Risk Management Newsletter

JURISK!

Volume 14
Issue 2
July 2019

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

CHAIRPERSON'S MESSAGE

Dear Members of the Bar,

One of the biggest threats today, is attacks on cyber security. With our increased dependence on technology, the scale of cyber attacks is growing considerably.

Any organisations that are networked and electronically connected are vulnerable to cyber security threats. Legal firms are no exception to this.

The day to day transactions of legal firms involve the use of sensitive data; be it personal or commercial. These data, if lost or breached, can come back to haunt in the form of legal suits.

This *Jurisk!* issue gives an insight to Members on the importance of cyber security in legal firms. The notion that cyber security is reserved for big firms is misconstrued. This is evident from the increasing number of cyber security related notifications received by the PII Scheme's Brokers. Case studies on such cyber security related notifications have been included in this issue. These would help Members comprehend the damage that security breaches can cause legal firms.

Members are advised to assess the status and strength of their cyber security measures by using the many cyber risk assessment tools available or by acquiring the services of a cyber security consultant, and to constantly update their cyber security measures.

The next step Members should take in order to ensure effective cyber security is to create and build a data secure culture in legal firms. This can be done by educating lawyers and staff members to be cyber vigilant. Policies and procedures must be developed and implemented in legal firms to this effect. This will prove useful for lawyers and staff in legal firms should they come across anything suspicious.

Members should also be aware that the PII Scheme Insurer does provide a separate Cyber Insurance Policy which Members can opt to take. Details on this is available in the article entitled "Malaysian Bar Mandatory PII Scheme, PII Did you Know – Does it Cover Cyber Incidents" in this issue.

It is hoped that from reading this *Jurisk!* issue, Members' attitude towards cyber security and data protection will change for the better.

Kuthubul Zaman Bukhari
Chairperson
PII Committee 2019/2020
Bar Council Malaysia

Contents

Dear Members,

In this issue...we present to you:

Cybersecurity
Keep abreast of cybersecurity threats that affect legal firms today. We have included case studies on cybersecurity-related notifications received by the Professional Indemnity Insurance ("PII") Scheme Insurer, as well as tips on how to best improve and boost the cybersecurity of legal firms.

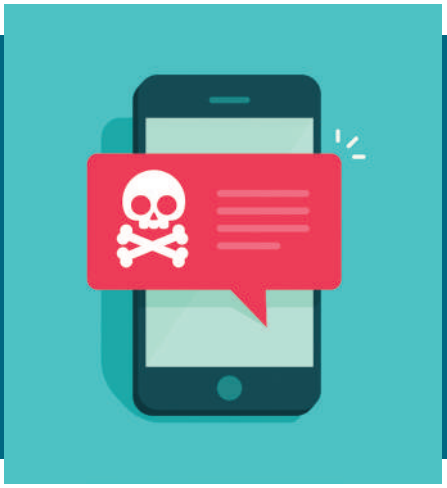
Cyber Insurance Policy
Understand the extent to which the Mandatory PII Policy provides cover for cyber incidents, and take note of the separate Cyber Insurance Policy that the Mandatory PII Scheme Insurer has to offer. Check out the comparison checklist to compare the extent of cover provided by these two policies in the "Malaysian Bar Mandatory PII Scheme – DID YOU KNOW?" section.

Practice Management
Read about the art of effective delegation to achieve a better work-life balance. Learn how effective delegation can increase productivity and allow you more control of your time.

Health
There is also a health write-up that shares ideas on how Members can deal with the burnout syndrome that is prevalent in the profession. We hope that with such information, Members will take initiatives to take a step back from work, to prioritise their mental and physical wellbeing.

Feedback or Queries
If you have any feedback or queries, please reach out to the PII and Risk Management Department officers directly by telephone at 03-2032 4511 or by email at pirm@malaysianbar.org.my.

Happy Reading!
Jurisk! team



LAW FIRMS ARE PRIME TARGETS OF CYBER ATTACKS

by Dennis Goh, Legal Risk Junior Manager,
Jardine Lloyd Thompson Sdn Bhd

LAW firms are increasingly being targeted by cyber criminals because they hold a vast amount of:

- **client funds;**
- **sensitive personal information;**
- **intellectual property rights;**
- **litigation strategies;**
- **merger and acquisition documents; and**
- **materials with the potential to cause damage to someone's reputation.**

Many firms do not even realise they have been compromised when a cyber-attack takes place. By the time the incident is discovered, significant damage may already have been perpetrated.

Recent Cyber Incidents Involving Law Firms

The Panama Papers leak in 2016 is a good example of cyber incidents perpetrated on law firms. Hackers were able to procure access into a Panamanian law firm's computer system which was using an outdated version of a web-server. The hackers procured and leaked over 11 million documents from the firm's database. These leaked documents exposed offshore dealings of several world leaders, politicians and public officials.

A more recent breach is that involving an American law firm, DLA Piper which had previously touted its expertise on cybersecurity and data protection. In 2017, DLA Piper's internal office network was infected by the NotPetya malware which caused a system breach. As a result, the phone system, email server and firm's web portal were shut down. The malware restricted the firm employees' access to communications and soft copy documents. Approximately 3,600 lawyers and support staff across 40 countries were on digital lockdown. The firm had to engage the services of 15,000 IT experts to salvage the firm's digital equipment but to no avail.

Although the examples above show cyber criminals are targeting firms with high-profile clients and offshore services, do not assume that smaller firms are not on their radar. Hackers look for the most vulnerable system and strike at any available opportunity.

Why Are Law Firms Vulnerable?

Law firms become vulnerable if cyber security do not form part of their overall risk evaluation. Despite adequate IT security software in place, the human element is often the weakest link in a law firm's defence against cyber-attacks. Most

cyber security breaches occur not due to hacking but through social engineering - when a careless or unsuspecting staff in your firm clicks on a link from a fake email, which in turn allows a hacker to gain access into your internal office network.

The cyber threat is real. Most firms and their lawyers do not realise this. Your firm would be at risk if:

- **every employee has a computer connected to the firm's internal network and the Internet;**
- **every employee has unimpeded access to client data, regardless of sensitivity;**
- **every employee is given great latitude to access the Internet and personal email through the firm's computers;**
- **a large number of non-encrypted portable devices belonging to members of the firm are used in less secure environments (eg public WiFi);**
- **the firm's computer software is not updated regularly;**
- **there is no policy in place for cyber or internet usage; and**
- **there is insufficient cyber security awareness.**

These factors make firms vulnerable and likely targets. Further, hackers no longer merely grab the goods and run. The malware employed enable them to stay hidden within a network for months, while collecting more and more sensitive data on employees, clients and other private information.

Act Now Before It's Too Late

As a lawyer, recognise that you are a fiduciary to your client. You are under a duty to protect your clients data and information - for its loss may cripple your clients and your firm. This issue of *Jurisk!* contains articles that provide information and tips on how you can protect yourself, your firm and your clients from cyber attack. Implement these steps but do not stop there. Even with the best protection in place, cyber breaches can still occur. Cyber criminals are constantly innovating new ways to infiltrate a system. It is most recommended and worthwhile to invest in a cyber insurance coverage as a safety net in the event a cyber risk materialises.

Remember, your law firm's value is in the information it holds - it is incumbent on you to protect your client's data and information against cyber risks.

CASE STUDY

CYBER NOTIFICATIONS RECEIVED BY THE PII SCHEME (2010-2017)

IDENTIFICATION THEFT

In one notification, an Insured Practice ("IP") was alerted by an individual from Korea of the theft of IP's identity. This Korean individual informed IP that he had recently been communicating with someone posing as a lawyer and identifying themselves as IP. The imposter had in place an elaborate scam to which the Korean individual almost fell victim. The scam was in respect of the setting up of Korean charitable foundation in the Korean individual's favour which purportedly involved IP as the legal advisors. The imposter had demanded the Korean individual to pay a sum of US$20,000 for legal fees, which apparently could not be deducted from the trust funds and had to be advanced by the Korean individual to enable the transaction to proceed. The scam was an intricate one; the imposter had even provided a sham agreement together with a certificate purportedly issued by the High Court of Malaya in support of the scam. Fortunately, the Korean individual thought to conduct an online search, which led him to discover that the purported email of the imposter differed with that of IP's firm email. This led to his email enquiry to IP. IP had then notified the Insurer and lodged a police report.

In another notification, an IP notified the Insurer of an email received by them. The aforementioned email had been received by IP from an unknown source enquiring as to the authenticity of an email purportedly authored by IP. Essentially, the email was a phishing scam, in which IP's identity had been stolen and made use of by hackers. IP proceeded to notify its lawyers and staff of

the existence of the scam, after which it was discovered that another lawyer in the firm had received a similar email in the past. However, that lawyer had taken no action; only dismissing the same as spam. Deciding to be cautious, IP then notified the Insurer of the scam.

Lesson:
Despite the fact that these fraudulent emails had caused neither loss nor damage in this case, it is imprudent to merely ignore or treat them as spam. You may never know who may fall victim as a result of your inaction. Protect your practice by notifying the Insurer, and reporting the incident to the police and your email service provider.

IDENTIFICATION FRAUD

In a notification received in 2014, the IP was notified by an instance of a hacker intercepting IP's emails. Having hacked into the IP's and client's email accounts, the hacker then posed as IP's client, providing instructions for the proceeds of a sale and purchase transaction of a property to be transferred to a local bank account. The hacker also provided information believed to have been extracted from previous email correspondences between IP and the client, to bolster the hacker's credibility as the purported client. This convinced IP to believe that it was dealing with its actual client. The actual client later called IP to enquire about the proceeds. Upon being told of the payment that IP had made, the client asserted that no instructions had been given to transfer money and the client had not received any money.

The Insurer was notified and a police report was lodged. The police was able to successfully apprehend the hacker and recover a substantial amount of the stolen funds. The IP chose to make good to its client the small portion of funds lost, which was lower than IP's base excess, and withdraw its notification to the Insurer.

