Guardians of Confidentiality: Navigating Cybersecurity and Data Protection in Legal Practice

by

Steven Thiru, President of the Commonwealth Lawyers Association[1]

The effectiveness of legal rules in general, and data subjects' rights in particular, depends to a considerable extent on the existence of appropriate mechanisms to enforce them. In the digital age, data processing has become ubiquitous and increasingly difficult for individuals to understand. To mitigate power imbalances between data subjects and controllers, individuals have been given certain rights to exercise greater control over the processing of their personal information.[2]

As legal professionals, we operate under strict ethical standards and professional conduct rules. At the heart of these duties lies the lawyer's obligation of confidentiality, which protects clients' right to privacy and underpins legal professional privilege. The profession rests on trust, and that trust depends in great part on the secure handling of client data. In today's digital era, safeguarding confidentiality demands vigilance in both cybersecurity and compliance with evolving data protection laws.

Professional Responsibility in the Face of Cybersecurity Threats

Cybersecurity is the practice of protecting people, systems, and data from cyberattacks by using various technologies, processes, and policies.[3]

Cybersecurity has become a critical concern for legal practitioners, as law firms increasingly store vast quantities of confidential and commercially sensitive information in digital form. Recent cyber incidents affecting law firms across multiple Commonwealth jurisdictions illustrate both the scale of the risk and the ethical responsibilities lawyers face in responding to it.

High-profile cases demonstrate how law firms have become attractive targets for cybercriminals. Hackers exfiltrated approximately four terabytes of sensitive client information and financial data from an Australian law firm's servers and demanded a ransom. When the firm refused to pay, a significant portion of the data was published online. The court granted injunctive and subsequent default relief, highlighting the limits of legal remedies once

[1] Ng Wan En and Allysha Anne Ronald assisted in the preparation of this paper.
[2] European Union Agency for Fundamental Rights, European Court of Human Rights and Council of Europe, *Handbook on European data protection legislation* (Publications Office of the European Union, Luxembourg 2018) 205.
[3] Alexandra Jonker, Gregg Lindemulder, and Matthew Kosinski, 'What is cybersecurity?' (IBM) <https://www.ibm.com/think/topics/cybersecurity> accessed 13 January 2026.

confidential data has already been disseminated. Similar issues arose in *XXX v Persons Unknown*,[4] where a UK firm sought injunctive and summary relief with the aim of having the judgment recognised and enforced in foreign jurisdictions after hackers accessed and threatened to publish confidential client data.

A Singaporean law firm was reportedly subjected to a ransomware attack in 2024, and allegedly paid a substantial ransom to secure the release of encrypted data, illustrating the commercial and ethical dilemmas firms may face when balancing client protection against encouraging criminal conduct. Cyber risks are not limited to external attacks either; it was reported that a different Australian law firm's payroll data leak in 2025 arose from an internal breach involving the unauthorised dissemination of sensitive employee information, demonstrating that insider threats and weak internal controls can be equally damaging.

These incidents underscore why cybersecurity is not merely a technical issue, but a professional one. Lawyers owe a duty of confidentiality, which is a foundational ethical obligation of the legal profession. Protecting client information today necessarily includes securing electronic files against unauthorised access, loss, or disclosure. A failure to implement reasonable cybersecurity safeguards risks breaching this duty, even where disclosure is inadvertent rather than intentional.

Closely related is the duty to protect a client's property.[5] Professional conduct rules define client property broadly to include correspondence, files, reports, and other documents, which plainly encompasses digital records. Caring for such property as a careful and prudent owner would require lawyers to consider and address foreseeable cyber risks through appropriate information technology ('IT') security planning.

In light of these obligations, substantive and practical measures are essential. Law firms should provide ongoing training to ensure that lawyers and staff understand confidentiality obligations, appreciate their ethical responsibilities when handling data, can recognise common cyber threats including phishing attempts, and know how to respond to such threats in accordance with established protocols. Firms must also at least secure electronic information systems by encrypting sensitive data, enforcing strong password policies and multi-factor authentication, implementing an emergency 'kill switch' protocol, and maintaining secure backups to ensure data recovery in the event of a breach.[6]

Evolving Data Protection Standards in the Commonwealth

Data protection is the practice of safeguarding sensitive information from loss, corruption, or unauthorised access, typically in compliance with regulatory requirements.[7]

---

[4] [2022] EWHC 2776.
[5] Bryan P Schwartz, Monica Adeler, Mike Myschyshyn and Robert Walichnowski, 'Cybersecurity and law firms' (2021) 21 Asper Review of International Business and Trade Law 59.
[6] ibid.
[7] ibid (n 3).

Across the Commonwealth, most jurisdictions have enacted data protection regimes — albeit with varying stages of development — that impose statutory obligations on organisations, including law practices, to secure personal data and respond appropriately to data breaches.

