firm and the client, to bolster the fraudster's credibility as the purported client. This led to the initial impression that the firm was dealing with its actual client.

It was also noted that the fraudster had used what appeared to be an almost similar/identical email address to that of the actual client, when giving instructions to the law firm. The firm has lodged a report to the police and Malaysian Communications and Multimedia Commission ("MCMC").

Case Study 2:

If Only It Was Confirmed in Writing

The Insured Practice ("IP") sent an email to their client informing him that the proceeds of a sale of land had been deposited with them. The following day, the client replied that the amount stated in the email was inaccurate. This email had stated the client's name although the email address differed from the one that IP had been using. Following the email, the client telephoned IP to discuss the discrepancy.

The client repeated the contents of the reply email apparently to assure IP of his identity and in the course of the telephone conversation, the client convinced IP to remit the proceeds to an account at Bank of Doomsday. IP did as instructed and remitted the proceeds of sale from the client's account maintained at Bank of Integrity.

A remittance slip was emailed to the client once the transfer had been effected. On the evening of the same day, the actual client called and denied that he had sent any email instructing IP to remit the sum to Bank of Doomsday. IP immediately notified Bank of Integrity of what had transpired and lodged a police report thereafter.

Case Study 3:

Almost Lost My Reputation

IP received an email from a Mr Irwin from Australia seeking to verify the identity of one of the partners of the firm known as T Bundy. Mr Irwin had apparently been emailed by T Bundy who claimed to be acting on behalf of a charity.

T Bundy then called Mr Irwin to get clarification on his email. It was then that T Bundy discovered someone was impersonating himself in an email as "T Bundy the Attorney". The imposter had apparently promised Mr Irwin that a sum of USD2.6 million would be transferred to him. This fund was apparently held at Bank of Honesty. The imposter had also advised Mr Irwin that he can assist in transferring the funds without any tax liability as the funds were a donation. However, in order to engage the services of this imposter, Mr Irwin would first have to remit a sum of RM20,000.00 to an account at Bank of Honesty as attorney's fees to him.

This triggered Mr Irwin to contact the firm to verify the identity of T Bundy. The real T Bundy informed him that there was no such proposition as presented by the imposter in the email. The real T Bundy immediately lodged a police report to protect himself.

Case Studies

Case Study 4:

A Click To Lose It All

IP received an email from his client with an attachment link to a cloud server. The link was said to lead to a shared document in the said server. IP clicked on the link and was directed to a login page.

The login page looked almost identical to a well-known cloud server. This cloud storage service was coincidentally also used by IP. Not suspecting anything, IP entered his username and password. IP's webmail account was subsequently hijacked and IP was locked out of his own webmail account. The hackers then accessed IP's contacts list to send out emails soliciting donations. Recipients of these emails were asked to reply and particulars of the payee would later be provided.

Upon discovering what had happened, IP informed the service provider of the cloud service. IP was put to significant hardship in trying to regain access of his own webmail account. A police report was made as IP was concerned that his email account may be used for nefarious purposes.

Case Study 5:

Read The Details

The loss involves a sale and purchase of a property. IP was appointed to act for the vendor in the said transaction. IP communicated and had received instructions from his client sent from an email account known as "mno123456@email.com".

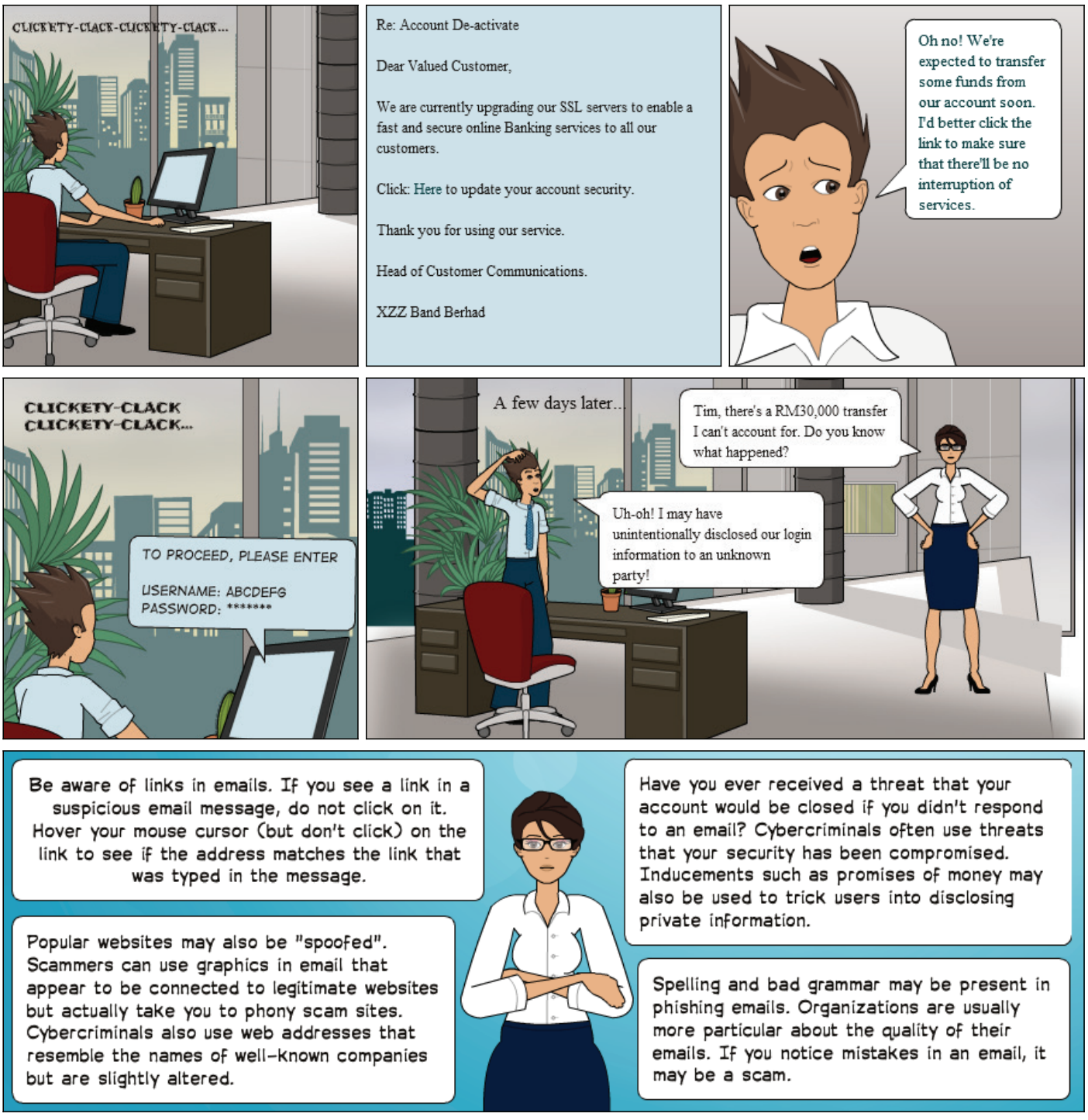
Subsequently, IP received an email with instructions to divert the proceeds of sale to a third party. Not suspecting anything amiss, IP did as instructed.

IP later received a telephone call from his client enquiring about the proceeds of the sale. Although IP informed that the money has been transferred, the client denied ever receiving the money or gave any instructions to transfer into a different account. Upon closer examination, IP noticed a minor difference in the email address used to communicate with the client and the email with instructions to divert the proceeds of sale to a third party. Unfortunately, IP did not detect the difference between the two email addresses as they were sent just minutes apart.

IP suspects that the firm's email account had been hacked and that the hacker may have gained knowledge of the sale. A police report was lodged by IP immediately following this discovery.

To avoid getting yourself into a similar situation, read our cyber tips on page 6 and Bar Council circular on page 32.

What Is A Phishing Scam?



The comic illustration above is used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

When The Unexpected Happens

When a sole proprietor suffers an untimely death, the orderly closure of the firm and the firms' client files have to be attended to. The same is the case when a sole proprietor is suffering from a serious medical condition and is unable to continue practice for an indeterminate period of time.

The following are two scenarios that may occur in such circumstances:

Scenario 1

Upon notification of a Member's death, the Bar Council will write to the deceased Member's family to enquire and/or inform inter alia the following:

- if during the Member's lifetime, the Member made plans for the unexpected and nominated a Solicitor to take over the firms' client files and accounts, in the event of the Member's death;
- if no such plan exist, whether the family member(s) would be able to appoint another solicitor to take over the firms' client files and accounts; or
- if the family member(s) prefer the Bar Council to handle the firm's client files and accounts.

Scenario 2

Upon notification of a Member's serious medical condition, the Bar Council will get in touch with the Member or the Member's family (whichever the case), to enquire if the Member or the Member's family can appoint another solicitor to take over the firms' client files and accounts or prefer the Bar Council handle the same.