In another notification, an IP had acted for a vendor in a sale and purchase transaction of a property. They agreed for communications to be made mainly through email. Upon the sale of the property, the proceeds amounting to approximately RM200,000 was paid to IP to be held as stakeholder. The vendor then instructed IP to deposit the said proceeds into the vendor's account held in Bank A. Instructions were given by email, as agreed.

Not long after, IP received a second email purportedly from the vendor. The second email was a hoax – created by hackers who had breached IP's computer system and remained undetected. There were minute differences between the vendor's real email address and that of the hoax – which was difficult to spot at a glance. This difference was not picked up by IP.

The hoax email instructed IP to pay the proceeds to a different account which belonged to an entity unrelated to the transaction. Unsuspecting that there is anything amiss, IP duly complied.

The following day, the owner of the entity who received IP's payment contacted IP. He informs IP that there must have been a mistake in the payment and refunded the full sum to IP. This incident should have set alarm bells ringing, however, it apparently made no difference in the halls of IP.

Still unsuspecting of anything amiss, IP informed the "client"/hackers of the mistake. This was also


SOFTWARE UPDATES
OFTEN FIX SECURITY
PROBLEMS
DOWNLOAD UPDATES AS SOON
AS THEY BECOME AVAILABLE.

done through email, which IP sent to the hoax email address. The hackers then instructed IP to deposit the monies into another account. Unlike IP, the hacker ensured that they made no mistake the second time around. IP complied with the instruction.

Several days later, the vendor queried IP as to why the proceeds had yet to be deposited into their account in Bank A. It was only then IP realised that he had fallen victim to cyber criminals. It was all too late. IP then notified the Insurer and lodged a police report.

Lesson:
Email has become the preferred communication method between lawyer-client because it is an easy, fast and convenient method. However, this does not excuse a lawyer from undertaking their work with care and thorough vigilance. When receiving instructions from clients via email, especially those purporting to be "urgent" or in respect of the transfer or release of monies or documents, always verify those instructions directly with the client by telephone. Do so even when you're convinced of the genuineness of the email instructions and follow up with a letter or email confirming it.

Look for small clues in the email to determine whether it is fraudulent. Check if the email address matches that of your client. Strange phrases, spelling or grammar errors and punctuation are red flags. A claim that the matter is urgent or that the client is uncontactable through telephone is often an indicator of possible fraud.

UNWITTING ACCOMPLICE

In 2017, an IP notified the Insurer of a claim in which IP was made a defendant. In this case, IP was approached by fraudsters who wanted the services of IP to receive foreign funds into IP's client account. The fraudsters posed as representatives from an esteemed Malaysian company. Despite failing to carry out any proper client due diligence procedure, IP was convinced of the legitimacy of the work instructed. The foreign funds (which were later discovered to be the proceeds of a successful phishing and identity scam perpetrated by the fraudsters against a foreign company) was duly paid into IP's client account. On the very same day upon receiving these funds, IP issued a cash cheque to the fraudster client who vanished thereafter. It was only upon being served with a Writ & Statement of Claim that IP had realised he had become a victim of fraud.

Upon being notified, the Insurer had rejected coverage. This was because the transaction carried out by IP, ie the use of IP's client account solely for the purposes of receiving funds, is not a service that an advocate and solicitor would ordinarily provide in the normal course of carrying on the profession in accordance to the Legal Profession Act 1976. To make things worse, IP had not retained any documents from the said transaction. The Insurer had to reject IP's argument that IP was a stakeholder to the funds

as there was no evidence of any agreement to show that parties had in fact appointed IP as stakeholder.

In hindsight, what would you have done if you were in IP's position?

Lesson:
Avoid being abused and tricked by fraudsters and money launderers by conducting due diligence on prospective clients. Verify identities and background especially where they purport to represent another person or entity. When there is anything amiss about their identity or the transaction itself, proceed with caution or consider declining the brief. Submit a Suspicious Transaction Report to the authorities. This is to safeguard your practice from becoming a victim of fraud and avoid non-compliance sanctions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

PHISHING SCAMS

In a 2016 claim notification, an IP received an email purportedly from his client. The email provided IP with a link to retrieve certain documents of which IP had earlier requested from the client. After clicking the link, IP was then directed to IP's email login page which prompted IP to re-enter the user name and password for the account. However, once the user name and password were entered, the email account was locked and IP could no longer access IP's email account. Only then IP came to know that his client's email was hacked, and subsequently used to phish for IP's information. The next day, IP was then informed by their clients and colleagues regarding an email purportedly received by them from IP's email account requesting for friendly loans and payments for legal fees to be transferred to a local bank account which did not belong to IP. Some of IP's clients had fallen victim upon paying monies to the hacker.

Lesson:
Be sceptical of emails requesting for personal or client information. Always verify email addresses to ensure that there are no discrepancies. Don't click on unknown links. Instead, type the address in full yourself. When in doubt, speak personally to the person requesting the said information. Ensure that your firm's computer system is protected with updated security tools and software.


RECEIVED AN EMAIL FROM AN UNKNOWN SENDER?
IF YOU DON'T KNOW WHO SENT IT,
SIMPLY DELETE IT!
CLICKING ON IT MAY LEAD TO SITES THAT CAN INFECT YOUR COMPUTER.

CYBER SECURITY & DATA PROTECTION

by Dennis Goh, Legal Risk Junior Manager,
Jardine Lloyd Thompson Sdn Bhd

CYBER security is an emerging risk that law firms must nowadays face. This is because lawyers are expected to use technology to remain competent and effective in the delivery of services to their clients. Despite the risks, law firms, especially small practices, lag in preparing for cyber-attacks due the perceived high costs involved. To have an effective cyber security program requires, at a minimum, up-to-date software which can be very expensive regardless of the size of the firm.

However, it would be foolish to assume that just because you're running a small practice you are less of a target. Every law firm has information valuable in the criminal economy. What more when you consider that a majority of cyber-crimes are crimes of opportunity. Hackers look for the most vulnerable systems and strike those first!

Cyber-attacks can cause bad outcomes to firms and their clients. These may range from general breaches of confidential information, theft of client funds or even the inability to access the firm's own IT system. All of these scenarios can ultimately lead to PII claims against firms.

WHAT CAN LAW FIRMS DO?

It is important to understand that while there are software and tools to address cyber threats, the ultimate key to cyber security is human behaviour.

UNDERSTAND THE RISKS: Constantly review the firm's cyber security system and procedures to ensure that the firm has the best protection. Ideally, invest in security software, up to date hardware and staff training toward the firm against cyber threats. The possible financial damage caused by a cyber-attack to your law firm may very well outweigh any investment costs of an adequate cyber security.

BE INFORMED: Stay current on technology, cyber security issues and threats. Subsequently, take steps to prevent or minimize them.

HINT: Subscribe to tech websites and blogs for weekly or monthly updates for FREE.

ENCRYPT AND PROTECT YOUR DATA: Encryption is the conversion of data into a secret code. Only someone holding a further secret password or conversion cipher will be able to read or have access to such encrypted file, so this is an effective way to ensure only those you authorise (and provide the code, password or cipher to) have access to specific data. Thus, the technique of encrypting of documents is a highly effective security measure when transmitting confidential documents through email.

PASSWORDS: Ensure all digital devices are password protected. Ensure that your lawyers and staff never leave computers or laptops unattended anywhere without employing locking devices. Create stronger passwords ie those that include a mix of fonts, cases, numbers and symbols. Do not use birth dates of you or your loved ones or names of your favourite people.

HINT: Trouble remembering passwords? Use a password keeper software program or app. Better yet, write them down on a piece of paper or note book and keep these physically locked away in safe storage, separate from where you keep your computer. Hackers can't hack into physical notebooks stored in a locked drawer.

AWARENESS: Arrange training for everyone in the office to raise awareness about cyber security, threats and preventive measures they need to undertake. Instil the need for everyone to be mindful and vigilant.

COMPLIANCE: Know and understand the provisions within the Personal Data Protection Act 2010 ("PDPA") and the issues surrounding client personal data. Compliance to the PDPA is a critical part of cyber security strategy.

NO PLAN IS PERFECT

It is also important to plan for the worst. No matter how sophisticated the computer system or how high your cyber-security budget, no establishment is impervious to the financial and reputational fall-out of a cyber incident. To that end, you should consider purchasing a Cyber Insurance Policy which provides coverage against potential losses arising from cybercrimes and other computer system failures.

If you would like to know more about the benefits of a Cyber Insurance Policy, please contact Jardine Lloyd Thompson Sdn Bhd at 03-2723 3241 or by email at mbar@jltasia.com.

MALAYSIAN BAR
Mandatory PII SCHEME
DID YOU KNOW?

PII: DOES IT COVER CYBER INCIDENTS?

In general, the Mandatory PII Policy provides indemnity against civil liability claims, defence costs and mitigation costs. Therefore, indemnity is provided if you are sued by your client for failing to protect the client's confidential data.

What is not covered when a cyber breach occurs is your firm's own costs and liabilities, ie, loss of income resulting from threats, damage or loss of information arising from use of your firm's computer systems and networks.

How can firms manage the cost of cyber-attacks?

Whilst firms can adopt steps to prevent and minimize the risks of cyber-attacks, firms must also be prepared to manage the costs resulting from such risks. To manage and recover from these losses, it is crucial to have a separate Cyber Insurance Policy.

The broker of the Mandatory PII Scheme for the Malaysian Bar has specifically designed a Cyber Insurance Policy to complement the cover afforded under the Mandatory PII Policy. This Cyber Insurance Policy protects your firm from many of the first and third party costs and expenses that may result from a cyber-attack, a breach in network security system or a cyber-incident affecting a third party service provider.

If you would like to know more about the benefits of a Cyber Insurance Policy, please contact Jardine Lloyd Thompson Sdn Bhd at 03-2723 3241 or by email at mbar@jltasia.com.

