



Cyber Security Breaches – UK Legal Risk Exposures



Contents

3. Executive summary

3. Legal risks viewed in a timeline

4. Data Protection law risks

6. Other regulatory schemes

7. Compensation claims and litigation by impacted individuals – large scale litigation

8. Compensation claims and litigation by impacted individuals – micro claims

9. Breach of contract exposure in commercial relationships

10. Corporate governance issues

11. Insurance cover


11. Ransomware attacks

12. Globalisation of legal risks

12. Secondary legal risks resulting from the manner of Incident Response itself

13. Strategic and tactical considerations for contentious legal business

14. About DWF's Data Protection and Cyber Security practice



“Cyber security breaches can have many legal impacts, some of which are non-obvious. Organisations and their legal functions need to address these risks in their preparations for dealing with an incident and during incident response itself.”

Executive summary

This report provides an overview of the main types of legal risk exposures that can arise after a cyber security breach.¹

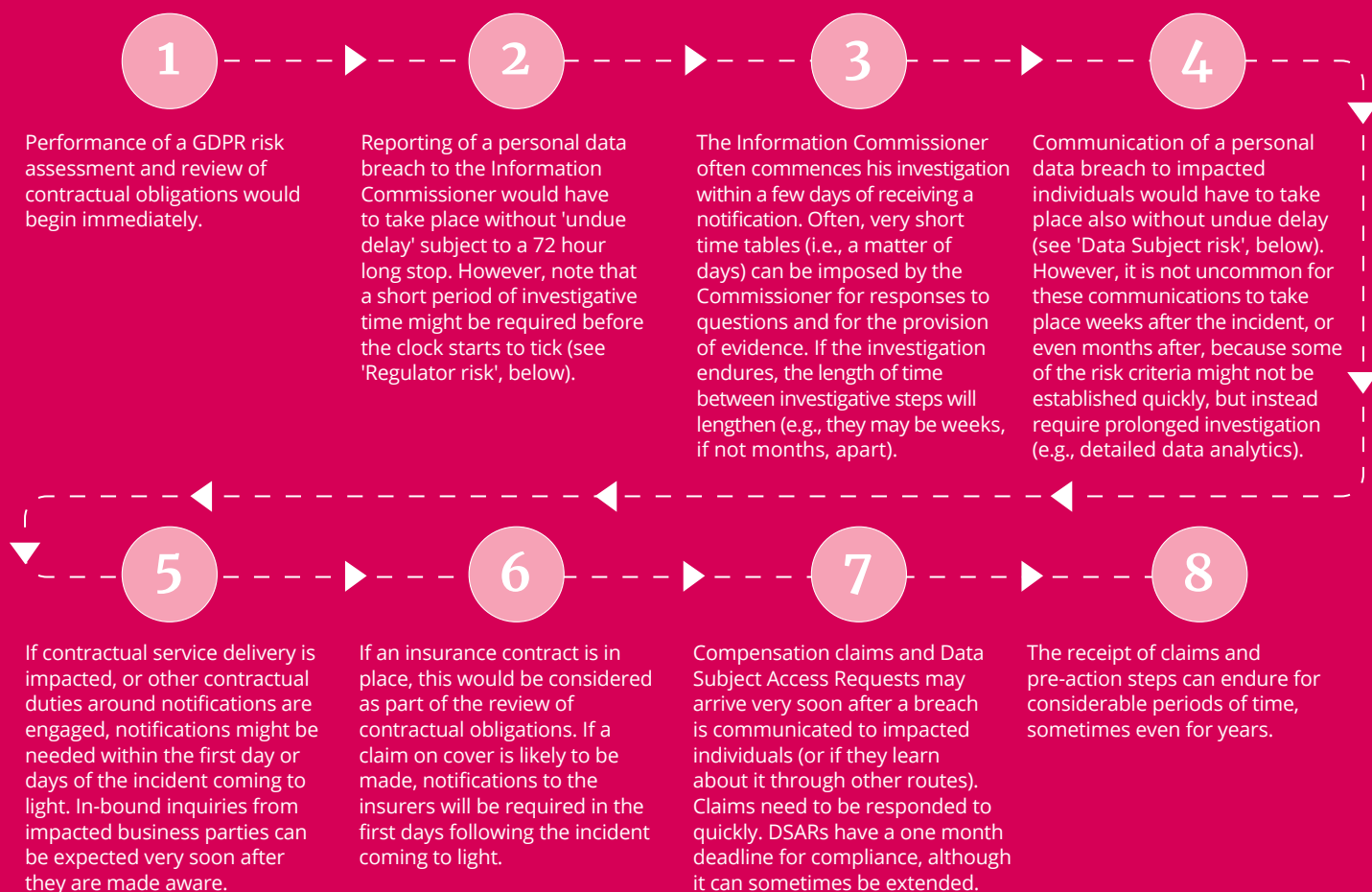
These include regulator risks, Data Subject risks (if the GDPR is engaged), compensation claims/litigation risks and breach of contract risks in B2B commercial situations. Poor security can also be framed as a corporate governance issue. For multi-nationals, legal risks may differ across territories and it should be noted that a decision taken for good reasons in one country can have negative impacts in another.

