LEWIS SILKIN

LS Response – a tactical approach to handling privacy and cyber security incidents

LEWIS SILKIN

Privacy and cyber security incidents come in many different forms. Attacks by hackers using technical expertise are usually the first thing that comes to mind. They are the stuff of headlines and film plots. But some of the biggest threats are more mundane and come from within. Think disgruntled or rogue employees. People are also prone to carelessness. Simple human error, such as a misdirected email or misplaced laptop, has the potential to cause just as much damage as an exploit by a hacker. As does a system glitch.

Whatever the cause, in a connected, always-on world, threats are constant and come from every direction. A recent government survey found that nearly half of UK businesses suffered a 'data breach' in 2016 – and that's just the ones those businesses know about or are prepared to tell outsiders. Mandatory breach reporting, which comes into effect from May 2018, will only increase public awareness of incidents suffered by organisations, as well as any shortcomings. With each incident that makes headlines, another organisation draws fire, harming its brand and reputation, not to mention its bottom line.

Organisations can also reap the commercial benefits of preparation in training and educating staff, and creating appropriate policies and procedures, ready to be put into effect if the worst does happen.

And at any time. Whilst you can't control when a privacy incident might take place, you can plan how you will respond to it. Planning reduces the impact of an incident, and helps prevent it from spiralling into a disaster. Ultimately, planning saves money: research shows that it reduces the costs associated with an incident, including in loss of business. In some cases, it can save a business from ruin.

The 'it won't happen to us' approach or leaving incident response to IT colleagues are no longer risk mitigation strategies that pass muster or that align with statutory obligations. Measures to be introduced from May 2018, such as fines of up to €20 million or 4% of global turnover, put that beyond doubt and are designed to make data privacy a board-level issue.

We're in it together

Responding to a privacy incident quickly and efficiently requires drawing on specialist skills which you won't necessary have within your organisation. Dealing with an incident is stressful enough without having to identify, instruct and liaise with various external advisors. That's why we've assembled a team of experts in fields such as IT, security, insurance and public relations, and keep them on standby to help when needed. Together, but with Lewis Silkin as your single point of contact, we cover all the angles and provide a seamless solution. So let us do the heavy lifting.

LS Response is an end to end solution to guide you through the before, during and after of a privacy or cyber security incident. Areas we can help you address.

Before

- Who does what? Assemble your Incident Response Team. Appoint a sponsor who will be responsible for designing and implementing the initiative, as well as leading the team. Internal team members should consist of senior executives representing key business functions; e.g. IT/HR/Legal/Marketing & PR/Finance etc. Don't forget their stand-ins. Make sure your external team is also in place. Those providers should know your business and have reviewed your Incident Response Plan. External team members will likely include forensic investigators, crisis communications experts, remediation providers and lawyers.
- What's the plan? Create an Incident Response Plan with input (and buy-in!) from key business functions and stakeholders. The plan will commonly document team members, their roles and responsibilities along with up-to-date contact details (including out of hours). It will set out the process to be followed on discovery of an incident (or if one is suspected) along with action points and timescales. It may also include reporting templates and drafts of communications which may need to be issued. The right response plan will help ensure that important matters aren't overlooked when up against the clock.
- Is it privileged? As part of your Incident Response Plan, establish a strategy to maximise your ability to maintain legal professional privilege in, for example, communications and reports. Be mindful of possible regulatory investigation and/or litigation (including group claims) in the event of an incident.
- Who's got what? 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 and keep it updated.
- Why have I got it? Once you know what you've got, work out why you've got it. Identifying whether you are a controller or a processor of data (or both) will inform your response to an incident. Only keep what you need. If you don't have a data retention policy, create one. Less data means lower risk, and that can only be a good thing when

things go wrong.

- How am I keeping it? The answer to this should be: 'safely' – though what is considered 'safe' will depend on what you're keeping. DataCheckPoint, a data and cyber security audit service which we provide with our selected partners (just one of our audit services), can help you identify any gaps in your information governance and then plug them. You're only as strong as the weakest link, so make sure your suppliers take their responsibilities as seriously as you do (remember, you could be on the hook for their failings).
- What should I do? It's one thing to write down a plan. It's quite another to put it into practice. 'Tabletop exercises' – which simulate a crisis – should be scheduled regularly. Doing so will make your response more fluid and provide opportunities for improvement. Wider staff training will help your people recognise and report potential issues.
- Who's footing the bill? 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. Cyber liability insurance can play an important role in risk mitigation. Your legal team will help you make sure that any policy is right for you.

During

- 'Who dunnit?' Activate your *Incident Response Team* and put the *Incident Response Plan* into action. Your IT security and forensics teams will need to move quickly to investigate and contain any incident. Evidence must be preserved. Working out the nature and volume of data compromised, as well as the cause and extent of the incident, is a priority. It will inform your response to an incident, especially when it comes to notification. Remember to create an audit trail by documenting the investigation and all decisions along the way.
- Do I have to tell anyone? If so: who, when and how? These are key strategic questions. Since the answers will have ramifications for your business, it is advisable to consult with your legal team. External notifications you might need to consider include:
  - *Insurer* – if you have a policy in place, one of your first contacts should be to your insurer. 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 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, those affected will generally need to 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 and social media.

After

- Is this fixed? If the cause of the incident has not been addressed, then it is likely to happen again. Next time round, critics are likely to be harsher.
- When will this end? Whilst the first 72 hours are crucial, the impact of a breach can endure for months, if not years, with regulatory investigations, litigation, rebuilding brand equity etc.
- What about next time? Once the dust has settled, evaluate the *Incident Response Plan* and improve it with the benefit of lessons learnt.
- Records up-to-date? Don't forget to record relevant details of the breach in a log which you can show your DPA (when asked).

LEWIS SILKIN

For further information on this subject please contact:

Nick Walker
Partner
T + 44 (0) 20 7074 8055
nick.walker@lewissilkin.com

Ali Vaziri
Senior Associate
T + 44 (0) 20 7074 8122
ali.vaziri@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com