Professional Indemnity Insurance Cover

After the death of the Member, the estate of the former Member may still be liable for any claim filed thereafter (depending on the statute of limitation). In this regard, under the Professional Indemnity Insurance ("PII") Scheme, the Insurer is liable to provide indemnity in respect of malpractice suits made against a former member (or his estate in the event of his death), subject to terms and conditions of the policy. The said indemnity also extends to cover costs incurred for claimant's costs, defence cost and mitigation cost.

Cover provided under the PII Scheme for a deceased Member is based on the Member's last policy year. This means the Member's last mandatory limit and base excess is applicable.

The estate of the deceased Member must make a notification to the Insurer within 60 days in the event they receive any writ, letters of demand, assertion of threat to sue or of any circumstances that may lead to a claim.

Welfare of the Sole Proprietor or his family members

The LawCare Committee of the Bar Council will also play an important role in providing financial assistance to the Members or their families in cases of illness, disability or death.

Payout in event of illness or disability of a Member

In the event a Member suffers from a total or partial permanent disability, a sum of RM40,000 (or a percentage of this sum) is paid to the Member.

Payout in event of death of a Member

A total payout amounting to RM42,000 is made to the beneficiary/ trustee/ nomineev (for non-Muslim Members) or to beneficiaries in accordance with the principles of faraid (for Muslim Members) in event of death of a Member.

In both instances, RM30,000 (and the additional RM2,000) is paid from the group insurance policy, and the remaining RM10,000 is paid from LawCare Fund.

In the above respect, it is extremely advantageous for the Member to nominate beneficiaries to facilitate the process of the payout. For more information please contact the Bar Council Secretariat or download, complete and return the nomination form from the Malaysian Bar website under the "Resources> Frequently Used Forms" tab.

A Tribute To One Of Our Own

Rao Suryana bt Abdul Rahman

We received the sad news of the passing of Rao Suryana bt Abdul Rahman on 17 Nov 2016. Rao was a member of the PII Committee since 2009.

Her involvement in the Committee came about from the time she spoke critically of the PII Scheme at the Malaysian Bar AGM of 2008.

Rao obviously made a lot of sense in criticising the Scheme, and Bar Council invited her to sit on the Committee and thereafter she had been a very active, vocal and vital member of our committee.

Rao rarely missed any of our meetings and even at one of our last meetings before her passing, she contacted us to say that she was so sorry that she would not be able to make it as she was still hospitalised.

Earlier in the year, Rao informed us of her ill health and she felt that it would be unfair to the Committee if she remained a member but failed to turn up for meetings. The Committee unanimously agreed that she is welcome to remain and she can take as much time off for her convalescence.

Rao was very fluent in English and Bahasa Malaysia, and this assisted us greatly in carrying out *Getting Started!* workshops in the smaller towns where some lawyers were more comfortable to engage us in Bahasa Malaysia. She was a constant feature in all our trainings and despite her health issues, she would travel the length and breadth of the country to impart her knowledge to young lawyers and lecture law students.

Rao started her legal career in 1998 upon completion of LLB at IIUM. She practised as a legal assistant in Penang and Kedah before setting up her own practice in Kedah under the name and style of Messrs Rao Suryana in December 2003. Rao was a quiet and gentle lady but passionate about her work. She was very much involved with Kedah/Perlis Bar Committee activities and was twice the Chairperson for Kedah/Perlis Bar (term 2011/2012 and 2010/2011), Co-chairperson of YBGK (LAC) Kedah/Perlis 2011/2012.

Just weeks prior to her early demise, Rao Suryana informed us of her intentions to come back actively involved in Committee work in 2017. However, news of her death was a great shock to the PII Committee. Rao was a high spirited and wonderful person, never feared to voice her opinions.

She will be missed. Our thoughts and prayers are with her son and family.

O	N	L	E	R	A	W	E	M	O	S	N	A	R	F
M	S	A	A	N	T	I	Q	U	E	P	O	O	R	I
G	O	P	H	T	U	P	P	E	R	W	A	R	E	R
D	I	D	Y	T	O	H	S	P	A	M	W	A	R	E
A	E	R	A	W	L	A	M	T	O	K	Y	O	A	W
T	S	T	A	R	A	O	O	E	N	I	L	N	O	A
A	N	T	I	V	I	R	U	S	L	B	L	A	B	L
B	W	A	S	H	E	D	E	Z	I	R	K	G	K	L
R	A	N	C	L	O	U	D	S	T	O	R	A	G	E
E	L	Y	N	S	P	E	R	M	A	Z	S	P	A	M
A	L	F	E	Y	P	T	W	O	P	W	A	R	S	O
C	O	O	K	I	E	A	Z	F	I	G	X	M	A	S
H	I	S	O	H	O	W	Y	M	T	R	O	J	A	N
A	N	S	P	H	I	S	H	I	N	G	E	N	O	A
B	E	V	I	R	D	D	R	A	H	A	C	K	E	R

Word Challenge: CYBER

ANTIVIRUS (*antivirus*)

A software utility that detects, prevents, and removes viruses, worms, and other malware from a computer. Most antivirus programs include an auto update feature that permits the program to download profiles of new viruses, enabling the system to check for new threats. Antivirus programs are essential utilities for any computer but the choice of which one is very important. One antivirus program might find a certain virus or worm while another cannot, or vice-versa. Anti virus software is also known as an anti-virus program or a vaccine. **

*Atur cara yang digunakan untuk mengesan dan menghapuskan virus komputer.**

FIREWALL (*tembok api*)

A software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both. A firewall is recognized as the first line of defence in securing sensitive information. For better safety, the data can be encrypted. **

*Perisian atau perkakasan yang digunakan untuk mengawal capaian keluar dan masuk ke prasarana pengkomputeran organisasi berasaskan dasar keselamatan. Perisian atau perkakasan ini mempunyai petua semburan tembok api paras rangkaian tertib rotor. **

CLOUD STORAGE (*simpanan di alam maya*)

A cloud computing model in which data is stored on remote servers accessed from the Internet, or "cloud". It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualization techniques. **

Tempat simpanan maklumat di pangkalan maya.

DATA BREACH (*pelanggaran data*)

An incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach is also known as a data spill or data leak. **

Kejadian yang berlaku sama ada dengan sengaja atau tidak sengaja yang menyebabkan maklumat sulit dibaca, dicapai oleh pihak luar atau tersebar.

COOKIE (*kuki*)

A text file that a Web browser stores on a user's machine. Cookies are a way for Web applications to maintain application state. They are used by websites for authentication, storing website information/preferences, other browsing information and anything else that can help the Web browser while accessing Web servers. HTTP cookies are known by many different names, including browser cookies, Web cookies or HTTP cookies. **

Fail-fail (kecil) yang disimpan dalam komputer pengguna yang mempunyai maklumat spesifik komputer tersebut untuk memudahkan laman sesawang menjejak penggunaan laman tersebut.

HACKER (*penggodam*)

A person who can gain access into a computer system multiple times in many ways.

*Orang yang dapat menggunakan sesuatu sistem komputer selepas mencuba berkali-kali dengan pelbagai cara.**

HARD DRIVE (*cakera keras*)

A data storage device used for storing and retrieving digital information.

Peranti simpanan data yang digunakan untuk menyimpan dan mendapatkan semula maklumat digital.

MALWARE (*perisian hasad*)

Any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc, which steal protected data, delete documents or add software not approved by a user. **

*Perisian yang direka bentuk untuk memusnahkan sistem komputer tanpa pengetahuan pemilik komputer. Contoh perisian ini ialah virus komputer, cecacing, kuda Trojan, perisian pintu belakang, perisian intip, perisian jenayah dan sesetengah perisian iklan. Perisian hasad berbeza daripada perisian cacat. Perisian hasad dicipta untuk tujuan jahat manakala perisian cacat merupakan perisian yang sah tetapi mengandungi pepijat.**

ONLINE (*dalam talian*)

Controlled by or connected to a computer and as an activity or service which is available on or performed using the Internet or other computer network.

*Berada dalam talian. **

PHISHING (*memancing data*)

An attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.

*Cubaan dengan niat jahat dan menyalahi peraturan untuk mendapatkan maklumat sensitif dalam talian seperti usernames, passwords dan kad kredit, dengan menyamar sebagai entiti sah.**

RANSOMWARE (*perisian tebusan*)

Ransomware is a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner. Ransomware may also be referred to as a crypto-virus, crypto-Trojan or crypto-worm. **

*Perisian hasad yang menyulitkan cakera keras komputer yang dijangkiti. Penggodam hanya akan mengembalikan semula data asal dalam cakera tersebut dengan perisian nyahsulit sekiranya pemilik komputer tersebut membayar tebusan.**

SPAM (*spam*)

Unsolicited or undesired emails.

E-mel yang tidak diminta atau diingini.