As noted in the final section, below, a discussion about legal risks following a cyber security breach is mainly a discussion about contentious legal business. Being successful in contentious business requires not only strong awareness of how regulatory

law, litigation and contractual breaches operate, but also foundational awareness of how security law and security operations interrelate. At the heart of this observation is the recognition that security law defers to the consensus of professional opinion on security operations, to set the detail of its requirements. Thus the question of whether or not there has been a legal contravention cannot be separated from an understanding of what would amount to reasonable operational security in a given scenario. The results of legal risk assessments can be distorted and unreliable if they build upon weak understanding of operational security.

Legal risks viewed in a timeline

The nature of the legal risks that will arise following a cyber security incident – and, therefore, the timelines that will apply for dealing with them – will be dependent on the nature of the incident. This includes the systems and data impacted; the impact on business obligations owed to third parties; and the range of regulatory and other private law obligations that are engaged. For example, if we were to assume that the incident impacted (1) the organisation's personal data; (2) the ability of the organisation to fulfil a contract with a third party; and (3) the systems/data of a third party, a typical timeline would be:



¹ These are viewed from the UK's perspective, mainly under English and Welsh law.

Data Protection law risks

These relate to personal data, such as (a) employee data; (b) personal data of people working for business partners; (c) and customer data. If an incident affects the confidentiality, integrity or availability of personal data, Data Protection law ('DP law') is engaged.

Breaches of DP law can generate four distinct forms of legal risk:

- 1. Regulator risk** – this includes investigations and regulatory action by the Information Commissioner;
- 2. Data Subject risks** – these involve the exercise of statutory rights by people whose data are impacted by an incident;
- 3. Litigation risks** – compensation claims brought by those people, for breach of statutory duty; and
- 4. Contractual risks** – where a supplier operating as a 'data processor' breaches the contractual duties that they owe to the 'data controller' under Article 28 of the GDPR, it could be exposed to a contractual damages claim. This is discussed in more depth in the section on exposure under commercial contracts. Note also that both parties could be exposed to regulator risk due to poor quality contracts, or poor contractual performance.

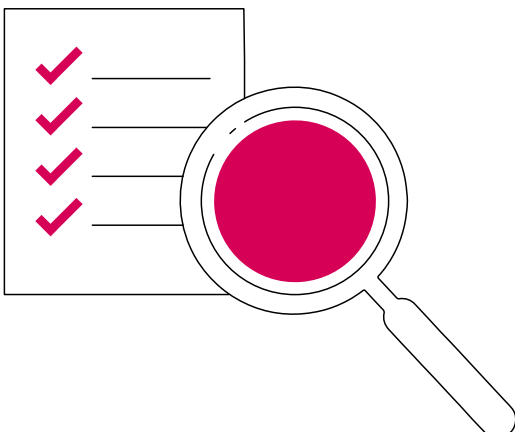
Regulator risk can involve these elements:

- 1. Breach notification** – a legal requirement arises under Article 33 of the UK GDPR, to notify the Information Commissioner's Office of personal data breaches that involve a risk to the 'rights and freedoms' of individuals. Where the notification duty applies, it must be complied with 'without undue delay', subject to a 72-hour long stop. A period of investigation might be needed before an organisation is aware that a notifiable breach has occurred, so the clock might not start to tick immediately upon discovery of the incident.
- 2. Regulatory investigations** – these are almost inevitable if you have to notify a breach. The impacts are variable and while most cases conclude quickly and without regulatory action, in serious cases investigations can run for many months, involving multiple investigatory steps all of which have business impacts and a need to incur professional services fees (legal and expert evidence).

A very serious investigation can involve formal regulatory audits and inspections, amplifying the business impacts and associated professional services fees, but these powers are used infrequently. More often, the investigation is a question and answer process conducted through correspondence that requires the organisation to give an account of their compliance with the law.

