Cyber security: data breach mitigation, planning & response

Data breaches are an immediate and critical risk that can give rise to significant reputational damage, loss of consumer trust, substantial regulatory fines, damages claims, and loss of corporate value. Breaches are increasing in frequency and scale, to the extent that experiencing a breach is now considered inevitable.

In addition to an external cyber attack there are a myriad of ways in which your business might be exposed to a breach: insufficient access controls; equipment failure; human error; environmental factors - such as flood or fire; and 'blagging' offences, where information is obtained via deception. With so many potential sources of a breach it is critical to plan ahead to reduce the likely impact of a data loss when it occurs.

Mitigating risk – planning

Accepting that a data breach is inevitable can provide the crucial edge needed to mitigate risk. The key preparatory steps are to:

- **Conduct a policy and procedure audit** - review IT, data, business continuity and disaster recovery policies and procedures
- **Secure your data -** encrypt all data, store and manage encryption keys, and control user access, assess network security, map data, and run penetration testing
- **Run a crisis simulation exercise –** so that you unearth any issues in your approach prior to a real breach occurring
- **Actively monitor threat levels on an ongoing basis**

Assembling a planning and incident response team

Your legal adviser will play a critical key role in ensuring your policy and procedure audit is robust and fit for purpose. And when a breach takes place your lawyers should be your first port of call - legal privilege can give you crucial protection over your communications when you need it most.

We can also help you select, in advance of a breach, the other advisers that will form your planning and incident response team. This could include:

- **Specialist cyber insurance providers**
- **Forensic IT and penetration testing experts**
- **Public relations crisis management consultants**
- **'Breach coach' advisors**
- **'Surge capacity' providers to field customer enquiries**

Why work with Wiggin?

We have the specialists you need under one roof - our highly regarded reputation management specialists will ensure your business's reputation is in the safest of hands, whilst our technology and data experts will guide you through the technical aspects of planning and breach management with ease.

Practical, clear advice for instant impact

We are trusted by some of the world's best-known businesses. Our lawyers work exclusively in the technology, media and brands sectors and tailor their advice based on analysis and experience of the client's situation. We deliver user-friendly, practical advice that can be readily implemented for instant impact.

Many of our lawyers have attended the ICO approved PDP and hold the Practitioner Certificate in data protection – each has achieved a distinction.

Flexible data breach planning and response service

Because clients' needs and the level of threat vary greatly, we don't believe that packaged cyber services provide enough flexibility. Instead we have developed relationships with a select group of relevant advisors, such as IT security consultants, public relations experts, surge capacity providers, and other specialists that fit your business. We work with, recommend, and connect our clients to the advisers that best meet their needs.

Managing an incident

If you've followed the steps outlined so far, you'll be in a good position to minimise the fallout and to manage the situation as smoothly as possible. The checklists below provide a high level overview of what you should do during a live incident, and flags the key points to avoid.

Post-breach action list

- Activate the incident response team
- Establish a secure communication channel
- Establish a "privileged" reporting and communication channel
- Interview personnel involved
- Use independent cyber/forensic experts
- Stop additional data loss
- Secure evidence
- Preserve computer logs
- Document the data breach
- Consider involving law enforcement and/or regulators
- Determine legal, contractual and insurance notification obligations
- Change security access and passwords

What the market says

"Everyone I have dealt with is extremely commercially aware and their advice always takes account of the practicalities. We feel confident placing our reputation in their hands."

Chambers & Partners

"Lawyers who are actually willing to answer questions and not sit on the fence."

Client feedback in relation to cyber security and data protection advice

Cyber response team - key contacts

Get in touch to find out how we can help you prepare your business:

Caroline Kean
Partner

t: +44 (0) 20 7927 9673
e: caroline.kean@wiggin.co.uk

Alan Owens
Partner

t: +44 (0) 20 7612 7715
e: alan.owens@wiggin.co.uk

David Naylor
Partner

t: +44 (0) 20 7927 6642
e: david.naylor@wiggin.co.uk

Patrick Rennie
Associate

t: +44 (0) 1242 631342
e: patrick.rennie@wiggin.co.uk