SPAMWARE (*perisian spam*)

Spamware is a software utility designed specifically by spammers for spamming. Spamware enables a user to search, sort and compile a list of email addresses and provides an automated email broadcasting solution. This can be used to send spam or unsolicited emails to unsuspecting recipients. Not all software that sends bulk email is spamware, as email listserver software can be used for legitimate purposes, rather than spam. **

*Perisian yang digunakan oleh penspam untuk menghantar e-mel spam secara automatik. Pakej perisian ini juga termasuk dalam alat pungutan e-mel. **

SPYWARE (*perisian intip*)

An infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer. Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users. Peer-to-peer (P2P) file sharing has increased the proliferation of spyware and its ramifications. **

*Perisian yang dipasang secara tersembunyi pada komputer peribadi untuk memintas atau mengambil sebahagian kawalan ke atas interaksi pengguna dengan komputer tanpa pengetahuan pengguna tersebut. Perisian ini secara rahsia mengawasi tingkah laku pengguna seperti laman web yang dilawati dan tabiat melayari Internet. Perisian ini juga dapat mengganggu kawalan pengguna terhadap komputer seperti memasang perisian tambahan dan mengalih aktiviti pelayar web. Selain itu, perisian ini dapat mengubah pengesetan komputer, mengakibatkan kelajuan capaian menjadi perlahan dan sambungan rangkaian terputus serta ketidakfungsian atur cara lain. Perisian intip boleh juga diklasifikasikan sebagai perisian langgar privasi. **

TROJAN (*trojan*)

A seemingly benign program that when activated, causes harm to a computer system. A Trojan horse is also known as a Trojan virus or Trojan Horse. **

*Atur cara komputer yang berfungsi sebagai umpan seperti kuda Troy dalam dongeng Yunani. Atur cara ini kononnya berfaedah tetapi sebenarnya mengandungi suruhan yang diletakkan oleh pencipta atur cara untuk menceroboh keselamatan sistem komputer apabila atur cara digunakan. **

Credit:

* Portal atas talian Dewan Bahasa dan Pustaka Malaysia.

** www.techopedia.com

RISK AWARE!

A REVIEW OF YOUR FIRM

The objective of the *Risk Aware!* A Review of Your Firm ("Review") is to evaluate the present approach to risk management at legal firms within Peninsula Malaysia. Evaluation consists of a firm's current risk management methods, systems as well as procedures in the conduct of its everyday affairs. Another aim of the Review is to document the processes involved and help identify any weak or risky areas within a firm so that suggestions for improvement can be put forth.

The Review is designed to assist firms to:

1. Appraise current risk management systems and procedures;
2. Identify vulnerabilities and avoidable risk exposures;
3. Address areas which commonly give rise to professional indemnity claims; and
4. Identify recommendations for implementation.

While there is no clear guideline set by Bar Council and/or the Insurer on best practices to manage risk, the recommendations provided are approaches that a firm can choose to adopt to improve and avoid unnecessary risks. The recommendations made will serve as a guide to firms and provide a risk appraisal of the firm to assist in the identification of any avoidable risk exposures arising from the firm's present operating systems, methods and procedures, which may render the firm susceptible to complaints or professional negligence claims.

Risk Management is essential for every Firm. The idea behind implementing good risk management practices is so each and every client is provided with the best legal care and service. Proper risk management also protects both the Firm and client from any negative fallout, and in particular, protects the Firm from being sued.

The Review itself comprises of four stages: pre-interview, the interview, written report, and follow-up review (if necessary).

The selected areas included in the Review are:

1. Firm Management and Procedures
2. Accounts Management and Financial Operations
3. Conveyancing procedures
4. Litigation procedures and processes

Interviews will be conducted with appropriate individuals of the Firm such as the Sole Proprietor or Managing Partner, Legal Assistant and/or Heads of Departments. As an added benefit, a risk management session will also be conducted.

After the relevant information is gathered, a report with recommendations will be prepared based on observations made by the Officers conducting the Review. If necessary, a follow-up visit will be carried out to assess the implementation of the recommendations suggested earlier.

All data collected from the Firm will be kept confidential and will only be used to provide recommendations, maintain statistics and research for the PII Committee. The Officers will not observe or collect information in relation to client's confidentiality. The report will comprise of the following:

1.

Methodology and Firm Structure – The Methodology used and a description of the structure of the firm.

2.

Risk Management Systems and Procedures – The body of the report outlines the generic issues associated with various areas of practice management. This section also outlines observations and comments regarding the techniques and methods currently in operation in the firm to identify, review and control risks, as well our recommendations for improvement.

3.

Executive Summary – Containing principle recommendations.

If you are interested in having your Firm participate in the *Risk Aware!* A Review Of Your Firm, do contact us at 03-2032 4511 or drop an email to pirm@malaysianbar.org.my.

Remember, prevention is better than cure!

SERANGAN SIBER! ADAKAH ANDA BERSEDIA?

Pada masa kini yang bergantung kepada teknologi, adalah penting untuk mengetahui yang terkini tentang perkembangan dan bahaya teknologi agar sentiasa bersedia. Jika anda menggunakan salah satu daripada yang berikut:

peranti mudah alih, komputer riba, komputer meja, pelayar web dsb

edisi Jurisk! ini boleh membantu anda mengambil langkah pertama.

Adakah Anda *Online...?*

Anda yang menentukan maklumat yang didedahkan, bila, kenapa dan kepada siapa!

Tip untuk kata laluan

- Pilih kata laluan yang sukar untuk diramal oleh orang lain.
- Jangan menggunakan kata laluan yang sama pada setiap akaun.
- Pilih kata laluan yang panjang, unik, dan campuran antara nombor, huruf besar dan huruf kecil.
- Tukar kata laluan dengan kerap dan jangan kongsikan dengan orang lain.

Mengenalpasti e-mel palsu

- Alamat e-mel pengirim tidak sama dengan alamat laman sesawang organisasi yang sebenar.
- E-mel dihantar menggunakan alamat yang sangat berbeza atau alamat e-mel dari laman percuma.
- E-mel yang tidak dimulakan dengan panggilan nama, tetapi dengan panggilan umum seperti, “Kepada Pelanggan Kami”, “Kepada Pemenang”.
- E-mel yang seakan mendesak; contohnya, ugutan untuk menutup akaun anda ataupun nyawa seseorang dalam bahaya sekiranya tiada respon dari pihak anda.
- Pautan palsu yang diterima menggunakan nama sebuah organisasi yang terkenal.
- E-mel yang meminta anda untuk menyertakan butiran peribadi seperti nama dan kata laluan serta maklumat bank anda.
- Terdapat kesalahan kosa kata atau ejaan pada e-mel tersebut.
- E-mel yang menunjukkan seperti anda menantikan respon dari penghantar e-mel.
- Kesemua teks e-mel tersebut diletakkan di dalam sebuah imej berbanding format teks yang biasa. Imej tersebut mengandungi pautan yang akan membawa anda ke laman sesawang palsu.

Sebaiknya

- Menggunakan antivirus.
- Pastikan perisian anda sentiasa dikemaskini.
- Pastikan pautan dan alamat pada laman sesawang adalah sama sebelum diklik.
- Pastikan penghantaran data dibuat melalui laman yang selamat.
- Fikir sebelum berkongsi maklumat dilaman sosial.
- Berhati-hati ketika menggunakan Wifi awam/percuma.
- Kunci gajet anda dengan kata laluan.
- Sekiranya anda kehilangan gajet, cuba padamkan segala data di dalam gajet terbabit dengan menggunakan gajet yang lain.
- Awasi cara maklumat didedahkan kerana kebanyakan penggodam tidak memerlukan alat yang canggih untuk mendapatkan maklumat tersebut.
- Ambil masa untuk menyemak alamat e-mel yang digunakan.
- Lakukan carian dalam talian.
- Aktifkan peranti keselamatan.
- Pastikan pautan yang anda layari adalah selamat sebelum memasukkan butiran pembayaran melalui kad dimana-mana laman sesawang.
- Lebih peka terhadap keselamatan di atas talian.
- Pastikan e-mel mempunyai tetapan keselamatan yang diperlukan seperti penyulitan e-mel.
- Periksa lapangan “From” / “Daripada” apabila menerima atau sebelum menghantar e-mel.

Elakkan

- Klik pada pop-up yang tidak diperlukan, e-mel yang tidak diketahui dan lampiran pada e-mel.
- Klik pada e-mel yang diterima luar jangkaan anda.
- Memberikan maklumat anda kepada laman sesawang yang boleh diakses dengan mudah.
- Klik pada pautan yang jarang anda lihat.
- Menggunakan kata laluan yang sama untuk laman sesawang yang berbeza.
- Dedahkan maklumat sewenang-wenangnya melainkan anda yakin tujuan untuk digunakan.
- Menerima jemputan dari media sosial tanpa ragu-ragu.
- Menyimpan butiran kad kredit di atas talian.
- Mendedahkan nama dan kata laluan anda kepada orang lain.
- Membalas e-mel spam yang diterima atau kepada pengirim tanpa sebarang sebab.

