ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 10/24 (October)

Defending Justice: Cybersecurity in the Legal Sector

INTRODUCTION

1. Law firms, which form the backbone of the legal sector, play a diverse yet vital role in society. Law firms have different functions from ensuring that private firms and individuals comply with the law and act in accordance with adopted regulations, to protecting intellectual property rights, to administering personal matters such as wills and divorce arrangements. In some countries, they have counterparts in the public service, which in effect acts as the prosecutor and legal advisor to the government, like the Attorney-General's Chambers in Singapore. Collectively, they form the legal services sector, which ensures that the rule of law is upheld in a country. Like most industries today, firms in the legal sector increasingly rely on information technology and digital services in their operations. Due to the unique nature of their work, the legal sector needs to process large volumes of confidential and sensitive data – both personal and commercial – with such data increasingly being digitised.

CYBER THREATS FACED BY LEGAL SERVICES

2. Advancements in digitalisation has made the legal services sector vulnerable to a range of cyber threats. Legal firms are especially vulnerable to third-party risks, given that their businesses are client-facing. Some of the impact of cyber-attacks include: data breaches that have undesirable legal and reputational consequences; data leaks that threaten the commercial and personal interests of clients; and cloud security issues with significant consequences for non-compliance with regulatory frameworks.

3. In 2023, the ABA Cybersecurity TechReport found that 29% of surveyed law firms in the United States suffered a security breach. Such security breaches have a significant financial impact on affected law firms, since security breaches can be associated with ransomware where malicious actors demand a ransom in exchange for the safe return of compromised data. A 2023 survey by Arctic Wolf Networks found that legal organisations paid USD1 million on average for ransoms in ransomware incidents. Yet, law firms do not seem thoroughly prepared to deal with such cyber threats. The same survey by Arctic Wolf Networks found that only 26% of surveyed law firms were "very prepared" to deal with cybersecurity breaches and incidents.

Case in point:
In 2016, journalists from German newspaper Süddeutsche Zeitung obtained 11.5 million documents that came from Mossack Fonseca, the law firm at the centre of the Panama Papers. These documents contained information of widespread corrupt activity, such as the use of shell companies to commit tax fraud. The allegations led to the resignation of the high-profile individuals that were implicated, including Iceland's former Prime Minister Sigmundur Davíð Gunnlaugsson. Although some alleged that the data leak came from an anonymous insider, Mossack Fonseca asserted that it was from a hack. Ultimately, Mossack Fonseca was forced to fold in March 2018 as a result of the incident.

This example highlights the widespread reputational damages and consequences arising from cyber breaches, which will no doubt have an adverse impact on their future operations.

CYBERSECURITY CHALLENGES SPECIFIC TO LEGAL SERVICES

4. Organisations like law firms in the legal services sector handle a multitude of sensitive data, ranging from client data, commercially sensitive information and case details to intellectual property rights (IPRs). The following are examples of the consequences of cybersecurity breaches that law firms face, depending on the nature of work that they engage in. The impact is not just on law firms but also consequences for the clients they serve.

a. Family Law. Law firms involved in family law handle a variety of confidential information ranging from family disputes, divorce settlements to wills. In the example of divorce settlements, law firms may handle data concerning the settlement of assets and the custody of children, who are minors. In the event of a data breach, crucial

information may be leaked to the other party, therefore potentially jeopardising the client's case. The law in many countries like Singapore has added confidentiality protections afforded to children and minors, such as the Children and Young Persons Act (CYPA), that seek to protect the anonymity of children involved in legal disputes, given that children are much more vulnerable and require these safeguards to ensure their rights and well-being. A data breach for family law firms may compromise confidential data of children and minors, therefore increasing their vulnerability and risks of exploitation.

b. IPRs. Law firms involved in the protection of IPRs handle sensitive corporate data that safeguard the business interests of their clients. These IPRs provide legal protection for a business' innovations, creative works and brand identity, therefore ensuring their competitive advantage over competitors. A cybersecurity breach of IPR law firms potentially exposes these IPRs to the wider public, therefore compromising on the competitive advantage of impacted client businesses. This may in turn hinder the growth and profitability of client businesses. Additionally, in cases where client businesses are involved in the production of goods of strategic value to a country, the compromising of such data can have wider economic and national security impacts on a country.

c. Criminal Law. Law firms involved in criminal law handle sensitive case data that is used to help influence decisions that guide the criminal lawsuit. From the perspective of plaintiffs, it is in their interest that the defendant does not get hold of data that can compromise the plaintiffs' chances of winning a case. Therefore, a cybersecurity breach exposes such sensitive and confidential data, which may derail the plaintiffs' efforts in winning the lawsuit. Likewise, the same can be said from the perspective of defendants, who want to maintain the integrity of data that can help them win the lawsuit against the plaintiff.

