LEWIS SILKIN

LS Response – a checklist to handling privacy incidents

Steps to take before an incident occurs

1. Identify your insurance coverage and requirements

- Consider taking out specialist cyber liability insurance.

2. Assemble your Incident Response Team

- Appoint a sponsor who will have overall responsibility for designing and implementing the initiative.
- The sponsor will assemble the *Incident Response Team* comprising:
    - Internal members in the form of senior executives from key business functions; e.g. IT/HR/Legal/Marketing & PR/Finance etc. Stand-ins for each role (in case of absences at the time of the response) should be identified.
    - External providers, to include:
        - Forensic investigators.
        - Crisis communications/PR experts.
        - Remediation providers.
        - Insurers.
        - Lawyers.

3. Create an Incident Response Plan

- The *Incident Response Plan* clearly describes what to do if an incident occurs and will usually document:
    - The sponsor.
    - Members (both internal and external) of the Incident Response Team and their respective roles.
    - Contact details (including out of hours).
    - Processes to be followed on discovery of an incident, or if one is suspected.
    - Key action points during and after an incident.
    - Timescales for completing those action points.
    - Reporting templates.
    - Drafts of internal/external communications likely to be issued.
- Ensure that the *Incident Response Plan* has buy-in from all *Incident Response Team* members, and keep it under review.
- Consider discussing the *Incident Response Plan* with your broker and insurer.

4. Privilege

- As part of your *Incident Response Plan*, establish a strategy to maximise your ability to maintain legal professional privilege.
- Be clear on the type of privilege you will rely on at each stage of an incident.

5. Know your data

- It's difficult to know what's been lost if you don't know what you've got in the first place, or where it is. Compile a data inventory (i.e. what data you hold and why) and keep it updated.
- Once you know what data you've got, work out why you've got it and where it came from. Are you a data controller or a processor?

- Identify where and how you are keeping the data. You're only as strong as the weakest link, so don't forget to review your supplier arrangements.
- If you don't already have one, create and implement a data retention policy to ensure you only keep what you need.
- Consider a full data and cyber security audit to identify potential issues and resolve them before an incident occurs. Our DataCheckPoint or other data audit services can help.

6. Practice makes perfect

- Run 'tabletop exercises' – which simulate a crisis – regularly. Doing so will make your response more fluid and provide opportunities for improvement.
- Ensure all staff receive training on preventing, recognising and reporting incidents.

7. Budget for a breach

- Breach preparation, including training, should be a budgeted business expense.
- Calculate the potential cost to your business of responding to a breach and allocate reserves.
- Discuss with your broker the cost of specialist cyber liability insurance.

Steps to take during an incident

1. Implement your *Incident Response Plan*

- Activate your *Incident Response Team* and put the *Incident Response Plan* into action.
- Investigate and contain the incident (usually with the assistance of IT security and forensics teams).
- Preserve evidence.
- Carry out a risk assessment.
- Assess the cause and extent of the breach. Questions which should be asked will include: What type of data is involved? How sensitive is it? Were there any protections in place? What has happened to the data? What could the data tell a third party about the individuals to whom the data relate? How many individuals are affected? Who are the individuals affected? What harm could come to them?
- Document your investigation and any decisions to create an audit trail.

2. Notification?

- In consultation with your legal team, some of the third parties you may need to consider notifying include:
    - *Insurer* – if you have a policy in place, one of your first contacts should be to your insurer (or broker). If you don't, cover might be declined. Some insurers will let you use your own team of trusted advisors. Others will have their own panel.
    - *Data Protection Authority (DPA)* – depending on the sector you operate in, you may already be subject to mandatory breach notification to the DPA and/or other regulators. From May 2018, where a breach involves personal data, you'll have 72 hours to report it to the DPA, unless exempted.
    - *Counterparties* – you may have entered into agreements containing a provision which requires you immediately to notify the counterparty in the event of a breach; e.g. if you provide services to that counterparty. From May 2018, all supplier agreements which involve the processing of personal data will contain such a provision. Note that where payment card data are affected, reports will likely also need to be made to payment card brands and/or acquirers to ensure compliance with industry standards – and, in most cases, immediately.
    - *Law enforcement* – where it is suspected that an incident involves criminality.
    - *Customers* – from May 2018, where a breach involving personal data is likely to result in "a high risk to the rights and freedoms of natural persons" then, unless exempted, those affected must be notified without undue delay. If a decision is taken to notify those affected, you'll need to think about what to communicate, and how.
    - *The media* – your internal and external communications teams will work closely with your reputation management lawyers to make external announcements, as well as to monitor and manage coverage in the press as well as social media.

Steps to take after an incident

- Has the cause of the incident been addressed to prevent a recurrence?
- In the longer term, be aware that regulatory and/or legal action can follow an incident, potentially making your privilege strategy all the more important.
- Evaluate your response and improve the *Incident Response Plan* with the benefit of lessons learnt.
- Update your data breach log (even if you didn't need to notify anyone) to record relevant details of the breach.

For further information please contact Nick Walker at nick.walker@lewissilkin.com or Ali Vaziri at ali.vaziri@lewissilkin.com.