Ancaman Siber Terhadap Firma Guaman

Awal tahun ini, lebih 40 buah firma guaman di Utara Amerika telah menjadi mangsa kepada sebuah kumpulan yang dipercayai penggodam dari Rusia. Modus operandi mereka adalah dengan menggodam sejumlah data peribadi yang digunakan untuk aktiviti dagangan dalam talian dan beberapa kesalahan lain. Kebanyakan daripada firma tersebut tidak mengetahui bahawa mereka adalah sasaran mahupun menyedari data mereka telah dicerobohi, sehinggalah siasatan penuh dijalankan.

Firma-firma yang terlibat bukanlah firma guaman yang sembarangan. Mereka menjadi sasaran khusus berdasarkan kerja yang dilakukan dan pelanggan yang mereka wakili. Mereka merupakan firma yang kukuh dan berjaya, serta membuat pelaburan berjuta-juta ringgit setahun hanya untuk memastikan rekod data mereka dilindungi. Sekiranya firma-firma besar yang stabil seperti ini boleh menjadi sasaran mudah, apatah lagi firma-firma yang bersaiz lebih kecil?

Pengamal undang-undang di Malaysia tiada bezanya. Sama seperti di Amerika, firma-firma guaman di Malaysia juga ditubuhkan atas dasar kepercayaan yang wujud diantara peguam dan klien itu sendiri. Secara amnya, peguam dan sesebuah firma guaman hendaklah melindungi klien mereka, serta maklumat-maklumat sulit dan penting yang berkaitan klien mereka. Maklumat-maklumat ini perlu dilindungi dengan rapi dan firma-firma guaman hendaklah mengambil langkah-langkah yang lebih proaktif bagi memastikan rekod data mereka tidak dicerobohi. Namun begitu, masih banyak firma yang bersikap sambil lewa tentang hal ini.

Mengapa Firma Undang-Undang Menjadi Sasaran?

Firma-firma guaman memiliki begitu banyak maklumat berharga, contohnya, peguam-peguam pemindahhakan yang mengendalikan urusan transaksi jual beli menyimpan segala maklumat berkaitan suatu hartanah yang terlibat. Peguam-peguam litigasi yang mengendalikan kes-kes keluarga pula menyimpan butiran peribadi, jumlah keseluruhan harta, portfolio menyeluruh, harta peribadi dan urusan perniagaan klien mereka. Begitu juga peguam-peguam komersial yang khusus mengendalikan kes-kes penggabungan dan pemerolehan menyimpan maklumat berharga klien seperti kedudukan kewangan, hak cipta dan tanda niaga, serta pelan perniagaan yang bakal diusahakan kelak.

Pada zaman ini, nilai maklumat serta rekod data sedemikian boleh dihitung bersamaan dengan nilai emas dan mata wang. Data yang digodam dari firma guaman inilah yang akan digunakan untuk pelbagai aktiviti penipuan oleh penggodam. Jual beli dalam talian, pengintipan korporat, kecurian identiti, dan menggodam sistem perbankan adalah hanya sebilangan kecil kes yang sering didengari. Banyak lagi kes penipuan yang boleh dilakukan melalui penggodaman. Firma-firma bersaiz sederhana lebih kerap menjadi sasaran berbanding firma-firma bersaiz besar kerana sistem keselamatan untuk melindungi data mereka adalah kurang memuaskan. Sistem firma-firma bersaiz sederhana juga lebih mudah ditembusi dan maklumat yang diperolehi adalah sama nilainya dengan firma-firma besar yang lain.

Kos Serangan Siber

Pendedahan maklumat rahsia yang dikenali sebagai "Panama Papers" telah pun meragut jawatan Perdana Menteri Iceland dan seterusnya telah mendorong persoalan-persoalan kurang selesa terhadap bekas Perdana Menteri United Kingdom sebelum ini, David Cameron yang turut dinamakan didalam dokumen tersebut. Sebenarnya, ia seharusnya mengakibatkan impak yang lebih besar lagi.

Dokumen-dokumen dari firma guaman Mossack Fonseca itu juga turut mengandungi beberapa nama klien lain yang berprofil tinggi di serata dunia. Menurut International Consortium of Investigative Journalists[1], secara keseluruhannya sejumlah 140 ahli politik dan penjawat awam serta lebih 214,000 pertubuhan telah dinamakan didalamnya.

Skandal "Panama Papers" telah membuktikan bahawa kebocoran maklumat di dalam sesebuah firma guaman boleh mendatangkan kesan yang besar, bukan sahaja kepada klien malahan juga kepada mereka yang berkait rapat dengan klien berkenaan. Jika data sulit dicerobohi dan akhirnya terdedah, klien akan berada dalam keadaan yang tidak dilindungi. Data peribadi, urusan perniagaan dan rakan perniagaan yang berkenaan akan menjadi berkepentingan kepada pelbagai pihak, lebih-lebih lagi sekiranya orang-orang yang dinamakan didalamnya adalah tokoh-tokoh awam atau orang-orang yang terkenal.

Bukan itu sahaja, reputasi firma terbabit juga tergugat oleh kerana kini firma tersebut akan sering dikaitkan dengan skandal tersebut. Lebih teruk lagi, firma itu juga akan berdepan dengan kemungkinan kehilangan beberapa klien, sama ada yang sedia ada mahupun bakal klien.

Apa yang Harus Firma Lakukan?

Anda boleh memilih untuk terus bersembunyi disebalik batu dan yakin anda tidak akan menjadi mangsa jenayah siber, ataupun anda boleh keluar dari tempat persembunyian dan lebih berhati-hati. Jika anda rasa anda terlalu kecil seperti ikan, fikir semula! Jenayah siber tidak mengira saiz firma mangsa mereka, tetapi hanya satu yang menjadi tumpuan utama: maklumat yang anda lindungi.

Dalam tahun 2014, SOPHOS, sebuah syarikat keselamatan IT yang berpangkalan di Amerika Syarikat telah menyenaraikan Malaysia ditangga keenam dunia sebagai negara yang paling berisiko dengan ancaman siber, dengan jumlah kerugian sebanyak $300 juta (RM1.2bilion). Ini bermaksud, secara puratanya, rakyat Malaysia tidak mengambil berat tentang kepentingan data keselamatan di internet. Ini juga bermakna, firma guaman **PERLU** bersikap lebih proaktif dan serius dalam menjaga amanah yang diberikan oleh klien kepada mereka.

Tidak kira sama ada firma milikan tunggal, kecil mahupun sederhana, kesemuanya perlu berusaha untuk mencari penyelesaian terbaik yang boleh digunakan untuk melindungi data. Kebanyakan firma guaman tahu dan faham akan kepentingan melindungi kebocoran data, tetapi mereka tidak tahu apakah langkah yang harus diambil. Menggaji pekerja IT yang baru tamat pengajian sahaja adalah tidak mencukupi. Menggunakan "Enterprise Solution System" yang agak mahal, rumit dan tidak begitu sesuai untuk firma kecil dan sederhana juga tidak memadai.

Apabila anda telah mendapat penyelesaian yang bersesuaian, sediakan prosedur keselamatan yang merangkumi keseluruhan firma anda. Prosedur ini perlu disimpan dalam bentuk dokumen yang boleh diedarkan dan dipatuhi oleh semua pekerja di firma termasuklah, Rakan Kongsi, Pembantu Undang-Undang, kerani dan kakitangan sokongan. Minta kerjasama Rakan Kongsi anda untuk memastikan prosedur IT berkenaan diguna pakai di dalam firma tersebut.

Kita mempunyai kewajipan menjaga kerahsiaan klien, dan kita berkewajipan untuk terus memastikan data klien dalam keadaan selamat. "Selamat" sebenarnya bukan hanya melindungi data daripada jatuh ke tangan orang yang tidak bertanggungjawab, tetapi ia turut menguji integriti diri kita sendiri dalam mengekalkan maklumat itu sebagai sulit walaupun kita mempunyai akses. Melindungi keselamatan sesebuah firma guaman adalah usaha beterusan dan memerlukan polisi diimplementasikan.

[1] https://panamapapers.icij.org

Tip Teknologi Buat

Milikan Tunggal & Peguam yang Baru Menubuhkan Firma Sendiri

Ditulis oleh Jeremiah Rais, pupil-in-chamber.
Terjemahan oleh Azwa Zulsamli

Gaya dan pertuturan seorang peguam itu mungkin kelihatan agak kuno, namun itu tidak seharusnya menjadi halangan buat anda dalam menyahut cabaran abad ke-21. Sungguhpun kebanyakkan firma guaman tidak dilengkapi dengan sumber atau tenaga pakar untuk mewujudkan robot dengan kepandaian luar biasa yang boleh menandingi peguam lebih muda dan paralegal, anda masih boleh dan perlu menggunakan cara lain untuk menggantikan kerja keras dengan membuat kerja dengan pintar.