3. Contravention – a finding of a contravention of law. Specific requirements for security are found in Articles 5, 32, 33 and 34 of the UK GDPR, while Articles such as 24, 25, 28 and 35 necessarily require security issues to be addressed. If there is a contravention, the ICO can take the following kinds of regulatory action:

- a. Reprimands** – if the ICO concludes that regulatory action is warranted, the 'lightest' form is the service and publication of a reprimand. Publication can attract media attention and the interests of the claims management industry. There has been a recent step-up in publication of reprimands and DWF predicts that they will continue to increase in frequency.
- b. Enforcement Notices** – these order the organisation to take steps to change its systems and operations for data processing. The power is also used infrequently, but when it is used, the impacts can be dramatic. For example, if a database or information system has to be redesigned, or a business process stopped, the business could be dealing with a very substantial project. Enforcement Notices are always published.
- c. Monetary Penalty Notices** – depending on how the ICO frames the contravention, the Information Commissioner has the power to impose fines of up to 2% or 4% of the annual worldwide turnover of the undertaking (i.e., if the company is part of a group, the overall turnover of the group is counted, not just that of the legal entity in contravention). Fines are



still relatively uncommon and we are nowhere near the situation of maximum-level fines being imposed, but we are in the era of £multi-million fines. DWF predicts that fines will become more common-place during the tenure of the current Information Commissioner.

d. Conceptualising the impact of regulatory investigations/actions against large organisations, for professional services fees - cases where notifications are made but the investigations, which are probing, end quickly without formal action commonly incur legal fees in the range of £20 - £50K. More involved cases that conclude after twelve months with the taking of formal regulatory action commonly incur legal fees between £150-250K. These fees would not include the costs incurred in dealing with the wider elements of Incident Response, or the other legal risks identified below.

Data Subject risk can involve these elements:

a) Breach communications – a legal requirement to inform impacted individuals of a breach will arise under Article 34 of the UK GDPR if due to the incident a high risk to their rights and freedoms is likely. If the duty applies, these communications must be made without undue delay.

The operational impacts and associated costs are context-specific, but to give an example of a recent case that DWF handled: the client incurred more than \$500K in professional services fees for data analysis; over £175K in professional services fees from the experts who designed the overall strategy for operationalising the communications strategy; and legal fees related to all of those elements of £150K.

b) Data Subject Access Requests (DSARs) – once people are made aware of an incident, the exercise of statutory rights to access information are almost inevitable. If a large class of people are impacted by an incident, literally many hundreds of DSARs can be received in a very short space of time.

DSARs have to be satisfied within one calendar month, which can be extended to three months.

Failure to comply with a DSAR constitutes a standalone regulatory contravention, which can justify the ICO taking standalone regulatory action, thereby bringing into play all of the previous considerations.

The cost of dealing with a DSAR turns largely on:

- whether the data are structured or unstructured;
- the volume of data;
- whether forensic search technology is required; and
- the extent to which legal exemptions are applied.

A structured dataset with relatively anodyne information will result in low per capita costs. Email inboxes containing very large volumes of unstructured data that require detailed analysis and application of legal exemptions can cost result in high £thousands per capita costs.



Other regulatory schemes

The Data Protection regulatory scheme provides a useful frame of reference for understanding the essential priorities of all regulatory schemes that have a focus on cyber security. These essential priorities are:

- 1. Standards for security** – adhering to express or implied standards for operational security. These standards are generally risk-based and while there are 'baseline' controls that will be required whatever the situation, the law will require an operational risk assessment to be performed and due regard to be had for the consensus of professional opinion. Priority outcomes that standards for operational security should support are resilience against insecurity and the ability to competently respond to an incident.
- 2. Transparency** – when an incident reaches a particular level of seriousness, there is a general expectation of transparency with the regulator and, where necessary, with impacted parties.

- 3. Accountability** – regulatory powers of investigation are usually aimed at obtaining an account of how the organisation achieved compliance with its legal obligations.

A good example of another regulatory scheme where we see these principles in action is the one built around the Network and Information Security Regulations 2018 ('NIS', or 'the Cyber Security Regulations'). These Regulations require the Operators of Essential Services and some Digital Services Providers to implement measures to guard against the risk of cyber security incidents, with serious incidents needing to be reported to the Competent Authority. Sectors impacted are energy, transport, health and drinking water supply and distribution. Other sectors are likely to

be added, to honour a recent government consultation and to keep up with the pace of developments in the EU.

Similarly, under the Communications Act, telecommunications companies are required to report certain types of security breaches to Ofcom. The FCA and the PRA have taken action for failures of digital resilience.

Many schemes of professional regulation adhere to these ideas.