5. Additionally, the continued operations of law firms are built upon a trust that is established between firm and client, as clients necessarily entrust sensitive and confidential information to the law firms that they engage. The continued operations of law firms, as well as future professional relationships that law firms

may build with potential clients, hinge on this established trust. Consequently, cybersecurity breaches represent a break in this established trust, not only risking professional working relationships with existing clients but also risking reputational damage that has consequences on securing new clients in the future. Therefore, guarding against such breaches is key to sustaining this trust.

6. Given the nature of their work, law firms are required to comply with a plethora of regulatory frameworks that seek to safeguard the integrity of their operations. The following are a few examples of such regulatory frameworks:

a. Data and privacy laws, which address issues of data security and privacy, and that aim to safeguard the use of personal data. Such data and privacy laws are often legally binding, requiring all companies, including law firms, that are operating within a specific jurisdiction to follow. For instance, Singapore established the **Personal Data Protection Act (PDPA)** that has been administered by the Personal Data Protection Commission since 2013. Other ASEAN countries have also adopted similar data and privacy laws. For instance, Brunei Darussalam is guided by the **Data Protection Policy** since 2014 and in the Philippines, the **Data Privacy Act** was first adopted in 2012. On a regional level, ASEAN first adopted the **ASEAN Framework on Personal Data Protection** in November 2016, which seeks to establish principles and norms that facilitate the implementation of personal data protection laws in the region. This mirrors the **General Data Protection Regulation (GDPR) act**, first published by the European Parliament in April 2016.

b. **ISO/IEC 27001** is an international standard for information security management systems. Despite the adoption of ISO/IEC 27001 not being mandatory, law firms choose to comply with it as a commitment to strong cybersecurity practices to reassure their clients of data protection measures.

c. All law firms operating in the United Kingdom are regulated by the **Solicitors Regulation Authority (SRA) Code of Conduct**. This Code of Conduct ensures that law firms protect the confidentiality of their clients, such as through the secure handling of all electronic communications and personal data.

7. In some cases, law firms that are working in specific areas must further comply with relevant regulatory requirements. Examples include:

a. **Health Insurance Portability and Accountability Act (HIPAA)** that applies to law firms in the United States that deal with healthcare-related information. HIPAA dictates that these relevant law firms must ensure the confidentiality and integrity of any and all electronic health records and to prevent any unauthorised access.

b. Law firms in the United Kingdom that either provide services for financial activities or represent clients in the financial services sector are required to comply with regulations set out by the **Financial Conduct Authority (FCA)**. These FCA regulations help to ensure the integrity of financial operations and also promote competition in the sector.

c. Singapore law firms that handle case data concerning information about children and minors are required to comply with **CYPA**, first published in 1993. Other ASEAN countries have since followed suit in implementing similar regulatory requirements that put additional safeguards for handling the data of minors, like **Malaysia's 2001 Child Act** and **Thailand's 2003 Child Protection Act**. These extra safeguards for the handling of the data of minors are essential, given the vulnerable position of children who are not old enough to make informed consent decisions.

8. Data breaches or cyber-related incidents carry a range of risks and consequences for those impacted. Apart from reputational damage, loss of clients and regulatory compliance issues as outlined above, compromised organisations might face legal consequences, financial damages, operational disruptions and even increased cybersecurity and insurance costs. The fallout from cybersecurity breaches should inspire organisations to put in place necessary measures to prevent breaches in the first place.

CYBERSECURITY BEST PRACTICES

9. Given the consequences of cybersecurity breaches in the legal services sector, it is important for them to implement best practices that safeguard their cyber operations. The following are examples of best practices that can be adopted:

a. Implementing robust cybersecurity policies and procedures. In the digital age, it is essential for the legal services sector to ensure that all software used is up to date, as software updates can contain features that fix malware or potential software vulnerabilities that have been detected. To that end, the information technology department can configure automatic update functions on internal hardware, such as laptops.

b. Securing client communications and electronic filings. By using encryption software, confidential information can be secured behind a password or key. Similarly, organisations can adopt access control to restrict the flow of sensitive information. These are important measures that limit the damage of any data breaches or hacks that the organisations might face, since they both limit the flow of confidential information and prevent data readability.

c. Continuous training of personnel. Newly-inducted personnel should be trained about the organisation's cybersecurity best practices so as to equip them with the necessary know-hows that prevent data breaches, such as through phishing. However, cyber threats are ever-evolving to become increasingly sophisticated and evasive. As such, it is critical that existing personnel are also continuously trained in cybersecurity best practices, so that their domain knowledge is refreshed and upskilled.