Note: Under the Mandatory PII Scheme, cover is always subject to terms, exclusions, limitations and conditions of the relevant Certificate of Insurance.

The Bahasa Malaysia translation on page 33 relating to the Master Policy, Certificate of Insurance and illustrative examples are for guidance only. In the event of inconsistency between the English version and the Bahasa Malaysia version, the English version will prevail.

COVERAGE UNDER THE MANDATORY PII POLICY AND CYBER INSURANCE POLICY

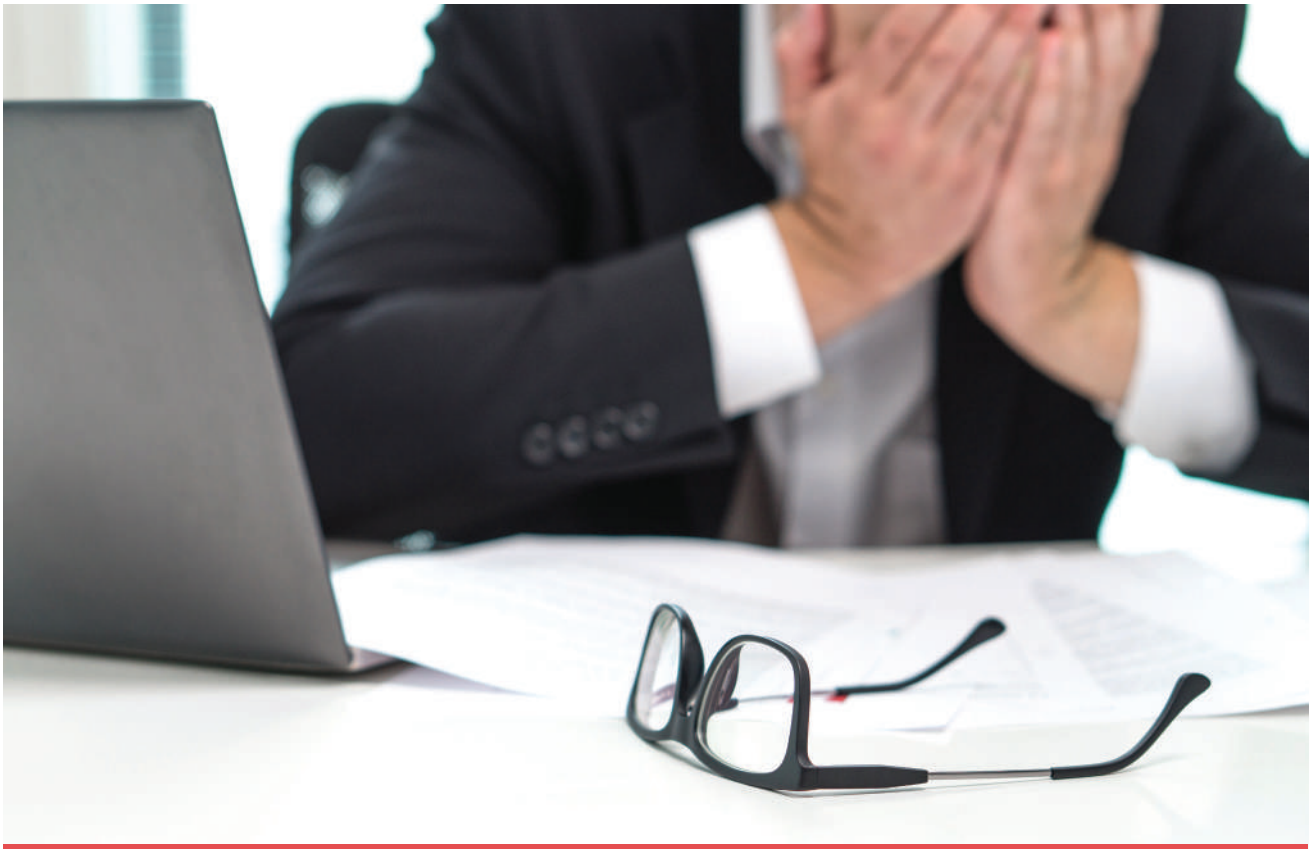
Legal Liability / Third Party Coverage	Mandatory PII Policy	Cyber Insurance
For failure to protect confidential data from threats or inadvertent release	√	*√
For failure or violation of the security of a computer system	√	*√
For a data breach claim that may not involve a client nor be associated with the provision of professional services (excluding claims by employees or third-party vendors)		√
Media liability claims (eg infringement of copyright/ trademark, defamation, plagiarism etc)	√	*√
Legal costs and expenses incurred to defend a regulatory claim by authorities or alike		√
Data administrative fines and penalties (where insurable by law)		√

**where PII coverage overlaps, the Cyber Insurance provides "top-up" over the mandatory PII*

Own Costs / First Party Coverage	Mandatory PII Policy	Cyber Insurance
Breach response costs including costs of specialist legal advice, forensic IT expenses and notification costs		√
Public relations and crisis management expenses		√
Data restoration costs (costs to restore electronic data, software and programs)		√
Loss of income and extra expenses incurred as a result of a security breach and technology failure of your computer systems		√
Cyber extortion		√
Fines, assessment costs and claim expenses incurred to defend a Payment Card Industry Claim		√

THE BURNOUT LAWYER

by Mohan Sankaran, Legal Risk Counsel, Jardine Lloyd Thompson Sdn Bhd



BURNOUT seems to be a pandemic in the legal fraternity. Burnout is defined as physical or mental collapse caused by overwork or stress. Recently, the chairman of the global legal giant Baker McKenzie made a decision to temporarily step down, citing exhaustion as his main reason. Sadly, six months after announcement of his decision, he passed away. The work culture of most legal firms – long hours, large workloads and demanding clients – seems to be the factors for lawyers experiencing burnout.

ACCORDING to the American Bar Association, burnout is a health hazard affecting lawyers globally. It is because of the perceived disparity between the demands of the job and the resources (both material and emotional) that an employee has available to him or her[1]. In Malaysia, given that almost 90% of our law firms comprise small firms[2], it is not surprising that lawyers here experience the same symptoms but their experiences have gone unreported. Lawyers in this category spend the vast majority of their time in the office trying to cope with the high demands of the job and making ends meet.

1. https://www.americanbar.org/publications/law_practice_magazine/2012/may_june/burnout-avoidable-not-inevitable/

2. Professional Demographics Statistic as at 02.05.2018 by JLT

They hardly have any time for themselves let alone their families. Over time, this leads to burn out because of the prolonged physical or emotional stress.

The situation is the same for partners in larger firms. Their work is demanding; high expectations to meet targeted revenue and work performance. With the firm's expectation escalating each year, it adds to the pressure to deliver.

Symptoms of a Burnout Lawyer

Common symptoms of a burnout lawyer:

- Become more irritable or impatient;
- Loss of appetite;
- The feeling of having to drag yourself to work every day;
- Constantly feeling lethargic;
- Unable to concentrate; and
- Trouble sleeping or often experiencing headaches.

All these will have a profound effect on your personal and professional relationships. If you experience any of these symptoms, tackle them early on before it affects your relationship, causes health breakdown or could even costs lives.

1. Take a step back and take stock of your current situation.
2. Make an honest assessment of your job load and responsibilities.
3. Identify the root causes of your stress which make you feel burnout.
4. Consider not taking on any new files whilst you try to resolve your backlogs.
5. Seek support from your peers.
6. Monitor your work routine and make improvements.
7. Invest in case and office management software.
8. Adopt a healthy lifestyle - regularly exercising, practice healthy eating, take up yoga or meditation.
9. Ensure you have enough rest and sleep.
10. Maintain a good social support system; value the time with friends and family.

In the event you find none of the above methods work and you are still excessively stressed, then it is time to seek professional help.

Learn to DELEGATE

by Mohan Sankaran, Legal Risk Counsel,
Jardine Lloyd Thompson Sdn Bhd

TODAY, clients are more demanding. So are your professional obligations. The to-do list gets longer by the day when court dates and meetings fill up your calendar. It forces you to spend more time to attend to these matters a common adage: too many things to do and too little time. For an owner of a small firm, the feeling of being stressed out and overwhelmed shackles you.

Your inability to delegate might result in you unable to achieve a work-life balance. This is because your mind will constantly be thinking of work even after you have left the office, ie meeting deadlines, chasing your overdue fees, getting new files and the list goes on. Hence, in the long run, having an assistant can help to alleviate this stress. However, for smaller firms where keeping their overheads low is of the utmost importance, the worry is that hiring an assistant involves additional cost! Therefore, you need to decide whether to maximise your revenue or having an assistant can help you achieve that healthy work-life balance.

Excuses! Excuses! Excuses!

As the old saying goes, ***"If it is important to you, you will find a way. If not, you will find an excuse."***

One of the common excuses for not hiring or delegating is that you are too busy and don't have the time or the patience to train someone. In addition, for smaller firms the extra cost can seem insurmountable. Some senior lawyers would prefer to draft every small thing themselves rather than to delegate it to their juniors, on the premise that having to redraft the junior's work is even more time-consuming. There may also be issues of insecurity and the fear of losing control.

Notwithstanding, we need to also be mindful that delegating work does not mean abandoning responsibility but spreading it so one individual do not become overwhelmed with so many duties.

How to Delegate

The art of effective delegation is simple.

1. Learn to Trust

Build your confidence by trusting others with responsibilities. Remember how your master trusted you in your early years of practice? You need to do the same. Don't get bogged down with routine work; delegate these tasks. It will ease your burden and free up your time. The protégé or receiver will learn the tasks and eventually become good at it. It empowers and develops them to take responsibility for the work they do and take on more complicated tasks in the future.

Suggestion: With all that free time, you can now expand the firm's clientele or go for the long overdue holiday, which, in the long run is essential for you mental and physical health.