Compensation claims and litigation by impacted individuals

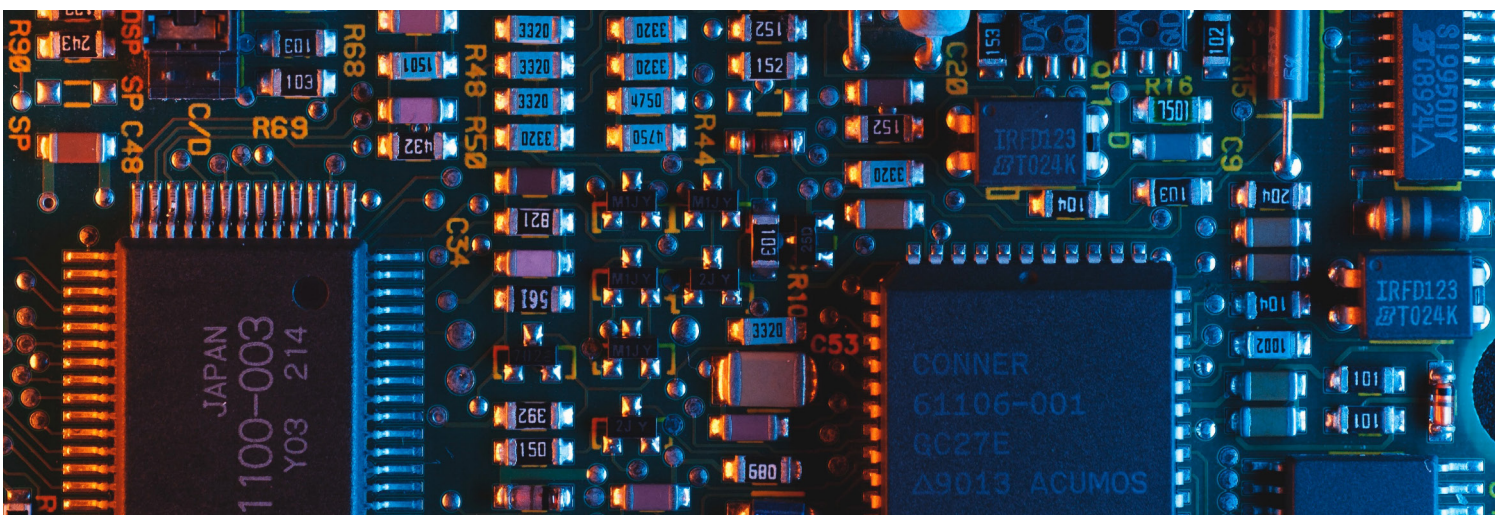
Large scale litigation risk.

1. Compensation claims are almost inevitable after a serious breach, that is if people are made aware of the incident through breach communications or through other routes (e.g., leaks, press reporting). The number of claims received generally correlates to the size of the class of people impacted. Where the class of impacted persons is large enough (usually, where thousands of people are affected), 'class actions' are a potential risk. These take two forms, namely 'group litigation' and 'representative actions'.
 2. If a claim relates to a personal data breach caused by a cyber attacker, it should be presented as a breach of statutory duty claim under the Data Protection Act. Other causes of action (tort of misuse of private information, confidentiality and Human Rights) have been held not to be suitable where the claim arises from a cyber-attack on an organisation that holds personal data that are impacted by the breach.
 3. Compensation under the DPA can be recovered for material and non-material damage, but the level of harm has to exceed the de minimis threshold to be compensatable.
 4. Regarding the size of the risk of large scale litigation, prior to the judgments of the Supreme Court in the Morrisons case (2020) and in Lloyd v. Google (2021), the risk of large-scale litigation was increasing exponentially, due to the expansion of the claims management industry and the impact of the GDPR breach communication rule. The claimants' losses in Morrisons and Lloyd (and subsequent cases involving DSG (2021) and TikTok (2022)) have taken much of the momentum out of the market. However, DWF perceive this as just temporary relief for businesses. We are expecting momentum to re-build in the medium term, as conceptually related litigation about the Phone Hacking Scandal has demonstrated that scalable litigation industries can be built around security and data contraventions.
- In the Morrisons case ('group litigation'), the group of claimants was 9,000. In the British Airways case the group was 16,000.
- Very large cases are multi-year problems for clients and they can generate £7-figure legal costs dealing with just the liability issues.

The maximum exposure in these cases is still very hard to quantify, as claimants and defendants are poles apart on how they should be valued, but an impacted class of 400K meriting £500 per person would be a notional exposure of £200M. Claimants would argue for much more, but Defendants are arguing for these cases to be disposed of in the 'small claims' court (where the usual costs rules do not apply).

