Professional Indemnity Scheme – RME Bulletin

Jun 2026

Issue No. 17

Editor's Note

ESSAR Insurance Services Limited, Managers of the Professional Indemnity Scheme in collaboration with Panel Solicitors Clyde & Co., issue this quarterly bulletin to highlight risk management issues learned from their handling of claims.

Cybersecurity Incidents and Proposed Mandatory Data-Breach Notification: Risk Management Implications for Hong Kong Law Firms

Law firms hold large volumes of highly sensitive information, including personal data, financial records and client monies, making them attractive targets for increasingly sophisticated cyber threats. Cybersecurity is therefore a core professional risk that goes directly to a firm's ability to operate. Common incidents range from phishing and ransomware to data leaks, spoofing, insider threats and third-party breaches. The use of artificial intelligence has further amplified these risks by enabling attacks to be executed at greater speed, scale and precision.

This bulletin examines how cybersecurity incidents and proposed legal reforms impact risk management for law firms in Hong Kong and how they should respond to such incidents.

A Recap: Solicitors' Professional Duties to Guard Against Cybersecurity Risks

Cybersecurity obligations are not optional for law firms. Solicitors at all levels are under a positive duty to safeguard confidential client information and to ensure that their use of information and communication technology complies with both the law and professional standards. These obligations are primarily set out in the Hong Kong Solicitors' Guide to Professional Conduct (the "**Guide**") and guidelines published by the Law Society.

Principle 1.07 of the Guide requires solicitors to ensure that their use of information communication technology does not result in a breach of professional duties or any applicable laws. In practical terms, this places responsibility on solicitors to assess whether the technology they use (directly or through third parties) is fit for purpose and appropriately secured, based on the information and knowledge available at the time of use. *Principle 8.01 of the Guide* further requires solicitors to hold all client information, including electronic communications, in strict confidence, subject only to limited exceptions.

Involvement of All Levels within a Firm

While the implementation of appropriate systems, controls and safeguards is typically a matter led by partners and management within a law firm, all members, including associates and trainees, should remain vigilant to risks arising in day-to-day practice and adhere to firm policies. Effective risk management requires not only adequate firm-level controls, but also awareness, consistent application and engagement at the individual level.

Recent Developments: Cyber-Dependent Crimes and Proposed Mandatory Data-Breach Notification

In January 2026, the Hong Kong Law Reform Commission published its report on Cyber-Dependent Crimes and Jurisdictional Issues, recommending the introduction of standalone cybercrime legislation. The proposals aim to modernise Hong Kong's legal framework and address enforcement gaps by criminalising unauthorised access to computer systems and data, interference with electronic communications, and the possession or distribution of cyber tools such as malware or ransomware for criminal use.

Separately, in February 2026, the Privacy Commissioner for Personal Data announced plans to consult the Legislative Council on potential amendments to the Personal Data (Privacy) Ordinance (Cap. 486). Of particular note is the possible introduction of mandatory data-breach notification

requirements and administrative fines for non-compliance. If implemented, these changes would mark a significant shift from the current regime, under which breach notification is generally voluntary and financial penalties are limited.

What Can Go Wrong?

A Hypothetical Scenario – Inadequate Cybersecurity Safeguards

A solicitor acting in matrimonial proceedings asks a client to upload detailed financial disclosure documents, including bank statements and asset information, to an online file-sharing platform operated by a third-party service provider. Unbeknownst to the solicitor, the platform has had ongoing but unaddressed security weaknesses, having not been updated for over two years. A data breach occurred shortly after, and as a result, the client's confidential financial information was accessed without authorisation and later publicised online.

Potential Breaches and Liability

Such a failure may place the solicitor in breach of Principles 1.07 and 8.01 of the Guide, expose the solicitor to disciplinary action, and potentially give rise to civil liability to the client.

Immediate Response to Cyber Incident

The framework below provides practical guidance for managing the critical initial phase in the event of a cyber incident. Law firms are encouraged to seek specialist advice and customise the steps to align with their own cyber incident and breach response plan ("**Breach Response Plan**"), while solicitors at all levels should ensure familiarity and compliance with the same.

1. **Cyber incident detected**: activate response plan, immediately notify designated incident response team (IT, compliance, management)
2. **Contain the breach**: identify and isolate affected systems and networks; secure logs, emails and other potential evidence; prevent further unauthorised access and restrict compromised credentials (where applicable)
3. **Assess scope and impact**: initial assessment to identify the nature of the cyber incident; evaluate scope to determine whether personal, confidential or client data may have been compromised
4. **Internal escalation and external advisers**: notify senior management; notify insurers (including the Managers of the Professional Indemnity Scheme, where applicable), obtain external assistance from cybersecurity forensic specialist and legal advisers; obtain advice on whether the firm may need to notify affected clients and understand reporting duties across relevant jurisdictions
5. **Documentation and communication**: record all actions, decisions and timelines for compliance; manage client and stakeholder communications to mitigate further legal or reputational risk

Key Takeaways

In anticipation of the further legislative developments in Hong Kong, both firm leadership and individual practitioners must take active roles in strengthening cybersecurity resilience.

From a governance perspective, partners and management should ensure that cybersecurity frameworks are properly designed, resourced and reviewed. From an individual perspective, solicitors and staff must understand and consistently apply those frameworks in practice, including recognising risks, escalating concerns, and complying with internal protocols and reporting obligations.

Checklist – Practical Steps:

Effective implementation requires coordinated efforts: partners and management are primarily responsible for establishing and overseeing the cybersecurity frameworks, while solicitors at all levels must understand them, apply them consistently and escalate promptly when required.

Part 1: prevention is better than cure	**Part 2: rapid response / crisis readiness**
• Know your data risk profile • Review and implement cybersecurity policies and escalation procedures • Raise awareness through regular staff training • Review contracts with third-party service providers for appropriate security and contractual safeguards • Conduct regular IT security audits • Stay up to date with legal and regulatory developments	• Pre-appoint and train a data breach crisis management team (internal and external) • Develop a cyber incident and Breach Response Plan • Have a pre-agreed position on when forensic investigation will be used • Understand what your firm can cope with itself, what needs to be outsourced, and who you will outsource to