2. Give Clear Instructions

When delegating, explain in simple language and clear steps. Ensure that those you delegate understand both the task given and the expected outcome. Do not assume that they automatically understand you. By doing this you can gauge their capability and can delegate based on their individual competencies. As a result, you get quality with minimal need for correction.

Suggestion: Gauge the receiver's depth and level of understanding by asking the receiver to repeat his understanding of your instruction. Take corrective measures in the event the receiver did not understand your instruction, which may include talking slowly, breaking down the steps required into smaller manageable steps (something you have come to take for granted in your years of experience), or using simple words. Once the task is completed, compare it with the instructions you provided. Repeat until the work is completed and completely satisfactory.

3. Give the necessary authority

Do not micromanage the task after delegating it. Give your staff the authority to execute the job. Be a mentor, not a dictator! Let them come up with ideas and suggestions on how to best deal with the tasks. This encourages creativity and confidence. Withholding authority will only make the task more difficult to carry out. If this continues, they will become frustrated and resentful, which is bad for the organisation in the long run.

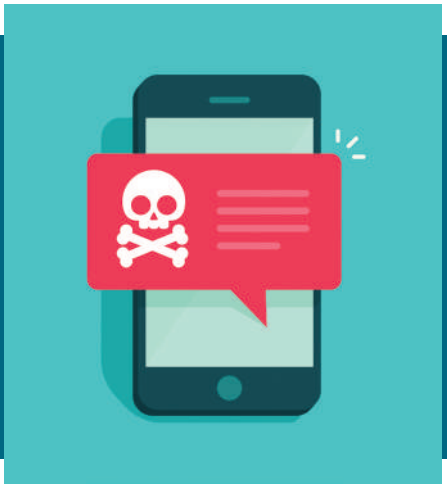
Suggestion: Allowing your staff to manage simple files with minimum supervision allows growth of your organisation. Your junior lawyers and staff will develop their own set of skills, knowledge and abilities; making them more confident and better at their work.

4. Monitor Progress

If you are worried about losing control, monitor the progress of the assigned task to alleviate your fears. Monitor by having periodical updates and meetings to keep abreast of developments. Periodical monitoring is necessary not only as a risk management measure, but to ensure your juniors and staff completes the assigned task on time. Similarly, it also enables you to spot mistakes and correct errors as the task progresses.

Suggestion: Schedule and make time to have a meeting with your team at least once a week or every fortnightly. Take down minutes so you have a record of it which can easily be follow up upon, monitor assigned tasks and plan for future action in time for the next meeting. It also helps you to keep track of the office workload.

It is natural to feel agitated when you first try to delegate. However, "practice makes perfect". Delegating will eventually become easier. When that happens, it will ease up your time and help you focus on other tasks or take on new briefs. Remember, your job is now to trust, supervise and monitor.



FIRMA GUAMAN MERUPAKAN SASARAN UTAMA SERANGAN SIBER

oleh Dennis Goh, Pengurus Penasihat Undang-undang, Jardine Lloyd Thompson Sdn Bhd

FIRMA guaman kini semakin menjadi sasaran penjenayah siber kerana ia mempunyai rekod simpanan yang luas berkenaan:

- **dana klien;**
- **maklumat peribadi yang sensitif;**
- **hak-hak harta intelek;**
- **strategi litigasi;**
- **dokumen-dokumen dari penggabungan dan pengambilalihan; dan**
- **bahan-bahan yang berpotensi merosakkan reputasi dan nama baik seseorang.**

Kebanyakan firma tidakpun menyedari mereka telah dikompromi apabila suatu serangan siber berlaku. Apabila insiden tersebut disedari, kerosakan yang amat mendalam telahpun dialami.

Insiden Siber Melibatkan Firma Guaman Sejak Baru-Baru Ini

Pendedahan "Panama Papers" pada tahun 2016 merupakan contoh terbaik insiden siber yang berlaku ke atas sebuah firma guaman. Penggodam telah memperolehi akses ke dalam sistem komputer sebuah firma guaman Panama yang menggunakan perkhidmatan rangkaian sesawang yang telah ketinggalan zaman. Penggodam itu telah memasuki dan membocorkan lebih daripada 11 juta fail dari pengkalan data firma tersebut. Dokumen-dokumen yang dibocorkan mendedahkan urusan luar pesisir *(offshore)* oleh beberapa ketua negara, ahli politik dan pemegang jawatan awam.

Satu perlanggaran yang lebih baru melibatkan sebuah firma guaman Amerika, DLA Piper, yang sebelum ini mewarwarkan kebijaksanaannya dalam bidang sekuriti siber. Pada tahun 2017, rangkaian dalaman pejabat DLA Piper telah dijangkiti perisian hasad atau kod merbahaya *(malware)* Petya yang menyebabkan kerosakan sistemnya. Oleh yang demikian, penggunaan sistem telefon, emel dan laman sesawang firma tersebut telah ditutup. Perisian hasad tersebut telah menyekat akses kakitangan firma tersebut kepada komunikasi dan salinan lembut dokumen-dokumen mereka. Dianggarkan 3,600 peguam dan kakitangan am merangkumi 40 negara mengalami sekatan digital. Firma tersebut terpaksa menggajikan 15,000 pakar IT dalam usaha menyelamatkan peralatan digital firma tersebut namun tidak berjaya.

Contoh di atas menunjukkan penggodam mensasarkan firma guaman yang mempunyai klien berprofil tinggi dan yang menawarkan


KEEP YOUR DATA SAFE
PROTECT YOUR DATA WITH ENCRYPTION

perkhidmatan luar pesisir, jangan sekali-kali terfikir bahawa firma-firma kecil tidak menjadi sasaran mereka. Penggodam senantiasa mencari sistem yang terdedah dan mudah diserang, dan akan menyambar sebaik sahaja menemui peluang yang terbuka.

Apa Sebab Firma Guaman Terdedah?

Firma guaman terdedah dan mudah diserang sekiranya sekuriti siber tidak dititikberatkan dalam penilaian risiko keseluruhan mereka. Walaupun perisian keselamatan IT yang mencukupi digunakan, elemen kemanusiaan sering menjadi tompok kelemahan dalam pertahanan sesebuah firma guaman terhadap serangan siber. Kebanyakkan perlanggaran siber tidak berlaku disebabkan penggodaman tetapi disebabkan pengaturan sosial – apabila seorang kakitangan firma anda yang cuai atau tidak peka menekan pautan dari sebuah emel palsu, yang kemudiannya membolehkan seorang penggodam mendapat akses ke dalam rangkaian dalaman pejabat anda.

Ancaman siber ini serius akibatnya. Kebanyakkan firma dan peguam mereka tidak menyedari perkara ini. Firma anda terancam sekiranya:

- **setiap kakitangan mempunyai komputer yang bersambung dengan rangkaian dalaman pejabat serta ke Internet.**
- **setiap kakitangan mempunyai akses tidak terhad ke atas data klien, tanpa mengira tahap sentivitinya;**
- **setiap kakitangan diberi kebebasan meluas untuk bersambung dengan internet dan emel peribadi menggunakan komputer-komputer milik firma tersebut;**
- **terdapat banyak peralatan mudahalih yang belum disulitkan *(non-encrypted)* kepunyaan ahli-ahli firma yang digunakan di tempat yang tidak selamat (contohnya, di kawasan WiFi awam);**
- **perisian komputer firma tidak dikemaskinikan dengan kerap dan tetap;**
- **tiada polisi ditetapkan berhubung penggunaaan siber atau internet; dan**
- **terdapatnya kesedaran sekuriti siber yang amat lemah.**

Faktor-faktor seperti ini menyebabkan sesebuah firma menjadi mudah diserang dan terdedah kepada sasaran. Selanjutnya, pihak penggodam tidak lagi bertindak sekadar ambil dan cabut lari. Perisian hasad yang digunakan membolehkan ia bersembunyi di dalam sesuatu rangkaian untuk tempoh berbulan-bulan lamanya, sambil mengumpulkan pelbagai data sensitif mengenai kakitangan, klien dan maklumat peribadi yang lain.

Bertindak Sekarang Sebelum Terlambat

Selaku seorang peguam, sedarlah bahawa anda merupakan seorang fidusiari terhadap data serta maklumat klien anda. Anda mempunyai tanggungjawab untuk melindungi maklumat tersebut – pendedahan dan kehilangannya boleh menyebabkan kejatuhan klien anda serta firma anda. Isu *Jurisk!* Ini mengandungi pelbagai rencana menunjukkan bagaimana anda boleh melindungi diri sendiri, firma serta klien anda. Laksanakanlah langkah-langkah ini tapi jangan sekadar berhenti di situ. Walaupun perlindungan terbaik diaturkan, perlanggaran siber masih boleh berlaku. Penjenayah siber sentiasa

menginovasi cara-cara baru untuk menyusup masuk sesuatu sistem. Amatlah disyorkan dan berbaloi untuk melabur dalam perlindungan insurans siber sebagai suatu jaring keselamatan sekiranya suatu risiko siber menjadi kenyataan.

Berwaspadalah, nilai firma guaman anda adalah terletak dalam maklumat yang dipegangnya. Tanggungjawab terletak pada bahu anda untuk melindungi klien anda dari risiko siber.