The wider impacts of these types of cases for defendants can be enormous in terms of business overheads, future insurability, loss of productivity and stress impact, due to their duration and the volume and type of issues/steps that they involve. Claimant law firms try to build their fees (as costs follow the event in litigation), which can involve seemingly endless rounds of correspondence; the weaponisation of DSARs; attempts to obtain pre-action disclosure; the interim procedural steps of establishing the litigation; then the various steps that litigation involves once proceedings are issued, such as 'pleadings', case management conferences, strike-out and summary judgment applications and disclosure of documents and witness evidence.

Organisations sometimes have cyber insurance cover in place to deal with these cases.



Compensation claims and litigation by impacted individuals

Micro claims.

Speculative micro claims (i.e., a lone individual making a standalone claim) run alongside, or separate to 'class actions'. Often they have nuisance value, as the administrative headaches and costs involved in dealing with them can be greater than the amount claimed. This creates incentives to settle, as does the desire to avoid matters being dealt with by the courts, which might result in unhelpful precedents being set.

There are no clear statistics about the volumes of these claims, because the parties often reach confidential settlements and many of them are disposed of under insurance policies. To conceptualise the nature of the problem, DWF employs teams that deal with these matters on a daily basis.

On the other hand, these cases can sometimes be easy to 'bat off', as there are many barriers that litigants need to overcome to commence and win litigation.



Breach of contract exposure in commercial relationships

Businesses can be exposed to assertions of breach of contract, potential claims and perhaps termination of contracts if they suffer a security breach.

There are two broad scenarios:

- a) Party A suffers a security breach that impacts Party B's systems or data².
- b) Party A suffers a security breach that causes an outage or other incapacity rendering them unable to fulfil their contractual obligations owed to Party B.

Poorly drafted commercial contracts can also expose an organisation to regulatory risk. For example, the Data Protection Act requires operational security to be addressed in contracts between organisations and their suppliers (i.e., 'data processors' – see Article 28 of the UK GDPR). The quality of these contracts is a common focus area for ICO if a supplier causes an organisation to contravene its security duties. Similarly, in these situations the ICO regularly investigates the quality of the procurement process that led to the engagement of the supplier (i.e., pre-contractual due diligence).

Other contractual mechanisms that are commonly triggered by cyber security breaches include notification duties (party A should report an incident to party B); requirements to implement new security controls; and requirements to undergo inspections and audits.

Typical contractual problems that are encountered in the two broad scenarios identified above include:

- a) Party A is over-exposed to contractual claims by Party B, due to weak exclusion clauses and/or overly generous liability caps.
- b) Party B is unable to recover all of its losses caused by a breach of cyber security at Party A, due to strong exclusion clauses/liability caps.
- c) Deficits in the procurement process.

Noteworthy issues that often come to light when a cyber-attack leads to a problem in commercial contracts include:

- a) Procurement not requesting legal input - often the procurement process does not give adequate attention to the impact of cyber security risks for commercial contracts. This happens most frequently where the organisation lacks a general policy about the engagement of the legal team, or where the organisation has financial thresholds for the involvement of the legal team, meaning that some contracts can be formed without sufficient legal care and attention. This can result in clients being under-protected from harm caused by a third party, or over-exposed to its commercial partner's losses. If procurement had been dealt with differently in these cases, with appropriate involvement of the legal function, the contracts would have been more balanced.
- b) Weak or incomplete terms and conditions for security - procurement/contracting problems can cause an organisation to fail to address all of its statutory obligations for the content of commercial contracts, thereby undermining its ability to resist regulatory liability. Legacy contracts can be particularly problematic if they have not been updated to reflect legal changes.
- c) Inequality of bargaining power - sometimes there may not be room for negotiation of different liability terms, meaning that the commercial risk of a cyber security breach can be greater in some sectors than it might be in others for the same levels of operational risk. In situations where

the organisation needs to accept disproportionate legal risks, it will need to find compensating measures for risk mitigation (i.e., operate at a higher level of security that it might otherwise do and/or obtain insurance).

- d) Information leakage - where there is a contractual requirement for notification of a breach to a commercial partner, this can increase the risk of the incident entering into the public domain (e.g., due to a leak).
- e) Security attestations - it is now commonplace for commercial contracts to require suppliers to provide periodic security attestations, such as annual declarations and provision of certifications. If an incident is revealed through this process, it might trigger other contractual requirements, such as enhanced liability, or a requirement to implement additional controls, or a requirement to pay for further due diligence performed by the customer.