Atur Diari Anda

Telefon pintar telah menjadi keperluan penting pada zaman sekarang, sepertimana pentingnya sebongkah kayu pada zaman batu nenek moyang kita dahulu. Telefon pintar sering digunakan ketika anda meluangkan masa dalam perjalanan ke tempat kerja, adalah lebih baik jika ia digunakan untuk mengatur jadual kerja anda. Terdapat fungsi kalendar pada kebanyakkan e-mel yang boleh digunakan untuk mengatur jadual harian. Ini amat berguna dalam membantu anda mencatit tarikh-tarikh penting, sama ada tarikh temujanji dengan klien atau tarikh memfailkan kes di mahkamah.

Kalendar ini boleh diselaraskan ke telefon pintar atau tablet tanpa perlu mengemaskini maklumat secara berasingan tanpa wayar. Ini membolehkan anda lebih peka dengan tarikh-tarikh penting tidak kira dimana jua anda berada, mahupun jika anda kehilangan salinan keras diari sekiranya berlaku kebakaran.

Jangan sia-siakan ciri asas yang telah tersedia dalam telefon pintar anda – ada sebab kenapa peranti PDA yang dikeluarkan awal tahun 2010 telah ketinggalan!

Komunikasi

Kepantasan dalam membuat keputusan boleh dicapai sekiranya terdapat komunikasi yang berkesan. Komunikasi juga merupakan kunci kecekapan bagi setiap amalan undang-undang. Pertimbangkan penggunaan mesej segera untuk perbincangan pantas dengan pekerja walaupun mereka berada di bilik sebelah atau di tempat yang lain. Fungsi seperti perkongsian dokumen dan perbualan kumpulan membolehkan anda untuk bertukar-tukar idea dengan lebih mudah. Kemudahan mesej segera ini tidak seharusnya diketepikan – bilangan mesyuarat mingguan yang menggerunkan dapat dikurangkan dengan hanya mengemaskini status kes yang anda kendalikan di mana saja anda berada.

Mesej yang dihantar boleh diakses dari sebarang peranti dengan sambungan internet melalui pelbagai cara komunikasi lantas meningkatkan kecekapan ditempat kerja. Apa yang lebih penting adalah, mesej ringkas dapat menjimatkan penggunaan kertas dan kebanyakkan pembekal perkhidmatan menyediakan enkripsi hujung-ke-hujung, dimana secara teorinya ini dapat menghindar komunikasi anda dan rakan sekerja dari diketahui oleh orang lain. Walaupun hampir kesemua kemudahan mesej ringkas memerlukan sedikit pelaburan, ia merupakan pilihan terbaik, bahkan untuk firma guaman yang mempunyai sumber terhad.

Footnote [1] Jane Croft, 'Legal Firms Unleash Office Automatons' Financial Times (16 May 2016) <http://www.ft.com/cms/s/0/19807d3e-1765-11e6-9d98-00386a18e39d.html#axzz4HiLoOIR6> accessed 10 August 2016

Page 25

Menggaji Bakat

Jangan lepaskan peluang untuk menggaji peguam muda yang baru tamat pengajian dengan meneliti media sosial mereka. Anda tidak perlu lagi menggunakan khidmat pencari bakat atau iklan berbayar untuk mendapatkan pekerja kerana ia boleh dilakukan dengan carian di laman web seperti LinkedIn dan Jobstreet. Kebelakangan ini, kebanyakkan golongan profesional muda mempunyai profil dan vitae kurikulum yang lengkap di laman web sosial yang berorientasikan perniagaan. Ini dapat memudahkan kerja anda untuk memilih mereka yang paling layak bagi jawatan yang ditawarkan tanpa bantuan dari Jabatan Sumber Manusia.

Seandainya keputusan masih tidak dapat dicapai berdasarkan maklumat yang ada, carian pantas ke atas nama atau e-mel calon pekerja boleh dilakukan, dan kemungkinan untuk menemui satu dua profil media sosial mereka adalah tinggi. Ini boleh menjadi kayu pengukur untuk menilai personaliti individu terbabit, malahan juga dapat menguji tahap penguasan penulisan Bahasa Inggeris mereka sebelum datang ke temuduga. Apabila pilihan telah dibuat dan calon tersebut berada di luar kawasan, temuduga secara persidangan video boleh dipertimbangkan.

Kajian Undang-Undang

Tanpa sumber undang-undang, sesebuah firma guaman itu tidak dapat berfungsi dengan baik. Namun melengkapkan sebuah perpustakaan dengan buku, laporan atau kajian undang-undang boleh membocorkan poket sesebuah firma udang-undang lebih-lebih lagi firma yang baru ditubuhkan atau yang bersaiz kecil. Sebagai pilihan, anda boleh melanggan pangkalan data undang-undang atas talian untuk mendapatkan maklumat berkaitan bidang amalan atau pihak berkuasa undang-undang dengan lebih meluas sejajar keperluan anda.

Pangkalan data undang-undang atas talian bukan sahaja menjimatkan dari segi kos, malahan juga menjimatkan masa dan tenaga semasa menjalankan kajian undang-undang dengan membawa perpustakaan undang-undang terbaik dunia terus ke meja anda. Anda tidak perlu lagi meneliti buku undang-undang yang tebal dan berat untuk menyemak tentang sesuatu prinsip, sebaliknya hanya dengan satu klik sahaja. Kebanyakkan pangkalan data undang-undang memberikan tempoh percubaan kepada pelanggan mereka dan peluang ini harus diambil bagi menentukan keperluan melanggan perkhidmatan tersebut.

Kewujudan Atas Talian

Laman web yang direka secara profesional merupakan salah satu kunci dalam membina kredibiliti sesebuah firma guaman, setanding nama-nama besar yang lain di dalam profesion undang-undang. Kecanggihan teknologi sekarang telah membantu klien untuk menentukan firma guaman pilihan mereka. Dengan adanya laman web rasmi, nama firma akan dimasukkan ke dalam enjin carian dan berpeluang untuk dipilih. Laman web yang menarik dan meyakinkan mampu menarik perhatian prospek klien, kerana pendekatan yang diambil menunjukkan firma tersebut berpandangan jauh.

Laman web juga boleh digunakan sebagai medium untuk menyuarakan kepakaran dan berkongsi pengalaman dalam mengendalikan kes-kes tertentu kepada pembaca diseluruh dunia. Ia merupakan peluang baik untuk mendapat kepercayaan bakal klien untuk memilih anda mewakili mereka.

Selain menjadi alat pemasaran yang baik, laman web turut membuatkan anda lebih dekat dengan klien. Jika terdapat sebarang pertanyaan, laman web firma akan dijadikan tempat rujukan pertama sebelum tindakan lain diambil. Oleh kerana ianya boleh diakses pada bila-bila masa, klien yang telah membuat keputusan berdasarkan maklumat firma yang tertera di laman web akan memilih untuk menggunakan khidmat anda berbanding firma yang tidak mempunyai laman web. Bukan itu sahaja, anda juga boleh mengoptimumkan asas carian enjin untuk memastikan kata kunci tertentu akan membawa pencari maklumat terus ke laman web anda. Ini dapat membuka mata klien anda yang semakin celik teknologi bahawa anda serius dalam apa yang anda lakukan.

BAHANA RANSOMWARE

Virus *ransomware* atau bahasa Melayunya perisian tebusan merupakan virus yang merbahaya dimana jika ianya diaktifkan, boleh menyulitkan seluruh sistem komputer dan juga sebarang peranti yang bersambung dengan komputer tersebut tidak boleh digunakan lagi. Kemudian, anda akan menerima mesej daripada entiti yang tidak dikenali untuk membuat sejumlah bayaran bagi mendapatkan 'kunci' untuk membuka data anda yang disulitkan tadi dan (dengan harapan) akhirnya boleh diguna pakai semula.

Virus *ransomware* ini kebanyakannya dihantar melalui e-mel *phishing* kepada pengguna komputer. Di awal kemunculannya, virus ini agak mudah dikenalpasti dan pengguna komputer dapat menyedari e-mel tersebut adalah palsu, lantas segera membuangnya. Namun, sejak kebelakangan ini, pemalsuan e-mel semakin berleluasa dan pendekatan yang digunakan juga telah mengelirukan sesebuah organisasi mahupun individu itu sendiri, dan membuatkan mereka masuk dalam perangkap.

Cubaan ke atas Firma Guaman

Secara ringkasnya, *ransomware* ialah virus yang menyekat akses kepada data yang disimpan di dalam komputer dan mengarahkan pengguna untuk membayar sejumlah wang bagi membuang sekatan tersebut. Kegagalan dalam membuat bayaran yang diminta akan mengakibatkan kesemua data yang disulitkan terpadam buat selamanya.