KAJIAN KES

NOTIFIKASI SIBER YANG DITERIMA OLEH SKIM PII (2010-2017)

PENCURIAN IDENTITI

Dalam satu notifikasi, sebuah amalan yang diinsuranskan ("IP") telah dimaklumkan oleh seorang individu dari Korea mengenai pencurian identiti IP. Individu Korea tersebut memaklumkan IP bagaimana beliau telah berkomunikasi dengan seseorang yang berpura-pura menjadi peguam dan memperkenalkan dirinya sebagai IP. Penyamar tersebut telah mereka skim penipuan yang amat terperinci yang hampir menjerat individu Korea tersebut sebagai mangsa. Skim Penipuan tersebut adalah berkenaan penubuhan sebuah yayasan amal di Korea yang memihak individu Korea tersebut, yang kononnya melibatkan IP sebagai penasihat undang-undang. Penyamar tersebut menuntut bayaran fi guaman sejumlah US$20,000, yang kononnya tidak boleh ditolak dari nilai yayasan amal tersebut dan perlu didahului oleh individu Korea tersebut bagi memastikan transaksi tersebut berjalan dengan lancar. Skim Penipuan tersebut amat rumit; penyamar tersebut turut mengemukakan perjanjian palsu beserta sijil yang kononnya dikeluarkan oleh Mahkamah Tinggi Malaya bagi menyokong skim tersebut. Mujur individu Korea tersebut terfikir untuk melakukan carian dalam talian, yang membolehkan dia mengesahkan bahawa alamat emel penyamar tersebut berbeza dari alamat emel firma IP. Lantas, individu Korea tersebut menghubungi IP sendiri. IP pula segera memberi notifikasi kepada Syarikat Insurans dan memfailkan laporan polis.

Dalam suatu notifikasi lain, sebuah IP memberi notifikasi kepada Syarikat Insurans berkenaan suatu emel yang diterimanya dari pihak yang

tidak dikenali dimana melalui emel tersebut pihak tersebut menanyakan kesahihan suatu emel yang kononnya dikarang oleh IP. Pendek kata, emel tersebut merupakan skim penipuan *phishing*, di mana identiti IP telah dicuri dan disalahguna oleh penggodam. IP terus memaklumkan kewujudan percubaan skim penipuan tersebut kepada peguam-peguam dan kakitangannya. Didapati salah seorang peguam IP pernah menerima emel yang serupa sebelum itu. Namun begitu, peguam tersebut tidak mengambil sebarang tindakan; sekadar mengenepikannya sebagai *spam*. IP memutuskan untuk bertindak secara berhati-hati dan telah memberi notifikasi kepada Syarikat Insurans mengenai skim penipuan tersebut.

Pengajaran:
Walaupun emel-emel palsu ini tidak menyebabkan sebarang kehilangan atau kerugian, adalah tidak berhemah untuk sekadar mengabaikannya atau menolaknya sebagai spam. Anda tidak tahu siapa yang boleh menjadi mangsa akibat kegagalan anda untuk tidak bertindak. Lindungilah amalan anda dengan memaklumkan Syarikat Insuran dan melaporkan insiden tersebut kepada pihak polis dan juga penyedia khidmat emel anda.

FROD IDENTITI

Dalam suatu notifikasi yang diterima pada tahun 2014, sebuah IP telah dimaklumkan tentang suatu kejadian di mana penggodam telah memintas akaun-akaun emel IP. Setelah akaun-akaun emel IP dan anakguam IP digodam, penggodam tersebut telah menyamar sebagai anakguam IP dan memberi arahan agar dana daripada suatu transaksi jual beli tanah dipindahkan ke dalam suatu akaun bank tempatan. Penggodam tersebut juga telah menggunakan maklumat yang dipercayai telah diekstrak dari emel-emel antara IP dan anakguam, untuk mengukuhkan kredibilitinya sebagai anakguam. Ini telah menyakinkan IP bahawa ia sedang berurusan dengan anakguam yang sebenar. Namun begitu, IP kemudiannya dihubungi anakguam sebenar, yang bertanyakan tentang dana tersebut. Apabila dimaklumkan tentang pembayaran yang telah dibuat oleh IP, anakguam tersebut telah menegaskan bahawa tiada arahan telah diberikan untuk memindahkan dana tersebut dan anakguam tersebut tidak menerima sebarang dana.

IP telah memberi notifikasi kepada Syarikat Insurans dan suatu laporan polis telah dibuat. Pihak polis telah berjaya untuk menahan penggodam tersebut dan mendapatkan kembali sebahagian besar jumlah dana yang telah dicuri. IP kemudiannya telah memilih untuk menanggung dan membayar balik kepada anakguamnya bahagian dana yang hilang. Oleh kerana jumlah bahagian yang hilang adalah kurang dari *base excess*, IP telah menarik balik notifikasi tersebut.

Dalam suatu notifikasi yang lain, sebuah IP telah bertindak bagi pihak penjual (anakguam) dalam suatu transaksi jual beli tanah. Mereka telah bersetuju untuk berkomunikasi melalui emel. Sebaik sahaja transaksi tersebut telah dilaksanakan, hasil jualan yang berjumlah kira-kira RM200,000 telah dibayar kepada IP untuk dipegang sebagai pemegang amanah. Seterusnya penjual telah mengarahkan IP untuk mendepositkan jumlah tersebut ke dalam akaunnya di Bank A. Arahan tersebut telah diberikan melalui emel, seperti yang telah dipersetujui.

FASTEN YOUR SEAT BELTS

JUST LIKE A SEAT BELT,

CYBER SECURITY CONTROLS

KEEP YOU SAFE.

REDUCE YOUR RISK BY KEEPING THEM IN PLACE.

Tidak lama kemudian, IP telah menerima emel kedua yang kononya daripada penjual. Emel kedua ini sebenarnya palsu – yang telah direka oleh penggodam yang telah menggodam sistem komputer IP dan belum lagi dikesan pada ketika itu. Terdapat beberapa perbezaan yang tidak ketara antara alamat emel penjual dan alamat emel palsu tersebut – di mana perbezaan-perbezaan ini sukar disedari sekilas mata. Perbezaan-perbezaan ini turut tidak ditemui oleh IP.

IP telah diarahkan melalui emel palsu tersebut untuk mendepositkan jumlah tersebut ke dalam suatu akaun yang lain yang dimiliki entiti yang tidak mempunyai apa-apa kaitan dengan tranksaksi tersebut. Tanpa menyedari bahawa terdapatnya sesuatu yang tidak kena, IP telah menurut arahan tersebut.

Pada keesokan harinya, pemilik entiti yang telah menerima bayaran tersebut telah menghubungi IP. Beliau telah memaklumkan IP bahawa terdapatnya kesilapan dalam bayaran jumlah tersebut dan telah memulangkan jumlah tersebut sepenuhnya kepada IP. Insiden ini sepatutnya mencetuskan kesedaran IP tentang penipuan tersebut tetapi disebaliknya, IP langsung tidak perasan.

Sekali lagi, tanpa menyedari terdapatnya suatu yang tidak kena, IP telah memaklumkan "penjual" / penggodam tersebut tentang kesilapan bayaran yang telah berlaku. Makluman ini juga telah disampaikan melalui emel kepada alamat emel yang palsu tersebut. Penggodam tersebut kemudiannya telah mengarahkan IP untuk mendepositkan wang tersebut ke dalam suatu akaun yang lain. Kali ini, penggodam tersebut telah memastikan bahawa mereka tidak membuat sebarang kesilapan kali kedua. IP telah mematuhi arahan yang telah diberikan.

Beberapa hari kemudian, penjual telah menanyakan IP mengapa jumlah tersebut masih belum didepositkan ke dalam akaunnya di Bank A. Pada ketika itulah IP menyedari ia telah menjadi mangsa kepada penjenayah siber. Namun semuanya sudah terlambat. IP kemudiannya telah memberi notifikasi kepada Syarikat Insurans dan membuat laporan polis.

Pengajaran:
Emel telah menjadi kaedah komunikasi terpilih di antara peguam-anakguam kerana ianya mudah, cepat and senang. Walau bagaimanapun, ia bukannya alasan bagi seseorang peguam untuk tidak menjalankan tugasnya dengan berjaga-jaga dan berwaspada. Apabila menerima arahan daripada anakguam melalui emel, terutamanya arahan-arahan yang kononnya "segera" ataupun berhubung pindahan atau perlepasan wang atau dokumen, amatlah penting untuk mengesahkan arahan itu secara terus dengan anakguam melalui telefon. Pengesahan ini perlu dibuat walaupun anda yakin dengan ketulenan arahan dalam emel tersebut. Pengesahan susulan juga perlu dibuat melalui surat atau emel.

Sentiasa peka mencari petunjuk-petunjuk dalam suatu emel bagi menentukan sama ada ia merupakan suatu penipuan atau tidak. Semak sama ada alamat emel itu padan dengan alamat emel anakguam anda. Frasa-frasa yang aneh, kesilapan-kesilapan ejaan tatabahasa dan tanda

baca adalah petanda merah. Suatu arahan untuk melakukan sesuatu perkara secara segera atau anakguam tidak boleh dihubungi melalui telefon kebiasaanya ialah suatu petanda bahawa ianya merupakan suatu penipuan.

PERSUHABATAN TIDAK SENGAJA

Pada tahun 2017, sebuah IP telah memberi notifikasi kepada Syarikat Insurans mengenai suatu tuntutan di mana IP telah dijadikan defendan. Dalam kes ini, IP telah didatangi oleh penyamar-penyamar yang mahu menggunakan perkhidmatan IP untuk menerima dana wang asing ke dalam akaun anakguam IP (client account). Penyamar-penyamar tersebut telah menyamar sebagai wakil-wakil suatu syarikat Malaysia yang dikenali. IP gagal membuat semakan latar belakang anakguam kerana IP yakin bahawa kerja yang diarahkan kepadanya ialah sah. Dana wang asing itu (yang kemudiannya diketahui merupakan hasil penipuan-penipuan *phishing* dan penyamaran identiti yang telah dilakukan oleh penyamar-penyamar tersebut ke atas suatu syarikat asing) telah dibayar ke dalam akaun anakguam IP. Pada hari yang sama IP menerima dana wang asing itu, IP telah mengeluarkan suatu cek tunai kepada penyamar-penyamar tersebut yang kemudiannya telah menghilangkan diri. IP hanya mengetahui tentang penipuan yang telah dilakukan selepas disampaikan dengan suatu Writ & Pernyataan Tuntutan.