Generally speaking, there is usually little incentive for companies to engage in public disputes about contractual liabilities arising from cyber security breaches, but the conditions of a case can cause exceptions. Furthermore, if the Data Protection regulatory system and/or litigation environments mature in a way that fix organisations with increased liability, it would be possible for the B2B contracting environment to become more visibly contentious.

A potential factor in the risks of B2B litigation is insurance. If an insurer has significant exposure, it might be minded to use its subrogation rights to seek remedies against the insured's contracting partners.

² Note that for the purposes of assessing contractual risk, the idea of 'data' should be interpreted more broadly than under Data Protection law, so as to cover other forms of confidential information, such as trade secrets and other IP.

Corporate governance issues

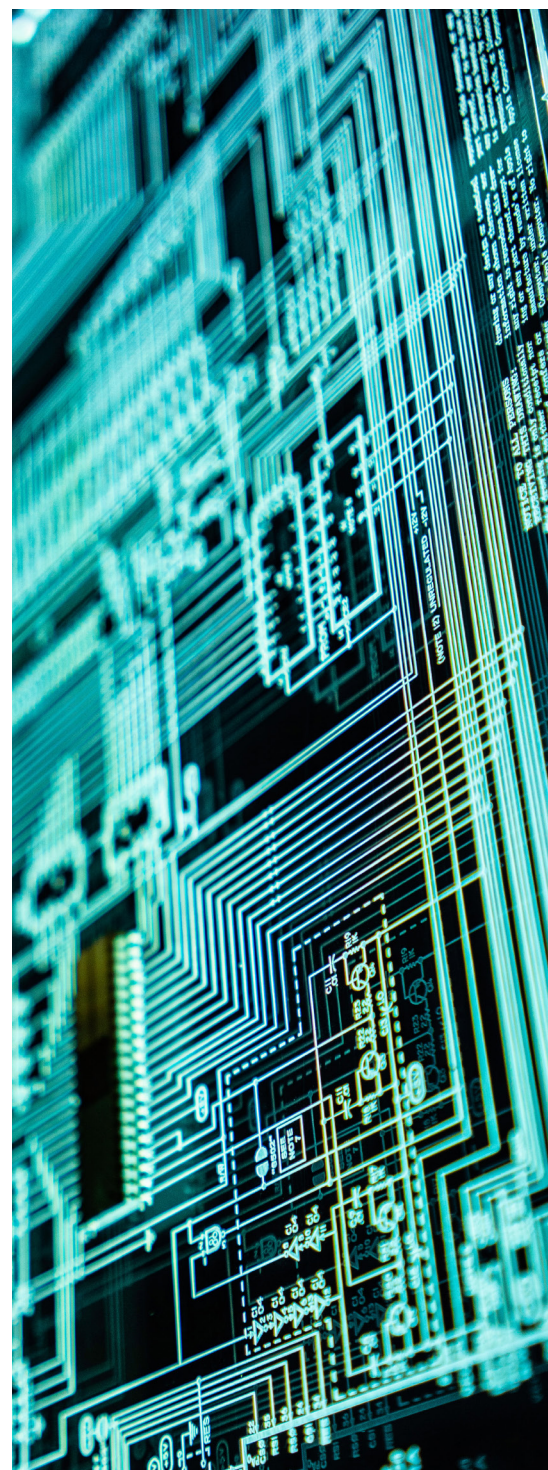
Cyber security involves various corporate governance issues, such as:

- a) Publicly listed companies may need to consider their disclosure obligations under listing rules, to understand whether a cyber security incident requires a RNS. For example, in September 2022 InterContinental Hotel Group³ made an announcement of their cyber security breach.
- b) The audit requirements under the **Corporate Governance Code**⁴ have been interpreted for a number of years now as requiring cyber security audits, as do other elements of the Companies Act. These audits regularly operate as 'smoking guns' in regulatory investigations if they are suggestive of unclosed audit findings being part of the root cause of the incident.
- c) The Companies Act places various duties on company directors regarding the performance of their duties. These have been widely interpreted as requiring appropriate awareness of cyber security issues and oversight of them.

Plainly, corporate governance requires an end-to-end focus on cyber security. Thus, there is a theoretical risk that a company and/or its directors might be said to have failed on corporate governance if the business suffers an avoidable security breach and/or it fails to respond appropriately to a breach (whether or not the breaches are avoidable). These are reasons to keep cyber security on the Board's agenda and to equip the Board with sufficient knowledge and understanding to enable them to present meaningful challenge to those with operational responsibilities.