Firma guaman yang lazimnya memberikan perkhidmatan undang-undang adalah lebih menarik perhatian kerana menyimpan maklumat peribadi klien yang berpengaruh di dalam sistem komputer mereka. Firma guaman yang terlibat selalunya terpaksa akur dengan kehendak penjenayah siber tersebut dan bersetuju membuat bayaran bagi mendapatkan kembali maklumat klien mereka demi menjaga reputasi firma serta klien berkenaan.

Bagaimana ia Dilakukan?

Langkah 1

Pengguna menerima satu e-mel yang kelihatan biasa. Terdapat dua kemungkinan daripada e-mel seperti ini:

1. E-mel tersebut mengandungi lampiran yang merbahaya, seperti fail sambungan yang berbentuk .pdf, .doc, .xls, and .exe. Lampiran-lampiran ini kelihatan biasa dan tiada salahnya, seperti invois atau faks elektronik, tetapi mengandungi kod merbahaya yang boleh menyerang pengguna sekiranya dimuat turun.
2. Menerima e-mel yang nampak biasa tetapi mengandungi pautan ke laman sesawang yang dicemari virus merbahaya. Apabila pengguna membuka fail merbahaya ataupun mengklik pautan di dalam e-mel palsu tersebut, segala data pengguna yang menyimpan maklumat kritikal mengenai perniagaan akan disulitkan secara automatik.

Langkah 2 & 3

Virus merbahaya akan dimuat turun ke dalam komputer anda dan segala fail yang terkandung di dalam komputer tersebut akan disulitkan oleh penggodam. Selain itu, virus tersebut akan terus menyulitkan kesemua fail yang disimpan di dalam seluruh sistem komputer firma sekiranya komputer berkenaan besambung dengan peranti yang lain. Fail yang disulitkan akan terkunci dan tidak boleh digunakan. Firma tidak akan dapat untuk membuka fail-fail yang berkaitan atau membuat salinan sandaran, dan fail-fail tersebut berkemungkinan akan hilang selamanya.

Langkah 4

Pengguna akan menerima notis tebusan daripada penggodam yang turut mengandungi butiran, cara dan tarikh tamat tempoh pembayaran.

Langkah 5

Setelah bayaran dibuat, (Nota: **adalah dinasihatkan untuk tidak membuat sebarang bayaran, lihat di bawah**), firma akan diberikan satu kod 'kunci' untuk membuka fail-fail yang telah disulitkan. Selepas itu, fail-fail ini (berkemungkinan) boleh digunakan semula.

Jangan Membuat Bayaran Tebusan

Walaupun ianya nampak mudah dengan hanya membayar jumlah tebusan bagi mendapatkan kembali maklumat yang hilang, kebanyakkan pakar keselamatan siber tidak menggalakkan langkah tersebut diambil. Ini berikutan peluang untuk mendapatkan kembali maklumat yang disulitkan itu adalah sangat tipis.

Juga adalah tidak mustahil anda akan dijadikan sasaran sekali lagi kerana anda telah meyakinkan penggodam yang anda sanggup mengeluarkan sejumlah wang untuk mendapatkan kembali maklumat yang telah hilang. Langkah yang boleh dilakukan untuk mengelak daripada menjadi mangsa adalah melalui pencegahan.

Pengguna boleh mencegah dari serangan perisian tebusan dengan cara-cara berikut:

1. **Elakkan dari mengklik pautan yang mencurigakan.** Setiap firma seharusnya lebih serius dalam mewujudkan kesedaran dengan memberi informasi tentang bahayanya virus ini kepada pekerja-pekerja mereka. Ini termasuklah kemampuan pekerja itu sendiri dalam mengenalpasti ancaman perisian tebusan yang dihantar melalui e-mel dan laman sesawang palsu.

2. **Membuat salinan data-data penting.** Jika peranti ataupun sistem komputer telah dijangkiti virus, salinan data merupakan cara yang terbaik untuk memulihkan data penting anda. Paling kurang, anda hanya akan kehilangan data beberapa hari sahaja. Penyalinan data bagi sesebuah firma hendaklah dijadikan rutin tetap dan seorang pekerja dipertanggungjawabkan untuk melakukannya. Namun begitu, penyalinan data sahaja adalah tidak mencukupi. Data-data tersebut juga perlu dilindungi dari tersebar untuk tujuan yang tidak baik. Elakkan menyimpan salinan data di dalam komputer yang bersambung dengan komputer yang lain mahupun dirangkaian yang disangka selamat. Sebaiknya salinan disimpan di cloud storage atau peranti yang tiada talian internet seperti pemacu luaran dan storan fizikal luar talian. Terdapat juga perisian tebusan yang mampu menyulitkan data yang disimpan di dalam *cloud storage* sewaktu sistem membuat salinan pada masa sebenar.

3. **Periksa berkali-kali.** Kenal pasti penghantar e-mel dan semak kandungan mesej yang dihantar. Sila lihat muka surat 17 untuk mendapatkan tip keselamatan e-mel.

4. **Pastikan perisian anda dikemaskini.** Pastikan antivirus yang digunakan difirma anda dikemaskini secara automatik dan imbasan virus dilakukan secara berkala seperti yang ditetapkan.

5. Untuk tip mengelak daripada ancaman siber, baca tip di muka surat 6.

Kajian Kes

JANGAN JADI MANGSA KEPADA JENAYAH SIBER

Ditulis oleh David Ng, Senior Manager, Malaysian Bar Scheme Department.
Jardine Lloyd Thompson Sdn Bhd, Terjemahan oleh Azwa Zulsamli.

Kajian Kes 1:

Penipuan Siber Yang Umum Terjadi

Firma guaman menerima arahan melalui e-mel untuk mendepositkan sejumlah wang ke akaun bank yang kononnya milik klien (dirujuk sebagai "Akaun Bogus"). Firma itu bernasib baik kerana mengambil tindakan untuk membuatkan pengesahan dengan klien mereka melalui panggilan telefon dan terselamat dari menjadi mangsa.

Didapati, penipuan ini terjadi apabila si penyamar berjaya menggodam akaun e-mel firma guaman dan/atau klien, lalu memintas komunikasi diantara mereka. Kemudian, penyamar akan bertindak sebagai klien dan menghantar e-mel kepada firma guaman untuk memindahkan wang ke Akaun Bogus. Untuk meyakinkan firma yang penyamar ini adalah klien, segala maklumat yang terdapat dalam e-mel sebelum ini (komunikasi antara klien sebenar dan firma) turut dinyatakan di dalam e-mel penyamar itu. Ini memberi tanggapan yang firma sedang berurusan dengan klien sebenar.

Selain itu, alamat e-mel yang digunakan si penyamar itu juga turut didapati hampir sama dengan alamat e-mel klien sebenar, yang selalu digunakan untuk memberi arahan kepada firma. Firma tersebut telah membuat laporan kepada polis dan Suruhanjaya Komunikasi dan Multimedia Malaysia ("SKMM").

Kajian Kes 2:

Pengesahan Bertulis Yang Sepatutnya Dibuat

Amalan Yang Diinsuranskan ("IP") telah menghantar e-mel kepada klien mereka untuk memberitahu tentang hasil jualan tanah yang telah didepositkan. Keesokkan harinya, e-mel tersebut telah dibalas oleh klien yang memberitahu jumlah wang yang dinyatakan di dalam e-mel adalah tidak tepat. Berikutan percanggahan itu, klien turut menghubungi IP untuk berbincang dengan lebih lanjut.

Klien tersebut mengulangi butiran e-mel yang dibalas untuk membuktikan identitinya kepada IP, dan menerusi perbualan melalui telefon, klien meyakinkan IP untuk membuat pembayaran ke akaun Bank of Doomsday. IP mengikut arahan tersebut dan memindahkan bayaran hasil jualan tersebut daripada akaun IP di Bank of Integrity.

Sejurus pembayaran dibuat, slip pembayaran di e-mel kepada klien sebagai bukti transaksi. Lewat petang itu, klien yang sebenar menghubungi IP dan menafikan e-mel tentang arahan memindahkan wang ke Bank of Doomsday. IP kemudian segera memaklumkan Bank of Integrity mengenai apa yang berlaku dan laporan polis turut dibuat.

Kajian Kes 3:

Hampir Kehilangan Reputasi

IP telah menerima e-mel daripada Mr Irwin yang berada di Australia untuk mengesahkan identiti salah seorang rakan kongsi firma yang dikenali sebagai T Bundy. Ini berikutan Mr Irwin telah dihubungi oleh T Bundy yang mendakwa dirinya merupakan wakil dari sebuah badan amal.