Apabila Syarikat Insurans telah dimaklumkan, Syarikat Insurans telah menolak perlindungan insurans. Ini adalah kerana transaksi yang telah dilakukan oleh IP (membenarkan akaun anakguamnya (client account) digunakan semata-mata untuk tujuan menerima dana wang asing), bukanlah suatu perkhidmatan yang wajar diberikan oleh seseorang peguamcara atau peguam bela dalam profesion undang-undang berdasarkan Akta Profesion Undang-Undang 1976. Lebih malang lagi, IP juga tidak menyimpan apa-apa dokumen berhubung dengan transaksi tersebut. Syarikat Insurans terpaksa menolak alasan IP bahawa IP telah bertindak sebagai pemegang amanah kepada dana wang asing tersebut memandangkan tiada sebarang bukti untuk menunjukkan bahawa terdapatnya suatu perjanjian di mana IP telah dilantik sebagai pemegang amanah.

Apakah tindakan yang anda akan ambil sekiranya anda berada dalam situasi sebegini?

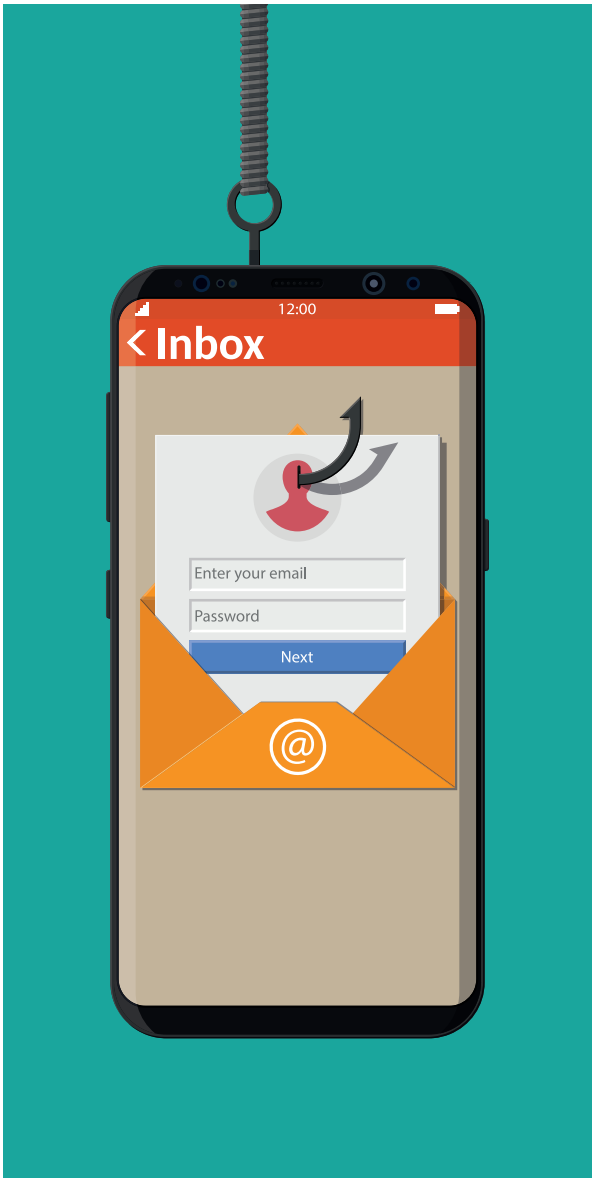
Pengajaran:
Elakkan diri daripada ditipu dan disalahgunakan oleh penipu-penipu dan peminjam-peminjam wang dengan menjalankan semakan latar belakang ke atas individu atau syarikat yang bakal menjadi anakguam. Sahkan identiti dan latar belakang mereka terutamanya jika mereka mendakwa untuk mewakili seseorang atau sesebuah entiti yang lain. Jika terdapat perkara yang mencurigakan tentang identiti anakguam atau tentang transaksi tersebut, anda hendaklah lebih berhati-hati atau pertimbangkan untuk berhenti daripada bertindak. Buat Laporan Transaksi Mencurigakan kepada pihak berkuasa. Ini haruslah dilakukan untuk melindungi firma anda daripada menjadi mangsa frod dan untuk mengelakkan diri daripada hukuman-hukuman di bawah Akta Pencegahan Pengubahan

Wang Haram dan Pencegahan Pembiayaan Keganasan 2001.

PENIPUAN -PENIPUAN *PHISHING*

Dalam suatu notifikasi tahun 2016, sebuah IP telah menerima suatu emel yang kononnya dihantar oleh anakguamnya. Emel tersebut mengandungi pautan untuk memuat turun dokumen-dokumen yang telah diminta oleh IP daripada anakguamnya. Setelah IP mengikuti pautan itu, IP telah dibawa ke halaman log masuk emel IP yang mendorong IP untuk memasukkan kembali nama pengguna dan kata laluan akaun emel IP. Walau bagaimanapun, sebaik sahaja IP memasukkan nama pengguna dan kata laluannya, akaun emel IP dikunci dan IP tidak lagi dapat mengakses akaun emelnya. Hanya selepas itu IP tahu bahawa akaun emel anakguamnya telah digodam, dan telah digunakan untuk memancing maklumat peribadi IP. Pada keesokkan harinya, IP telah dimaklumkan oleh anakguam-anakguam IP serta rakan-rakan sekerja IP mengenai suatu emel yang diterima oleh mereka kononnya dari akaun emel IP. Emel tersebut meminta mereka memasukkan bayaran fi guaman dan pinjaman wang ke dalam suatu akaun bank tempatan yang bukan dimiliki IP. Sesetengah anakguam IP telah menjadi mangsa dalam penipuan ini dan telah membayar wang kepada penggodam tersebut.

Pengajaran:
Sentiasa berwaspada terhadap emel-emel yang meminta maklumat peribadi atau maklumat anakguam. Sentiasa sahkan alamat-alamat emel untuk memastikan bahawa tiada apa-apa perbezaan. Jangan klik pautan-pautan yang tidak diketahui. Sebaliknya, taipkan alamat halaman web sepenuhnya. Jika terdapat sebarang keraguan, hubungi orang yang meminta maklumat itu dan bercakap secara langsung dengannya. Pastikan sistem komputer firma anda dilindungi dengan perisian keselamatan yang terkini.



KESELAMATAN SIBER & PERLINDUNGAN DATA

oleh Dennis Goh, Pengurus Penasihat Undang-undang,
Jardine Lloyd Thompson Sdn Bhd

KESELAMATAN siber merupakan suatu risiko yang perlu ditangani oleh firma guaman pada masa kini. Ini kerana peguam turut tidak ketinggalan dalam menggunakan teknologi bagi penyediaan perkhidmatan yang cekap dan berkesan kepada klien mereka. Namun begitu, firma-firma guaman, terutamanya amalan yang kecil, meskipun terdedah kepada pelbagai risiko, sering sahaja ketinggalan dalam persediaannya terhadap serangan siber disebabkan kos tinggi yang perlu dilaburkan. Tak kira saiz sesuatu firma, bagi memastikan suatu program keselamatan siber yang berkesan dapat melindunginya, apa yang diperlukan adalah sekurang-kurangnya perisian digital yang terkini, walaupun kosnya mungkin agak mahal.

Walau bagaimanapun, adalah tidak wajar sekiranya anda anggap bahawa anda tidak mungkin menjadi sasaran hanya kerana firma anda merupakan sebuah amalan yang kecil. Setiap firma guaman mempunyai maklumat bernilai di pasaran ekonomi jenayah. Apatah lagi apabila memikirkan bahawa kebanyakan jenayah siber merupakan jenayah berlandaskan peluang *(crimes of opportunity)*. Penggodam sentiasa mencari sistem yang paling terdedah dan akan menyerangnya terlebih dahulu!

Serangan siber boleh menyebabkan pelbagai kemungkinan yang tidak baik bagi firma-firma serta klien mereka. Antaranya termasuklah perlanggaran am maklumat sulit, pencurian dana klien dan juga ketidakupayaan mengakses sistem IT dalaman firma tersebut. Kesemua senario sedemikian boleh menjurus kepada suatu tuntutan PII terhadap sesebuah firma.

APAKAH YANG BOLEH DILAKUKAN OLEH FIRMA GUAMAN?

Adalah mustahak untuk memahami bahawa walaupun terdapatnya perisian dan peralatan bagi menangani ancaman siber, sikap seseorang itu merupakan kunci utama.

FAHAMI RISIKONYA: Sentiasa dan kerap membuat kajian semula sistem keselamatan siber firma anda serta prosedur yang diaturkan bagi memastikan firma tersebut mempunyai perlindungan yang terbaik. Secara idealnya, laburkanlah wang untuk perisian perlindungan, perkakasan yang terkini dan latihan bagi pihak kakitangan untuk melindungi firma tersebut dari serangan siber. Nilai kerugian kewangan yang mungkin dihadapi disebabkan suatu serangan siber ke atas firma guaman anda adalah lebih tinggi berbanding sebarang pelaburan kos terhadap keselamatan siber yang mencukupi.

SENTIASA DIMAKLUMKAN: Pastikan anda kemaskini dalam hal teknologi, isu-isu keselamatan serta ancaman siber. Kemudian, atur langkah-langkah yang perlu bagi menghalang atau mengurangkannya.

PETUNJUK: Langgani laman sesawang serta blog teknologi untuk mendapatkan pengemaskinian mingguan atau bulanan yang PERCUMA.

SULITKAN DAN LINDUNGI DATA ANDA: Penyulitan *(encryption)* adalah proses menukarkan data menjadi kod rahsia. Hanya seseorang yang memegang kata laluan rahsia atau cipher pertukaran *(conversion cipher)* khas boleh membaca atau mendapat akses kepada fail yang telah disulitkan itu; lantas begitu, penyulitan merupakan suatu cara yang berkesan untuk memastikan hanya mereka yang diberi kuasa (melalui penyerahan kata laluan atau cipher itu) mendapat akses kepada data tertentu. Oleh yang demikian, penggunaan teknik menyulitkan dokumen adalah suatu langkah keselamatan yang amat berkesan apabila hendak menghantar dokumen sulit melalui emel.

