Cyber Breach Readiness - Key Legal & Technical Steps

1. Preparation (Pre-Incident)

- Understand local legal requirements (especially in Asia: different notification timelines, different enforcement practices)
- Build a robust vendor-management system (technical and contractual due diligence)
- Ensure clear rights in vendor agreements : audit, termination, insurance requirements
- Maintain up-to-date, accessible, tested incident response plans
- Train teams; run simulations regularly

2. Detection & Initial Response

- Secure evidence immediately
- Consider privilege at the outset
- Rapid assessment of reporting obligations (notification timelines vary from 1 hour to 72 hours depending on the jurisdictions; some jurisdictions require criminal complaints prior to insurance coverage)
- Isolate affected networks; disconnect backups; disable compromised user access
- Engage forensics early (your own panel or insurer-recommended)

3. Containment & Eradication

- Legal and technical teams to align on scope, objectives and communications
- Maintain privileged and non-privileged workstreams separately
- Document decisions and rationales – future investigations or enforcement actions may require communicating this documentation
- Control internal/external communications: accuracy, consistency, no speculation

---

Listen to our podcast here.

We walk through the practical steps of managing a cyber incident – from first detection through to containment, stakeholder communication and post-incident risk mitigation.

Top tips from the panel:

- **Train relentlessly - simulations materially change outcomes**
- **Engage legal and forensics early**
- **Keep a clear decision log**
- **Avoid turning on auto-transcription tools that create risky records**

Common mistakes:

- **Not following (or not updating) incident response plans**
- **Inadequate documentation of decisions**
- **Informal internal chats that undermine later legal positions**
- **Premature or inaccurate public/regulator statements**
- **Overestimating privilege protections**

Cyber Breach Readiness - Key Legal & Technical Steps

4. Third-Party / Vendor Breaches

- Identify compromised data, data subjects, roles (controller/processor)
- Review contracts: liability caps, notification clauses, rights to forensics
- Expect limited access to forensic environments – consider relying on vendor reporting
- Escalate contractually if needed; ensure forensic reports are from reputable providers

5. Post-Incident & Litigation Risk

- Conduct a structured, legally-led internal investigation
- Preserve forensic findings, logs and key artefacts
- Ensure regulatory notifications are accurate and consistent
- For defendants: test whether claimants have suffered concrete loss
- Demonstrate reasonable care, prompt containment and remediation
- Consider seeking injunctive reliefs from vendors and ADR where appropriate

---

Talk to us

If helpful, we'd be very happy to:

- **Run a short tabletop exercise** with your team based on a sector-specific scenario; or
- **Review your incident response playbook** (including notification and privilege strategy) to spot any obvious gaps.
- **Present our Cyber Response + tool** that will allow you to be fully prepared for data breaches

No obligation at all – but if you'd like to explore either option, just let us know and we can set up a brief call.

Disputes in a Fragmenting World

This content forms part of our *Disputes in a Fragmenting World* initiative, which focuses on four widening fault lines where commercial pressure increasingly becomes disputes risk:

1. Digital opportunities
2. Asset valuation and financial volatility
3. Corporate accountability
4. Doing business across borders

Contacts

Simmons & Simmons

Robert Allen
Partner
T +44 20 7825 4852
Email Robert Allen

Sarah Bailey
Partner
T +44 20 7825 1613
Email Sarah Bailey

Jingyuan Shi
Partner
T +852 25838 346
Email Jingyuan Shi

Wiliam Dunning
Managing Associate
T +44 20 7825 4787
Email William Dunning

Emilie Danglades-Perez
Managing Associate
T +331 5329 1644
Email Emilie Danglades-Perez

Beazley

Jad Nehmé
Client Experience Manager
T +33 1 70 81 32 78
Email Jad Nehmé

For additional information on our firm, please visit our website at **simmons-simmons.com**.

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice.

Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.