d. Implementing an incident response plan. As much as organisations seek to prevent cyber-attacks, it is essential that organisations have an incident response plan that can deal with these undesirable cybersecurity breaches in case it happens. By establishing

appropriate protocols, organisations can contain the fallout and damages of cyber breaches.

e. Conducting regular internal and external reviews. It is important for organisations to ensure that only the right stakeholders have access to the necessary information, and nothing more. Regular internal and external audits are helpful in ensuring this, and these audits can also serve to check that former employees no longer have access to the organisations' databases. Additionally, these audits can cross check that external vendors only have access to the necessary internal data for the duration of their projects.

f. Secure storage and sharing of data. In past cases of data breaches, organisations have had their operations impaired due to difficulties with accessing compromised data. As such, organisations should back up their data to secure clouds and servers, and adopt sensible policies regarding the sharing of such data. This serves to ensure operational resilience even amidst data breaches.

g. Ensuring mobile security. Covid has accelerated the use of personal electronic devices, such as mobile phones, where work may be done remotely and shopping and other transactions may be done online. Mobile security may thus be a potential blind spot for many organisations as the personal electronic devices of employees fall out of the purview of an organisation's information technology department. Therefore, organisations should look at the necessary encryption of corporate data accessed on such devices, such as by setting up 2-factor authentication that adds an additional security layer.

FUTURE TRENDS AND CHALLENGES

10. Given the ever-changing technology landscape, the nature of cybersecurity threats that the legal services sector faces will keep evolving. For instance, the legal services sector has begun to leverage AI since it raises operational efficiencies, thereby having a positive impact on workforce productivity. Yet, the increased use of AI carries new and emerging threats as well, as AI can be subject

to abuse by cyber criminals, who may carry out ransomware attacks or AI-assisted hacking. Organisations therefore need to be cognisant of such risks and their potential impacts.

CONCLUSION

11. Organisations in the legal services industry come under increasing cybersecurity threats that threaten to paralyse their operations and compromise their reputations. Furthermore, given the client-facing nature of the legal services industry, cybersecurity breaches have implications on their clients too, potentially exposing client data to the detriment of clients. As previously mentioned, additional safeguarding measures should be given to protect minors. To that end, Singapore established CYPA in 1993, with other ASEAN countries following suit. More generally, client data needs to be protected and regulated, with various ASEAN countries passing regulations to safeguard the use of personal data like PDPA in Singapore. Mirroring the European Union's GDPR, ASEAN has implemented the ASEAN Framework on Personal Data Protection, which seeks to synchronise personal data protection regulations in the region.

12. Beyond the need to follow personal data protection regulations, it is essential that law firms implement cybersecurity best practices and contingency plans to react appropriately to cyber breaches, so as to contain the fallout and damages. Additionally, given the ever-evolving landscape of cybersecurity threats, the legal services sector needs to keep abreast of developments in this sphere, thereby ensuring that their operations are not compromised by organisational blind spots.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •

REFERENCES

1. The Top 11 Legal Industry Cyber Attacks – Arctic Wolf
https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/

2. What is a Civil Case – SG Courts
https://www.judiciary.gov.sg/who-we-are/what-is-civil-case#:~:text=One%20party%20files%20an%20application,defendant%20settles%2C%20the%20case%20concludes

3. 2024 Law Firm Data Security Guide – Clio
https://www.clio.com/blog/data-security-law-firms/

4. 5 Lessons From Law Firm Data Breaches – Lupl
https://lupl.com/blog/law-firm-data-breach/

5. Cyber Threats and Cyber Defence in the Legal Sector – Law Gazette
https://lawgazette.com.sg/practice/tech-talk/cyber-threats-and-cyber-defence-in-the-legal-sector/

6. General Data Protection Regulation – Intersoft Consulting
https://gdpr-info.eu

7. Personal Data Protection – IMDA
https://www.imda.gov.sg/about-imda/data-protection/personal-data-protection

8. ISO/IEC 27001:2022 – ISO
https://www.iso.org/standard/27001

9. SRA Code of Conduct for Solicitors, RELs and RFLs – Solicitors Regulation Authority
https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors/

10. HIPAA For Professionals – U.S. Department of Health and Human Services
https://www.hhs.gov/hipaa/for-professionals/index.html

11. FCA Handbook – Financial Conduct Authority
https://www.handbook.fca.org.uk/handbook

12. Data and privacy protection in ASEAN: What does it mean for businesses in the region? – Deloitte
https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf

13. Children and Young Persons Act 1993 – Singapore Statutes Online
https://sso.agc.gov.sg/Act/CYPA1993

14. Act 611: Child Act 2001 – Laws of Malaysia
https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Malaysia-Child-Act-1.pdf

15. Thai Family Laws: Child Protection Act – Thailand Law Online
https://www.thailandlawonline.com/thai-family-and-marriage-law/child-protection-act