Incident Timeline

Day 0

Phishing Email and Initial Compromise

- A barrister – but it could be, just as well, a chambers' PA - receives a phishing email look like an official communication from Microsoft.
- The barrister clicks the (malicious) link and enters MS 365 credentials.
- The barrister approves the multifactor authentication (MFA) prompt.

Day 1

Threat actor accesses Microsoft 365

- The threat actor gains full access to the chambers' Microsoft 365 (OneDrive, SharePoint, and Exchange Online) for the barrister.
- The threat actor downloads electronic solicitor's briefs, counsel's advices and the barrister's emails with their solicitors and also senior/junior email traffic.

Days 2-3

Attack Escalation

- The threat actor escalates their access to other accounts within the chambers, downloading like material.
- The chambers' workstations, again, have basic **antivirus software**, but no endpoint protection (ie **EDR**).
- The threat actor installs malware on each barrister's workstation, captures keystrokes and gains more credentials for lateral movement across the network.

Day 4

Discovery of the Breach

- A staff member notices unusual file -sharing activity in OneDrive and reports it to IT administrator.
- The IT administrator investigates the logs, and discovers sensitive files were accessed and shared externally.
- The IT administrator suspects malicious activity and locks down the compromised barrister's MS 365 account.
- Chambers' barristers inform briefing solicitors – undertaken to Privacy Act 1988 (Cth) 72 hour window obligation – that their sensitive data has been exposed in the breach, and of the steps being taken to remedy this deleterious outcome.
- OAIC also notified within such 72 hour obligation.
- Ransomware demand received by email from Russian email address.

Days 5-10

Business Operation Impact

- Chambers' barristers engage legal advisors to advise on obligations under notifiable data breach scheme in the *Privacy Act 1988* (Cth).
- Barristers notify insurers, briefing solicitors and clients.
- Access to OneDrive and SharePoint is suspended to prevent further data loss, halting legal work by chambers' barristers on active cases.
- Chambers begins to experience significant operational disruptions (cannot access electronic briefs, advices and opinions; limited email access).

Days 5-15

Reputation and Client Trust Erosion

- As Chambers continues to respond to the incident, practice and reputational damage ensues as follows.
- Solicitors and their clients take action steps in response. Alternative counsel are briefed by solicitors.
- Such solicitors and clients reserve the rights to sue the barristers for damages.
- The breach is reported in the media, leading to negative publicity for the chambers and the individual barrister.
- Technical root cause analysis investigation reveals phishing email as the point of access for threat actor.

Days 15 - 20

Litigation and Regulatory Consequences

- The OAIC and the ASIC - given the nature of the breach and the potential exposure of personal data – each launch investigation s and reserve their right to prosecute for statutory contravention.

- The QLSC:

  - Launches an investigation, acing after the complaint of some affected solicitors and clients.

  - Reserves their right to prosecute each barrister for professional misconduct or unprofessional conduct under the *Legal Profession Act 2007* (Qld).

- Diminished paying work has been undertaken and much worry incurred, by chambers' barristers, in the interim.
- High costs for cyber remediation are incurred by chambers.
- Some disgruntled barristers advise they are looking to leave chambers, and join other groups.