At this juncture, DWF does not perceive that there is a high risk of companies/directors being held directly to account under corporate governance rules (not least, because there are other legal avenues for an account), but we do expect corporate governance topics and arguments to feature more prominently in the overall legal narrative as time progresses. For example, we can perceive how it would be strongly in the interests of a regulator, an activist, or a litigant, or the press to run arguments based around the elements of corporate governance identified above.

Security issues, particularly where personal data and privacy are potentially at risk, can also be regarded as potential ESG issues. Similarly, security is a matter of increasing concern for investors in business, thus it features as a key area of due diligence in corporate transactions.



³ <https://www.londonstockexchange.com/news-article/IHG/unauthorised-access-to-technology-systems/15617013>

⁴ https://www.frc.org.uk/getattachment/b23698f9-a587-4222-b32a-b947dd7b3300/FRC-Digital-Security-Risk-Disclosure_August-2022.pdf

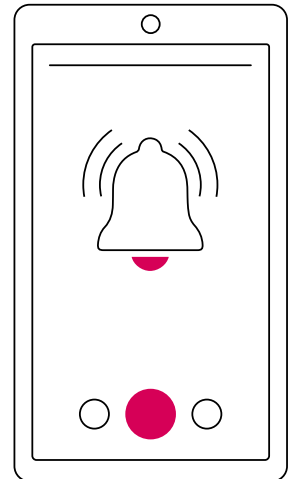
Insurance cover

Many businesses take advantage of cyber security insurance, although lots self-insure. A cyber security breach can have impacts for insurance cover in three ways:

- 1) If a breach occurs, it might reveal evidence of past material non-disclosures or misrepresentations, leading to a loss of cover;
- 2) It might make the process of obtaining insurance in the future unduly arduous, with coverage limitations, increased premiums and increased deductibles; and

- 3) It might make a company uninsurable in the future.

Insurance contracts require a fair presentation of risk and updates on material issues to be provided promptly, which involves early notification of incidents if there is to be a claim on cover, or insurance renewals.



Ransomware attacks

A ransomware attack, or any other attack that involves an organisation succumbing to extortion, requires specialised handling.

This is because payments of ransoms can result in infringement of sanctions and anti-terror legislation if money is paid to a sanctioned/proscribed entity. In that case, serious criminal offences and civil contraventions would be committed.

There are pathways that can be followed to avoid these risks, enabling the payment of a ransom to be an option. However, these pathways do not eliminate all legal risks and, moreover, it is easy for organisations to misstep due to inadequate processes or incomplete advice.



Globalisation of legal risks

The analysis above focuses on the UK, principally from the perspectives of English and Welsh law.

Multi-national companies and UK-only businesses that offer their goods and services abroad need to consider the legal risks from a broader perspective, including to understand nuances in national laws and the situations where the legal requirements are more stringent and the risks are greater.

For example:

- a) DP law under the EU GDPR is now on a different path to the UK. Fines are rising at a faster pace in the EU and they are being imposed with greater frequency.
- b) The UK and the EU are now divergent on critical infrastructure cyber security rules: many more sectors and entities are brought within EU cyber security rules than under UK law. Cyber security rules for the financial services sector differ also.
- c) Litigation risks and regulatory risks are significantly more enhanced in the USA in contrast to the UK.
- d) The US expectations of director duties and other corporate governance issues are evolving at a quicker pace than in the UK.
- e) New legislation seems to be emerging everywhere.
- f) Privilege rules differ from country to country, so what might be perceived as privileged in the UK may not be protected elsewhere.

The international consequences of decisions made nationally in one country need to be thought through.

Secondary legal risks resulting from the manner of Incident Response itself

In the 'heat of the moment', many organisations overlook the fact that the steps that they need to take for Incident Response can themselves generate legal risks.

Typical problem areas include:

1. A ransomware attack might disable systems, or raise concerns about ongoing reconnaissance by the Threat Actor, causing the organisation to adopt temporary 'out of band' communications systems. The adoption of any temporary systems needs to be risk-assessed. For example, if a temporary system is used to process personal data, it will fall within the parameters of Article 25 of the GDPR, which contains express requirements for risk assessments to be performed prior to the adoption of the system.
2. Various suppliers might be engaged to provide discrete services. Care and attention is needed during procurement and agreement of the terms and conditions and the scope of work, for the reasons referred to or alluded to above.
3. Many types of breaches can bring personnel under suspicion and/or require investigations to be carried out that impact their fundamental rights or their employment law rights. General procedures for legal hygiene should be adhered to.