KATA LALUAN: Pastikan semua peralatan digital terlindung dengan kata laluan. Pastikan tiada peguam dan kakitangan firma anda yang meninggalkan komputer atau komputer riba mereka merata-rata tanpa pengawasan dengan tidak menggunakan peranti menguncian. Gunakan kata laluan yang kuat, iaitu yang menggunapakai pencampuran fon, kes kata, nombor serta simbol. Jangan sesekali mengunakan tarikh lahir anda atau orang-orang kesayangan mahupun nama-nama orang kesayangan anda sebagai kata laluan.

PETUNJUK: Sukar mengingati kata laluan? Gunakan peranti atau aplikasi penyimpanan kata laluan. Lebih baik dari itu, tuliskannya di atas kertas atau di dalam sebuah buku nota dan simpan di tempat simpanan yang berkunci dan selamat, di mana-mana tempat selain dari tempat anda menyimpan komputer anda. Penggodam tidak boleh menggodam buku nota fizikal yang disimpan dalam laci berkunci.

KESEDARAN: Adakan latihan yang dihadiri semua kakitangan di firma anda bagi meningkatkan kesedaran mengenai keselamatan siber, ancaman dan langkah-langkah berjaga-jaga yang perlu mereka lakukan. Terapkan kepentingan untuk sentiasa peka dan berwaspada.

PEMATUHAN: Ketahui dan fahamilah isi kandungan Akta Perlindungan Data Peribadi 2010 ("PDPA") dan isu-isu berhubung isu data perlindungan klien. Pematuhan PDPA adalah bahagian kritikal dalam sesuatu strategi keselamatan siber.

KITA HANYA BOLEH MERANCANG

Tiada langkah berjaga-jaga yang sempurna. Oleh yang demikian, ia adalah penting bagi kita merancang untuk sebarang kemungkinan. Tidak kira betapa canggih pun sistem komputer atau betapa tingginya bajet keselamatan siber anda, tiada organisasi yang langsung lali atau tahan terhadap kerugian kewangan dan reputasi yang timbul akibat kerosakan melalui insiden siber. Oleh yang demikian, anda disyorkan membeli Polisi Insurans Siber yang menyediakan perlindungan terhadap kerugian yang mungkin timbul akibat jenayah siber dan lain-lain kerosakan sistem komputer.

Untuk mengetahui lebih lanjut mengenai manfaat Polisi Insurans Siber, sila hubungi Jardine Lloyd Thompson Sdn Bhd di 03-2723 3241 atau secara emel di mbar@jltasia.com.

SKIM Mandatori PII
BADAN PEGUAM MALAYSIA
TAHUKAH ANDA?

PII: ADAKAH IA MELIPUTI INSIDEN SIBER?

Secara amnya, Polisi PII Mandatori menyediakan indemniti terhadap tuntutan liabiliti sivil, kos pembelaan dan kos mitigasi. Oleh yang demikian, indemniti disediakan sekiranya anda disaman oleh klien kerana gagal melindungi data sulit mereka.

Apa yang tidak diliputi apabila suatu perlanggaran siber berlaku adalah kos dan liabiliti firma anda sendiri, iaitu kehilangan pendapatan disebabkan ancaman, kerosakan atau kehilangan maklumat atau penggunaan sistem yang timbul dari penggunaan sistem dan rangkaian komputer firma anda.

Bagaimanakah boleh firma-firma menguruskan kos yang timbul akibat serangan siber?

Walaupun firma-firma boleh mengatur langkah untuk mengelakkan dan mengurangkan risiko serangan siber, firma-firma juga perlu bersedia untuk menguruskan kos yang timbul akibat risiko berkenaan. Untuk menguruskan dan pulih dari kerugian yang timbul, amatlah penting untuk memperolehi perlindungan di bawah Polisi Insurans Siber yang berasingan.

Broker bagi Skim PII Mandatori untuk pihak Badan Peguam telah merancangkan Polisi Insurans Siber yang spesifik sebagai pelengkap liputan yang diberi bawah Polisi PII Mandatori tersebut. Polisi Insurans Siber ini melindungi firma anda dari kebanyakan kos dan perbelanjaan yang mungkin timbul disebabkan suatu serangan siber, perlanggaran sistem perlindungan rangkaian atau insiden siber yang melibatkan pembekal perkhidmatan pihak ketiga.

Sekiranya anda ingin tahu lebih lanjut mengenai manfaat sesebuah Polisi Insurans Siber, sila hubungi Jardine Lloyd Thompson Sdn Bhd di 03-2723 3241 atau secara emel di mbar@jltasia.com.

Nota: Di bawah Skim Mandatori PII, perlindungan adalah tertakluk kepada terma pengecualian, had dan syarat-syarat 'Certificate of Insurance'.

Terjemahan berkaitan 'Master Policy', 'Certificate of Insurance' dan contoh ilustrasi adalah sebagai panduan sahaja, dan sekiranya terdapat perbezaan antara Bahasa Inggeris dan terjemahan Bahasa Malaysia, versi Bahasa Inggeris akan digunakan.

PERLINDUNGAN DI BAWAH POLISI PII WAJIB DAN POLISI INSURANS SIBER

Liabiliti Di Bawah Undang-Undang / Liputan Pihak Ketiga	Polisi PII Wajib	Insurans Siber
Disebabkan kegagalan melindungi data sulit dari ancaman atau pelepasannya secara tidak sengaja	√	*√
Disebabkan kegagalan atau perlanggaran keselamatan sistem komputer	√	*√
Bagi tuntutan perlanggaran data yang mungkin tidak melibatkan anakguam atau merangkumi penyediaan perkhidmatan profesional (tidak termasuk tuntutan oleh kakitangan atau penjual pihak ketiga)		√
Tuntutan liabiliti media (cth perlanggaran hakcipta/tanda niaga, fitnah, plagiarisme dsb)	√	*√
Kos guaman dan perbelanjaan yang timbul akibat membela tuntutan pengawalseliaan oleh pihak berkuasa dan sebagainya		√
Denda atau penalti pentadbiran data (yang boleh diinsuranskan mengikut undang-undang)		√

**di mana liputan PII bertindih, Insurans Siber tersebut menyediakan penambahan ("top-up") pada PII Wajib*

Kos Sendiri / Liputan Pihak Pertama	Polisi PII Wajib	Insurans Siber
Kos akibat tindakbalas perlanggaran termasuk kos nasihat undang-undang pakar, perbelanjaan forensik IT dan kos pemakluman		√
Perbelanjaan perhubungan awam dan pengurusan krisis		√
Kos pemulihan data (kos untuk memulihkan data elektronik, perisian dan program)		√
Kehilangan pendapatan dan perbelanjaan tambahan akibat dari perlanggaran perlindungan dan kegagalan teknologi sistem komputer anda		√
Pemerasan siber		√
Denda, kos penilaian dan perbelanjaan tuntutan yang timbul bagi membela Tuntutan Kad Bayaran Industri		√

PEGUAM MENGALAMI MASALAH BURNOUT

oleh Mohan Sankaran, Penasihat Risiko Undang-undang, Jardine Lloyd Thompson Sdn Bhd

Masalah dan fenomena **BURNOUT** semakin menjadi pandemik dalam persaudaraan guaman. Burnout ditakrifkan sebagai kelesuan fizikal atau mental disebabkan kerja secara berlebihan atau tekanan mental. Baru-baru ini, seorang pengerusi syarikat guaman global yang gergasi, Baker McKenzie memutuskan untuk mengundur diri buat sementara, dengan memberi keletihan sebagai alasan utamanya. Malangnya, enam bulan selepas keputusannya, beliau telah meninggal dunia. Budaya kerja di kebanyakan firma guaman – waktu bekerja yang panjang, beban kerja yang besar dan klien yang suka mendesak – merupakan factor menyebabkan peguam mengalami *burnout*.

MENURUT American Bar Association, *burnout* merupakan suatu kemudaratan kesihatan yang memberi kesan kepada peguam seantero dunia. Ia disebabkan persepsi ketaksamaan di antara desakan kerja serta sumber yang sedia ada (secara material mahupun emosi) pada seseorang kakitangan[1]. Di Malaysia, memandangkan hampir 90% firma guaman kita merupakan firma kecil[2], tak hairanlah bahawa peguam di sini turut mengalami gejala yang sama walaupun pengalaman mereka tidak dilaporkan. Peguam dalam kategori ini meluangkan kebanyakan masa mereka di pejabat, cuba menangani dan mengatasi kedesakan kerja mereka sambil cuba mencari punca kehidupan. Mereka tidak mempunyai masa untuk diluangkan pada diri

1. https://www.americanbar.org/publications/law_practice_magazine/2012/may_june/burnout-avoidable-not-inevitable/

2. Professional Demographics Statistic as at 02.05.2018 by JLT

mereka sendiri mahupun keluarga mereka. Masa demi masa, ini menyebabkan keadaan *burnout* berlanjutan dari tekanan fizikal dan emosi yang berpanjangan.

Begitulah juga keadaannya bagi rakan kongsi di firma-firma besar. Kerja mereka amat mendesak disebabkan tuntutan tinggi untuk mencapai sasaran pendapatan dan prestasi kerja. Dengan permintaan firma yang semakin meningkat setiap tahun, ia menambahkan lagi tekanan demi mencapai sasaran.

Gejala-gejala Peguam Yang Mengalami *Burnout*

Gejala-gejala lazim seorang peguam yang mengalami *burnout*:

- Menjadi semakin cepat marah dan tidak sabar;
- Hilang selera makan;
- Perasaan perlu memaksa diri hendak ke kerja setiap hari;
- Sentiasa lesu dan tidak bermaya;
- Gagal menumpukan perhatian; dan
- Masalah tidur atau sering mengalami sakit kepala.