T Bundy kemudian menguhubungi Mr Irwin untuk mendapatkan pengesahan tentang e-mel yang diterimanya. Ketika itulah T Bundy menyedari seseorang telah menyamar sebagai dirinya di dalam e-mel tersebut dengan menggunakan nama "T Bundy the Attorney". Penyamar itu telah menjanjikan sejumlah wang benilai USD2.6 juta yang disimpan di Bank of Honesty akan dipindahkan ke dalam akaun Mr Irwin. Penyamar itu turut meyakinkan Mr Irwin yang dia boleh membantu dalam memindahkan dana tersebut tanpa sebarang liabiliti cukai kerana ia merupakan sumbangan. Namun, menurut penyamar itu, sebelum dana tersebut boleh dipindahkan, En Irwin perlu memasukkan RM20,000.00 ke dalam akaun di Bank of Honesty sebagai yuran guaman menggunakkan perkhidmatannya.

Ini telah menimbulkan keraguan kepada Mr Irwin yang lantas menghubungi firma terbabit untuk mengesahkan identiti T Bundy. T Bundy yang sebenar turut mengesahkan pihaknya tidak membuat sebarang tawaran seperti yang dinyatakan oleh penyamar di dalam e-mel tersebut. Laporan polis segera dilakukan oleh T Bundy bagi mengelakkan sebarang kejadian yang tidak diingini.

Kajian Kes

Kajian Kes 4:

Satu Klik Hilang Semua

IP menerima e-mel beserta pautan ke pelayan awan yang dihantar oleh seorang klien. Menurut klien tersebut, pautan berkenaan adalah untuk melihat ke dokumen yang dikongsikan di dalam pelayan itu. Selepas mengklik pautan, IP terus dibawa ke laman log masuk.

Laman log masuk tersebut kelihatan hampir serupa dengan sebuah pelayan awan yang terkenal dan digunakan oleh IP. Tanpa rasa ragu-ragu, IP telah memasukkan nama dan kata laluannya untuk melihat dokumen yang dinyatakan. Akibatnya, webmail IP telah digodam dan IP telah dilog keluar dari webmailnya sendiri. Penggodam mengambil kesempatan untuk menggunakan senarai kenalan IP dan menghantar e-mel bagi mendapatkan derma. Mereka yang menerima e-mel itu diminta untuk membalas dan melengkapkan maklumat peribadi yang diminta.

Menyedari apa yang terjadi, IP terus memaklumkan kepada pembekal perkhidmatan pelayan awan tersebut. IP juga telah mencuba sehabis daya untuk mendapatkan semula akaun webmailnya kembali. Bimbang e-melnya akan digunakan untuk tujuan yang tidak baik, IP segera membuat laporan kepada pihak polis.

Kajian Kes 5:

Baca Keterangan

Kerugian yang dialami melibatkan jual beli hartanah. IP telah dilantik untuk mewakili penjual dalam transaksi ini. Sepanjang masa, IP berhubung dan menerima arahan daripada akaun e-mel kliennya, "mno123456@email.com".

Kemudian IP menerima arahan untuk menyerahkan hasil penjualan hartanah itu kepada pihak ketiga. Arahan dituruti oleh IP tanpa mengesyaki apa-apa.

Tidak lama selepas itu, IP menerima panggilan telefon daripada klien dan bertanyakan tentang hasil jualan hartanah yang diuruskan IP. IP memaklumkan wang berkenaan telah dipindahkan seperti yang diarahkan namun klien menafikan yang dia telah menerima wang mahupun memberi arahan tersebut. Berdasarkan semakan yang dilakukan, IP menyedari terdapat sedikit perbezaan pada alamat e-mel yang digunakan oleh kliennya sebelum ini dengan alamat e-mel yang mengarahkan pembayaran dibuat kepada pihak ketiga. Malangnya IP tidak dapat mengesan perbezaan pada kedua-dua alamat e-mel berkenaan kerana perbezaan masa hanya selang beberapa minit.

IP mengesyaki e-mel firma terbabit telah digodam dan penggodam mungkin telah mengetahui tentang urusan jual beli tersebut. IP terus membuat laporan polis sejurus perkara tersebut diketahui.

Untuk mengelak daripada menjadi mangsa dalam situasi yang sama, baca tip siber di muka surat 22 dan Pekeliling Bar Council di muka surat 32.

Apabila Yang Tidak Dijangka Berlaku

Apabila seorang pemilik tunggal meninggal dunia secara tiba-tiba, penutupan teratur firma tersebut dan fail-fail klien perlu diuruskan. Perkara yang sama juga perlu diuruskan sekiranya pemilik tunggal sebuah firma tidak dapat meneruskan amalan guamannya untuk suatu tempoh yang tidak dapat dijangkakan lanjutan daripada masalah kesihatan yang serius.

Berikut adalah dua senario yang mungkin berlaku dalam keadaan sedemikian:

Senario 1

Setelah suatu pemakluman kematian Ahli dibuat, Majlis Peguam akan menulis surat kepada anggota keluarga Ahli yang telah meninggal untuk mengetahui dan / atau memaklumkan antara lain perkara-perkara berikut:

- jika Ahli tersebut semasa hayatnya ada membuat perancangan berhubung pengurusan fail-fail serta akaun-akaun firmanya sekiranya saat kematiannya yang tidak dijangka tiba, dengan membuat pencalonan seorang peguam untuk mengambil alih fail-fail klien dan akaun-akaun firmanya;
- jika tiada, adakah ahli keluarga tersebut dapat melantik seorang peguam untuk mengambil alih fail-fail dan akaun-akaun firma tersebut; atau
- jika ahli keluarga tersebut memilih Majlis Peguam mengendalikan urusan-urusan tersebut.

Senario 2

Setelah dimaklumkan berhubung suatu keadaan kesihatan yang serius seseorang Ahli, Majlis Peguam akan berhubung dengan Ahli tersebut atau anggota keluarga Ahli tersebut (bersesuaian dengan keadaan), untuk bertanya jika Ahli tersebut atau anggota keluarga Ahli tersebut dapat melantik peguam lain untuk mengambil alih fail-fail dan akaun-akaun firma tersebut.

Professional Indemnity Insurance Cover

Sesuatu tuntutan terhadap estet seorang Ahli yang telah meninggal berkaitan fail-fail yang telah dikendalikan semasa hayatnya masih boleh dibuat (bergantung kepada statut had masa). Sehubungan dengan ini, syarikat insurans adalah bertanggungjawab di bawah Skim Insurans Indemniti Profesional ("PII") untuk menyediakan indemniti berhubung tuntutan sedemikian berdasarkan terma-terma dan syarat-syarat polisi. Indemniti tersebut juga diperluaskan untuk merangkumi kos-kos berkenaan kos penuntut, kos pembelaan dan kos mitigasi.

Perlindungan yang disediakan di bawah Skim PII untuk bekas Ahli tersebut adalah berdasarkan tahun polisi terakhir bekas Ahli tersebut. Ini bermakna had mandatori dan *base excess* terakhir bekas Ahli tersebut adalah terpakai.

Estet Ahli tersebut mesti membuat pemberitahuan kepada syarikat insurans dalam tempoh 60 hari sekiranya mereka menerima sebarang writ, surat tuntutan, ancaman untuk mendakwa atau sebarang kebarangkalian yang boleh membawa kepada tuntutan.

Kebajikan Pemilik Tunggal atau ahli keluarganya

Jawatankuasa LawCare di bawah Majlis Peguam juga akan memainkan peranan penting dalam menyediakan bantuan kewangan kepada Ahli-ahli atau keluarga mereka dalam kes-kes berkaitan masalah kesihatan yang serius, kehilangan upaya atau kematian.

Pembayaran dalam kes-kes masalah kesihatan yang serius atau kehilangan upaya

Sekiranya seorang Ahli hilang keupayaan samada kekal atau sebahagian, jumlah sebanyak RM40,000 (atau peratusan daripada jumlah ini) akan dibayar kepada Ahli.

Pembayaran selepas kematian seorang Ahli

Pembayaran berjumlah RM42,000 akan dibuat kepada waris / pemegang amanah / penama (untuk Ahli bukan Islam) atau kepada benefisiari mengikut prinsip faraid (untuk Ahli Muslim) sekiranya seorang Ahli meninggal dunia.

Dalam kedua-dua kes diatas, pembayaran berjumlah RM30,000 (dan RM2,000 tambahan) akan dibayar daripada polisi insurans kumpulan, dan RM10,000 lagi akan dibayar daripada Kumpulan Wang LawCare.

Sehubungan dengan perkara di atas, ia adalah amat berfaedah untuk Ahli membuat penamaan bagi memudahkan proses bayaran. Untuk maklumat lanjut sila hubungi Sekretariat Bar Council atau muat turun, isi dan kembalikan borang pencalonan daripada laman web Bar Council di bawah "> Borang Sering Digunakan Resources".