Strategic and tactical considerations for contentious legal business

Regulator risks, Data Subject risks, litigation risks and breach of contract risks can all be grouped together as actual or potential contentious legal business.

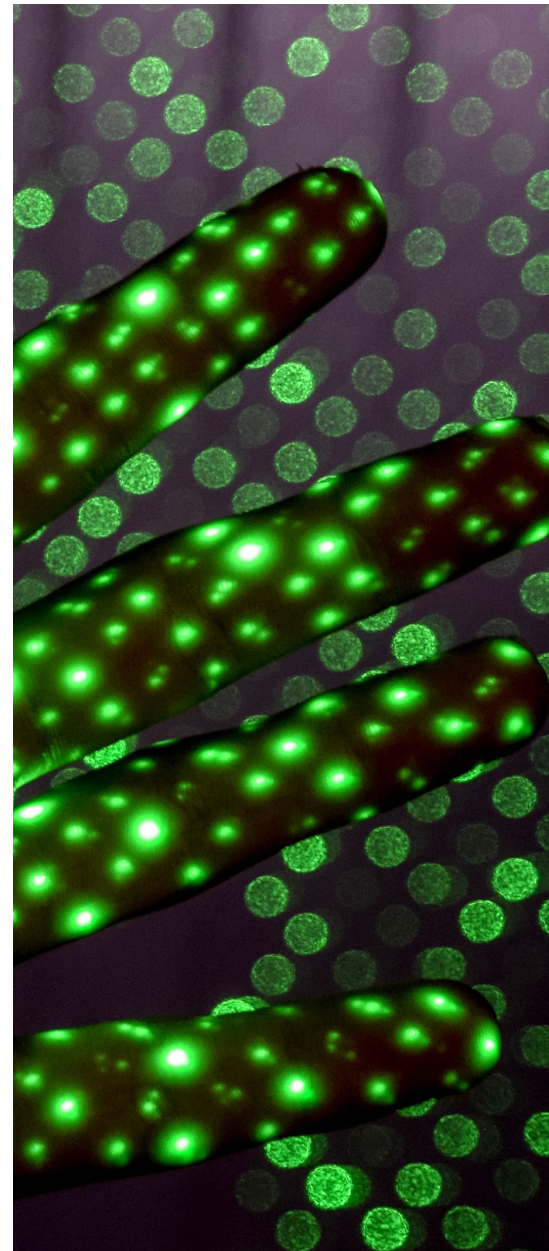
In these contentious business situations the critical issues that need to be addressed as part of risk mitigation include maintenance of audit trails; evidence preservation; contents of communications/documents; maintenance of secrecy and confidentiality; and establishment of legal professional privilege.

The areas of tactical focus that are relevant to risk mitigation include:

- a) Roles and responsibilities for issuing instructions to third party experts and the manner and mechanisms for receipt of deliverables.
- b) Roles and responsibilities for issuing and dealing with in-bound communications, content reviews and copy clearance.
- c) Roles and responsibilities for generating internal reports.
- d) Distribution lists for reports, communications and documentation.
- e) The maintenance of the incident log.
- f) The use of protective marking schemes.
- g) The conduct of correspondence with regulators, Data Subjects, claimants, contracting parties and other potentially adverse parties.

While the range of potential legal exposures that can arise from a cyber security breach are relatively easy to identify and list, the extent of actual exposures turns on the nature of the legal contravention/breach, the quality of Incident Response and, most acutely, the quality of the organisation's thinking and approach to handling actual or potential contentious business.

In other words, it is DWF's experience and advice to clients that legal risk can be very substantially mitigated by integrating sophisticated contentious business thinking into all elements of Incident Response and its aftermath.



About DWF's Data Protection and Cyber Security practice

DWF's Data Protection and Cyber Security practice is rated as one of the UK's leading practices by the main legal directories.

We are renowned for our Incident Response services, our experience in handling regulatory investigations and our leading position as one of the main security breach 'class action' defence teams. Our insurance teams handle compensation claims on a daily basis. We also provide cyber security and Incident Response management consultancy services.

We are providing our clients with a range of complimentary value-add services including:



Ransomware and Data Extortion training;



RAPID Incident Response Readiness assessments;



Security breach retainer letters;



Incident Response Playbooks for General Counsel.

Please make contact with any member of our team if you would like to take advantage of these offers.



Contact **DPCS@dwf.law** for more information





DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients.

We deliver integrated legal and business services on a global scale through our three offerings; Legal Advisory, Mindcrest and Connected Services, across our eight key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com