In the United Kingdom, the Data Protection Act 2018 gives domestic effect to the UK General Data Protection Regulation, mirroring the EU's General Data Protection Regulation 2016. It imposes stringent duties on data controllers and processors, covering lawfulness, transparency, data minimisation, and security, with significant administrative fines for non-compliance. The recent Data (Use and Access) Act 2025 aims to foster innovation and economic growth by modernising the UK's digital information framework while maintaining robust individual data protection rights.[8]

In Malaysia, the Personal Data Protection Act 2010 ('PDPA') regulates the processing of personal data in commercial transactions, and was amended in 2024.[9] The amendments strengthen accountability through mandatory breach notifications, appointment of data protection officers, and enhanced penalties. The recent Guidelines for Cross Border Personal Data Transfer ('CBPDT Guidelines') issued by the Personal Data Protection Commissioner of Malaysia in April 2025 also provide the operational details and practical steps required for compliance in relation to cross-border personal data transfers under the PDPA.[10]

Australia's regime is centred on the Privacy Act 1988 (Cth) and Australian Privacy Principles. More recently, the Privacy and Other Legislation Amendment Act 2024 introduced a statutory tort for serious invasions of privacy, enhanced enforcement powers, and frameworks for children's online privacy and doxxing.[11]

Hong Kong regulates personal data under the Personal Data (Privacy) Ordinance (Cap. 486), most recently amended in 2021 to introduce offences of doxxing.[12] Complementing these obligations, Hong Kong's Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) came into force on 1 January 2026, establishing the city's first comprehensive

---

[8] Information Commissioner's Office, 'The Data Use and Access Act 2025 (DUAA) – what does it mean for organisations?' (ICO 2025) <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/> accessed 9 January 2026.

[9] Kandiah S, 'The privacy, data protection and cyber security law review: Malaysia' (2017) 4 Law Business Research Ltd 220.

[10] Greenleaf G, 'Malaysia's complex new guidelines on cross-border data transfers' (2025) 196 Privacy Laws & Business International Report 20.

[11] Eliza-Jayne Sinclair and Kelly Dickson, 'Australia's 2024-25 Privacy law reboot: Rewiring data protection, security and enforcement' (Lexology 2025) <https://www.lexology.com/library/detail.aspx?g=1c24b74c-7b4a-42f8-b849-2537f0e18bbb> accessed 9 January 2026.

[12] Privacy Commissioner for Personal Data (PCPD), 'The Personal Data (Privacy) Ordinance' (PCPD) <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html> accessed 9 January 2026.

cybersecurity regime for critical infrastructure. Obligations cover organisational measures, preventive controls for computer systems, and incident reporting.[13]

Although some Commonwealth countries have implemented cross-border personal data transfer mechanisms, the diversity of domestic regimes nonetheless presents compliance challenges for law firms that operate across borders or handle client data processed in multiple jurisdictions. Recognising this fragmentation, Commonwealth Law Ministers adopted the Commonwealth Model Provisions on Data Protection ('CMP')[14] in November 2022. Described as one of the strongest international privacy instruments developed,[15] the CMP provides a comprehensive template covering consent, cross-border data transfers, breach investigation mechanisms, privacy compliance obligations, and restrictions on data usage.[16] While not legally binding, it serves as a harmonisation tool for legislators seeking to modernise or align national data protection laws.

Recent developments in data protection regimes across Commonwealth jurisdictions signal a move towards the modernisation of personal data protection, aimed at strengthening safeguards against cyberattacks and misuse, while also supporting commercial and technological growth. Accountability for organisations is enforced through statutory powers, mandatory breach notifications, and the rights of individuals to exercise control over their personal data.

For legal practitioners, this means that protecting client information is not just a professional and ethical duty under professional conduct rules, but also an increasingly significant legal obligation that demands both organisational and technical safeguards to maintain client confidentiality. From a practical standpoint, practitioners should ensure that personal data is processed lawfully and transparently; implement robust security measures; and detect, document, and report data breaches promptly in accordance with statutory deadlines.

Cybersecurity and Data Protection as Professional Imperatives

In modern legal practice, cybersecurity and data protection have become inseparable pillars of ethical and professional responsibility. Cyberattacks and data breaches can cause irreparable harm to clients, law firms, and public confidence in the legal profession. Lawyers and law firms

[13] Gabriela Kennedy and Joanna K.C. Wong, 'Hong Kong passes first cybersecurity legislation for regulating critical infrastructures' <https://www.mayerbrown.com/en/insights/publications/2025/07/hong-kong-passes-first-cybersecurity-legislation-for-regulating-critical-infrastructures> accessed 10 January 2026.

[14] The Commonwealth Office of Civil and Criminal Justice Reform, 'Model provisions on data protection' (Commonwealth Secretariat 2023) <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-02/ROL%20Model%20Law%20Provisions%20on%20Data%20Protection.pdf?VersionId=FpgmtvhD6E3dm3JfQiEVp8lP0zO_mGy0> accessed 10 January 2026.

[15] Greenleaf G, 'Model provisions for data protection in Commonwealth countries: How do they fit?' (2023) 184 Privacy Laws & Business International Report, 21.

[16] The Commonwealth, 'Commonwealth ministers adopt new model law to strengthen data protection rules' (The Commonwealth 2022) <https://thecommonwealth.org/news/commonwealth-ministers-adopt-new-model-law-strengthen-data-protection-rules> accessed 10 January 2026.

who fail to take reasonable steps to secure electronic information risk breaching their professional duties, with serious legal and ethical consequences.

Additionally, data protection has become equally critical, as lawyers must ensure that client information is processed lawfully, securely, and in compliance with evolving legal frameworks, including cross-border requirements.

With the increasing need to integrate cybersecurity measures and data protection compliance in everyday legal practice, the modern lawyer functions not only as an advisor and advocate but also as a guardian of confidential information, responsible for safeguarding client data in an era of cyber risks and global data flows.

Steven Thiru
President
Commonwealth Lawyers Association

19 January 2026

This paper was presented at the Presidents' Roundtable themed 'Ethics and Technology: Professionalism in the Digital Era' on 19 January 2026, on the occasion of the Ceremonial Opening of the Legal Year 2026 in Hong Kong.