Majlis Peguam
Bar Council Malaysia

www.malaysianbar.org.my

15 Leboh Pasar Besar
50050 Kuala Lumpur, Malaysia
Tel : +603-2050 2050
Fax : +603-2026 1313, 2034 2825, 2072 5818
Email : council@malaysianbar.org.my

Circular No 137/2014
Dated 1 July 2014

To Members of the Malaysian Bar

Practice Alert: Legal Firm Scammed into Releasing Client's Money to Fraudster

It has come to Bar Council's attention that a legal firm has been scammed into releasing its client's money to a bank account based on information by a fraudster.

The legal firm received instructions by telephone to transfer balance monies to a bank account purportedly belonging to its client (hereinafter referred to as "Account ABC"). This was subsequently confirmed in writing, through email. All checks and verifications with the client were confirmed through email correspondence.

It is believed that the fraudster intercepted the legal firm's emails by hacking into the email accounts of the legal firm and the client. The fraudster then posed as the client and provided instructions for the money to be transferred to Account ABC. The fraudster also provided information believed to have been extracted from previous email correspondence between the legal firm and the client, to bolster the fraudster's credibility as the purported client. This led the legal firm to believe that it was dealing with its actual client.

The actual client later called the legal firm to enquire about the proceeds. Upon being told of the payment that the legal firm had made, the client asserted that no instructions had been given to transfer money to Account ABC, and the client had not received any money.

The police are currently investigating the matter.

Members of the Bar are urged to be wary of communications involving emails, particularly any request, which relies on email, to transfer funds.

What Can You Do?

Some protective measures that Members can implement include:

(1) Verify instructions in person

It is best to verify instructions that are received, particularly those involving financial transactions, in person or by telephone. If conflicting or unusual instructions are given subsequent to an earlier verification by email, confirm the instructions again in person or by telephone. Do not rely solely on email communications for verification.

(2) Check the sender's email address

Some free email providers do not automatically display the sender's email address unless the user **expands** the "From:" field in the header section of the email. If your dealings with your client are by email, make it a habit to always check the "From:" field to ensure that emails you receive are actually being transmitted from your client's email address. If the address appears unusual, always speak to your client to verify the email! Do not reply to that email address.

(3) Know your client

Some fraudulent schemes may be perpetrated with the help of a client. Run a background check first if you are dealing with a client you are not familiar with. Refer to the 100-Point Identity Checklist on the *Praktis* website.

(4) Prevent hacking!

Boost your Internet security settings by taking these quick steps:

(a) **Use safe email practices** — Check that your firm's email settings have the requisite security settings, such as encryption of emails. If you are using a web-based free email provider such as Gmail or Yahoo Mail, ensure that your emails are encrypted using Secure Sockets Layer ("SSL") technology. SSL-encrypted web pages can be identified by the little padlock icon displayed on the browser page or by the fact that the URL begins with "https" rather than "http".[1] It is not advisable to send emails, especially those containing sensitive information, over open or public Wi-Fi connections, as these connections are unsecured and may be vulnerable to hacking activities.

(b) **Keep software up to date** — Vendors of operating systems or software applications often issue updates to fix existing vulnerabilities. Update your operating systems and browser software regularly to ensure that you have the latest security settings.[2]

(c) **Install anti-virus programmes** — Ensure that your firm has a good anti-virus programme installed in computers to prevent the use of malware and spyware.

(d) **Change your password** — Modify your password regularly for greater security. When choosing a password, it is best to use a mix of alphabetical and numeric characters, as well as symbols, for added security. Avoid using the same password for different accounts.

Members of the Bar are reminded to be vigilant and to report suspected or confirmed scams to Bar Council by sending an email to the Professional Indemnity Insurance and Risk Management ("PII") Department at pirm@malaysianbar.org.my.

Should you have any enquiries, please contact the officers of the PII Department by telephone at 03-2032 4511 or by email at pirm@malaysianbar.org.my.

Thank you.

Ragunath Kesavan
Chairperson
Professional Indemnity Insurance Committee

[1] Adapted from Tony Bradley, "Top Secret! Keep Your E-Mail Private and Secure" (*PC World,* 30 November 2010), accessed on 30 June 2014.

[2] Adapted from "Keep Security Software Up To Date" (*Stay Smart Online)*, accessed on 30 June 2014.

2016 Risk Management Highlights

The risk management initiatives for the year 2016 include website update, events organisation, publications and a new initiative where firms are visited by the Officers of PII and Risk Management Department.

RISK AWARE!

A REVIEW OF YOUR FIRM

Risk Aware! is an initiative where a firm's practices and procedures are reviewed by Officers from PII and Risk Management Department. The objective is to evaluate and provide suggestions for improvements to the firm to reduce exposure to malpractice suits.

Approximately 12 randomly selected firms from Melaka, Terengganu, Perak and Pahang have participated in the review.

PRAKTIS
MALAYSIAN BAR PROFESSIONAL INDEMNITY INSURANCE SCHEME PORTAL
www.PRAKTIS.com.my

Praktis website stores information on PII, articles on risk management, case studies, checklists, circulars etc. The website is easily navigated, and search function allows visitors to search for their selected area or topic.

Events

Two risk management workshops were conducted at Bar Council.

(a) Billing & Collections in Kuala Lumpur (25 Aug 2016)

Billing & Collections

The half-day workshop is suitable for practitioners of all background. Topics covered are billing "how to's", fee agreements, managing cash flows, tracking and systems, and managing client expectations.

(b) *Getting Started!* in Kuala Lumpur (13 Oct 2016)

Getting Started!

This Workshop is ideal for Members who intend to set-up a new firm, recently set-up a new firm or joining a partnership. It is also suitable for lawyers who have just started practice, and is useful as a refresher course for senior lawyers.

The full-day workshop features broad and comprehensive aspects on practice and matter management, accounting and taxation, litigation and conveyancing.

Jurisk!

Jurisk!, a bi-annual risk management newsletter focuses on different practice related issues in each publication. The newsletter features case studies of actual claims from the PII Scheme, practice tips and a variety of ideas to improve a firm's practice management.

Forging Partnerships

Building Firm Foundations

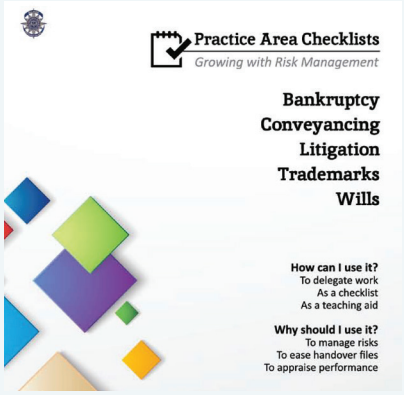
A Tribute To One Of Our Own

Start Kit

Bar Council Malaysia launched 'START', the first-ever legal starter kit of its kind in February 2011. An initiative by the Bar Council's Professional Indemnity Insurance ("PII") Committee, the START Kit forms part of Bar Council's risk management programme and strategy to enhance the quality and standards of new lawyers in the country.

Since its introduction in 2011, START Kit has been aggressively distributed to new firms upon obtaining their "no objection" letter from Bar Council and pupils attending Ethics Course. The kit consists of Best Practice Guides (Setting Up Practice, Accounting for Lawyers, Time Management for Lawyers and Law Practice Management), Practice Area Checklist CD-ROM, Office Management DVD-ROM and the Start File (consisting of 4 booklets).

The kit was updated in 2016 to reflect current information. In particular, the Practice Area Checklist CD-ROM content has been updated and new checklists (bankruptcy, wills) were added.



Others

A briefing on PII and risk management is delivered at every Ethics Course in Kuala Lumpur to explain its relevance and importance. Pupils are taken through the PII Scheme, type of cover and how to avoid malpractice suits. An explanation of the PII Scheme is also provided at selected CPD events as and when required. Participants have the opportunity to understand the Scheme better and seek clarification on PII coverage.

PI INSURANCE & RISK MANAGEMENT DEPARTMENT
Bar Council Malaysia
Suite 4.03A, 4th Floor, Wisma Maran
28 Medan Pasar, 50050 Kuala Lumpur, Malaysia

Tel: **03-2032 4511** Fax: **03-2031 6124**
Email: **pirm@malaysianbar.org.my**

BAR COUNCIL MALAYSIA
No 15, Leboh Pasar Besar
50050 Kuala Lumpur, Malaysia
Tel: 03-2050 2050
Fax: 03-2034 2825 / 2026 1313 / 2072 5818
Email: council@malaysianbar.org.my

Mysahra Shawkat Executive Officer
✉ mysahra@malaysianbar.org.my

Azwa Zulsamli Officer
✉ azwa@malaysianbar.org.my

Have you been hacked?

Clicked on a suspicious link?

Emails intercepted?

Is your email account compromised?

Are you a victim of cyber crime?

If in doubt or you need assistance, contact PII and Risk Management Department at 03-2032 4511.