Kesemua ini mempunyai kesan yang mendalam terhadap hubungan peribadi dan profesional anda. Sekiranya anda mengalami mana-mana gejala-gejala tersebut, ia perlu ditangani dari awal sebelum ia memberi kesan terhadap perhubungan anda, memudaratkan kesihatan mahupun meragut nyawa.

Cara Menangani Burnout

1. Berundur seketika dan perhatikan keadaan anda pada masa ini.
2. Buat penilaian yang jujur terhadap beban kerja dan tanggungjawab anda.
3. Kenalpasti penyebab utama tekanan yang membuat anda merasa *burnout*.
4. Fikirkan cara untuk tidak mengambil beban fail baru sementara anda menangani *backlog* yang sedia ada.
5. Minta sokongan dan pertolongan dari rakan sekerja.
6. Pantau rutin kerja dan perbaikinya.
7. Laburkan wang terhadap perisian pengurusan kes dan pejabat.
8. Amalkan cara hidup yang lebih sihat – selalu bersenam, amalkan pemakanan yang sihat, lakukan meditasi atau yoga.
9. Pastikan anda mendapat rehat dan tidur yang mencukupi.
10. Pastikan anda mempunyai sistem sokongan sosial yang baik; pergunakanlah masa bersama rakan-rakan dan keluarga secara baik.

Sekiranya semua cara di atas gagal membantu dan anda masih berasa tertekan, sudah tiba masanya untuk mendapatkan bantuan profesional.

Pelajari Teknik MENDELEGASI KERJA

oleh Mohan Sankaran, Penasihat Risiko Undang-undang, Jardine Lloyd Thompson Sdn Bhd

KINI, klien sudah semakin mendesak. Begitulah juga tanggungjawab profesional anda. Senarai kerja yang perlu dibuat semakin meningkat bila tarikh mahkamah dan mesyuarat memenuhi diari anda. Ia memaksa anda meluangkan lebih masa untuk menanganinya – bak pepatah yang tak lekang dari kerja: terlalu banyak kerja dan tak cukup masa *(too many things to do, not enough time)*. Sebagai pemilik firma kecil, perasaan tertekan dan terharu sering membelenggu.

Kegagalan anda mendelegasi kerja mungkin menghalang anda dari mencapai keseimbangan antara kerja dan kehidupan *(work-life balance)*. Ini kerana minda anda akan sentiasa memikirkan hal kerja meskipun anda sudah meninggalkan pejabat, seperti merisaukan cara-cara mencapai sasaran tarikh kerja, mengejar yuran yang masih belum berbayar, mendapat fail baru, dan senarainya tidak akan berkesudahan. Oleh yang demikian, dalam memikirkan pelan jangka masa panjang, memperolehi bantuan seorang peguam pembantu boleh mengurangkan beban anda. Lebih-lebih lagi, bagi firma-firma kecil yang amat menintikberatkan langkah-langkah pengurangan beban kos bulanan, kos tambahan menggajikan seorang peguam bantuan turut menambahkan kerunsingan. Oleh itu, dalam hendak mencapai keseimbangan kerja-kehidupan yang lebih sihat, anda perlu memikirkan mana lebih penting - memaksimakan pendapatan atau mendapatkan bantuan.

Semua alasan semata-mata!

Bak kata pepatah ***"Nak seribu daya. Tak nak seribu dalih."***

Antara alasan yang paling kerap dipetik untuk tidak mengajikan pembantu atau tidak mendelegasi kerja adalah kerana terlalu sibuk dan tidak ada masa atau kesabaran untuk mendidik orang lain. Tambahan pula, bagi firma yang lebih kecil, isu kos tambahan turut merupakan suatu halangan yang difikirkan sukar diatasi. Sesetengah peguam senior lebih sanggup memilih untuk mendraf segala perkara kecil sendiri dari mendelegasi kepada peguam baru, atas premis bahawa masa yang diperlukan untuk memperbetulkan kerja yang dilakukan oleh peguam baru itu lebih membebankan. Tidak kurang juga kemungkinan terdapatnya isu perasaan tergugat dan tidak rasa selamat serta kerana takut hilang kawalan.

Walau apapun, perlu juga diingat bahawa mendelegasi kerja bukanlah bererti anda melepaskan tanggungjawab kepada yang lain, sebaliknya ia merupakan perkongsian tanggungjawab agar seorang individu sahaja tidak terharu dan terbeban dengan tanggungjawab lain.

Bagaimana Hendak Menugaskan Kerja

Menugaskan kerja ada caranya yang tersendiri.

1. Belajar untuk Mempercayai

Tingkatkan keyakinan diri dalam meletakkan kepercayaan dan tanggungjawab pada seseorang lain. Ingat kembali masa bila *master* anda meletakkan kepercayaan pada anda semasa anda baru memulakan amalan? Jadi begitulah juga anda perlu melakukannya. Janganlah terperangkap dengan kerja-kerja rutin; delegasikanlah perkara-perkara kecil ini. Ia akan mengurangkan beban anda dan meluangkan masa anda. Si *protégé* atau penerima akan mempelajari kerja itu dan dari hari ke hari memperbaiki dirinya dalam menguruskannya. Ia akan mengajar mereka untuk mengambil tanggungjawab atas kerja yang didelegasikan kepada mereka serta mengambil kerja yang lebih rumit di masa akan datang.

Cadangan: Dengan masa yang terluang, anda boleh menambahkan klien firma atau mengambil cuti yang sudah lama diimpikan, dimana kesihatan mental dan fizikal adalah sesuatu yang penting untuk jangka masa panjang.

2. Beri Arahan Yang Jelas

Bila mendelegasi kerja, beri penjelasan dan arahan menggunakan bahasa dan langkah / jalan kerja yang mudah dan tidak rumit. Pastikan orang yang menerima kerja itu memahami arahan yang diberikan serta hasil yang diharapkan. Jangan anggap mereka memahami anda secara otomatik. Dengan cara ini anda juga boleh mengukur kebolehan mereka dan boleh mendelegasi kerja mengikut kebolehan setiap individu. Oleh yang demikian, anda boleh memperolehi kualiti tanpa perlu banyak membuat pembetulan.

Cadangan: Ukur kedalaman dan tahap pemahaman si penerima kerja dengan cara meminta beliau mengulangi pemahaman arahan yang diberikan. Ambil langkah pembetulan sekiranya pemahaman si penerima kerja tidak tepat; antaranya melibatkan cara bercakap dengan lebih perlahan, memecahkan langkah-langkah menjadi langkah lebih kecil dan mudah ditangani (perkara yang mungkin anda sudah ambil ringan memandangkan usia dan pengalaman yang ada pada diri anda), atau menggunakan perkataan yang lebih mudah difahami. Apabila kerja siap dihantar, bandingkan dengan arahan yang diberikan. Ulangi hingga kerja itu siap dan langsung memuaskan.

3. Berikan Kuasa Yang Perlu

Jangan masuk campur urusan kerja yang remeh *(micromanage)* selepas mendelegasi kerja kepada seseorang. Berikan kakitangan anda kuasa yang secukupnya untuk melaksanakan tugas yang diberi. Jadilah seorang mentor dan bukannya diktator! Berilah mereka peluang untuk tampil dengan idea dan cadangan sendiri bagaimana hendak menanganinya. Ini menggalakkan kreativiti serta membina keyakinan diri. Menyekat kebebasan kuasa hanya menyebabkan tugas itu lebih sukar dijalankan.

Sekiranya ia berterusan, mereka akan menjadi kecewa dan ini menimbulkan perasaan benci dan geram, yang tidak baik untuk dinamiks organisasi dalam jangka masa panjang.

Cadangan: Membenarkan kakitangan anda untuk menguruskan fail yang kecil dengan penyeliaan yang minima membolehkan perkembangan organisasi anda. Peguam baru dan kakitangan anda akan membina dan meningkatkan kemahiran, pengetahuan dan kebolehan sendiri, dan ini akan memberi keyakinan kepada mereka dan turut meningkatkan kebolehan mereka dalam membuat kerja.

4. Pantau Perkembangan

Sekiranya anda risau kehilangan kawalan, pantaulah perkembangan setiap tugasan yang ditugaskan untuk meredakan kerisauan. Pantau dengan cara mengadakan mesyuarat dan meminta laporan kemaskini secara berkala agar selalu mengukur nadi urusan tugasan. Bukan sahaja pantauan berkala merupakan cara menguruskan risiko, tetapi juga untuk memastikan kakitangan dan peguam baru menyiapkan tugasan yang diutuskan pada masa yang dikehendaki. Selanjutnya, ia membolehkan anda menemui sebarang kesalahan di peringkat awal dan memperbetulkannya sementara tugasan tersebut berterusan.

Cadangan: Jadualkan dan beri masa untuk mengadakan mesyuarat dengan ahli-ahli pasukan anda sekurang-kurangnya sekali seminggu atau setiap dua minggu. Ambil minit mesyuarat agar ada rekod yang mudah dirujuk semula, membolehkan anda memantau tugasan yang diutus dan merancang tugas sampingan menjurus ke mesyuarat seterusnya. Ia turut membolehkan anda memantau dan menjejaki beban kerja pejabat secara amnya.

Biasalah perasan kurang selesa apabila anda mula-mula cuba membahagi kerja. Walau bagaimanapun, ini adalah sesuatu yang perlu diamalkan. Mendelegasi kerja akan menjadi lebih mudah. Semakin ia diterapkan, alah bisa tegal biasa. Apabila sudah menjadi lazim, ini membolehkan masa anda lebih terluang dan membolehkan anda fokus pada kerja lain atau mengambil kerja baru untuk guaman anda. Jangan lupa tugasan baru anda, percaya, menyelia dan pantau.

PII & 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
Legal Risk Junior Counsel
Email: mysahra@malaysianbar.org.my

Shamine Parisamy
Legal Risk Junior Counsel
Email: shamine@malaysianbar.org.my

Azwa Zulsamli
Officer
Email: azwa@malaysianbar.org.my