# CRISIS CONTENDERS

Global
Legal Briefings – By **Daniel Hudson, Partner**, **Andrew Moir, Partner**, **Howard Watson, Partner** and **Stephane Brabant, Partner**

Significant adverse events are ever present in the corporate landscape – think environmental disasters, rogue traders and fake emissions reports – so there's little doubt they'll continue throughout 2016.

Top contenders as the source of major stories in the year ahead are likely to be terrorism risks to personnel safety and economic terrorism through cyber security breaches. These risks alongside political instability and economic volatility or uncertainty are likely to be features of the risk landscape for 2016 and should form key pillars of corporate risk management planning.

Preventive measures can minimise the likelihood of your organisation being caught up in a crisis stemming from these and other trends. But if events make it through your defences, making sure that employees, directors and officers know how to respond in the immediate aftermath can have a significant impact on the legal consequences that follow.

"The demands of the 24-hour news cycle, for example, mean senior figures in your organisation may feel compelled to step into the spotlight to try to explain and inform, but this is not necessarily the right course of action," advises Andrew Procter, who co-leads the crisis prevention and management practice at Herbert Smith Freehills. "Sometimes stepping back, locking down and taking good advice is the best way to limit the damage."

The best crisis management does not begin on the day a crisis breaks, but months and even years in advance. Thinking ahead about how your organisation would respond in a range of plausible scenarios and rehearsing your practical response can significantly improve your ability to manage a crisis. For example, key personnel must be trained in incident response and integration among internal and external stakeholders must be seamless.

Equally important is maintaining focus on implementing your crisis management strategy effectively as a crisis evolves.

“In the event of a crisis, there are some fundamentals to remember,” says Anna Sutherland, who co-leads the crisis prevention and management practice. “The first rule in a crisis is to ensure your immediate response plan doesn't make the situation worse. It is key to identify your stakeholders, contact your insurers… What organisations often forget is that, as time passes, it’s easy for the team managing the crisis to slip back into default, business-as-usual decision-making. We recommend encouraging the team to hit the pause button and take stock regularly. This can provide an opportunity to check that the response strategy is still relevant and to keep everyone focused on the end goal.”

**Be prepared for the unpredictable and be ready to implement your plans professionally**. Are you ready to respond to the risks scattered across the evolving corporate landscape? We explore some of the major threats facing organisations in the year ahead.

## THE FIRST CONVICTION OF A COMPANY UNDER THE UK BRIBERY ACT

As governments and law enforcement agencies increase their focus on corporate economic crime, the UK, which already saw the first convictions of individuals, witnessed its first conviction of a corporate under the Bribery Act 2010. Section 7 of the Act makes it an offence for a corporation to fail to stop bribery taking place on its behalf.

The Act, although part of UK legislation, has implications for companies internationally.

Daniel Hudson, one of our partners specialising in anti-bribery and corruption, advises: “If your organisation has a presence in the UK, you must adhere to the Act’s requirements. You should be particularly alert when making commercial arrangements with companies in jurisdictions where bribery and corruption laws may be non-existent.”

In these situations, the right contracts can safeguard your company’s position and reputation to some extent. Critically, contracts should include clauses requiring individuals such as directors and employees not to engage in corrupt activity.

## MORE DEFERRED PROSECUTION AGREEMENTS

In November 2015, the UK’s Serious Fraud Office announced that it had entered into its first deferred prosecution (DPA), in this instance in relation to a bribery case with a division of ICBC Standard Bank, and we anticipate more DPAs in 2016. DPAs are a relatively new instrument conceived to help law enforcement agencies deal with corporate economic crime. Legal proceedings against a company are suspended provided the company agrees to meet certain conditions. This process will often make it easier for the prosecutor to untangle the web of information, connections and money that typically lies at the heart of fraud, tax evasion and bribery cases.

“From a crisis management perspective, a DPA can benefit the company involved as well as the prosecutor,” says Daniel. “By agreeing to co-operate with the prosecutor, as well as receiving credit when it comes to punishment, the company can mitigate negative press coverage and present itself as a ‘good’ organisation, seeking to put matters right as quickly as possible.”

This, of course, should be more than a public relations exercise. Organisations subject to fraud and bribery investigations must undertake a thorough review of their procedures in order to prevent further incidents.

## MORE SECURITY BREACHES

The frequency and severity of hacking incidents has been growing steadily in recent years. In 2015, the FBI, Ashley Madison, TalkTalk and several US financial institutions were among the high-profile names to suffer at the hands of hackers. In 2016, this trend is set to continue.

“Opportunities for cyber criminals will grow as organisations move more data into the digital domain and offer more services through digital channels in order to meet consumer expectations,” explains Andrew Moir, Global Head of Cyber & Data Security for Herbert Smith Freehills. “As a result, for most businesses, a hacking attempt is effectively no longer a matter of ‘if’ but ‘when’.”

The financial impact of a data breach can be enormous – the TalkTalk data loss, for example, is estimated to have cost the business up to £60 million so far. This means implementing robust security and policies to try to prevent an attack in the first place is by far the wisest and most cost-effective course of action. In addition, pre-crisis scenario planning will position your organisation to respond quickly and decisively in the event of a successful attack.

“The growing nature of the cyber threat means you should also start extending your focus out beyond your own defences to consider how you might be exposed through your supply chain” advises Andrew. “Do the parties you are contracting with have their own cyber security under control?”

While contracts can be agreed to protect your organisation from liability for data loss caused by a third party, safeguarding your reputation must also be a cause of concern. In the event of a data loss, the source of the breach will be of little concern to consumers. It is the market-facing organisation that will suffer the reputational damage – another reason to put the emphasis on preventing data loss ever occurring.

## TOUGHENING REGULATION AROUND DATA PROTECTION

The growing cyber threat means the European Commission has been looking at how to improve member states' cyber security capabilities and co-operation on cyber security. A new directive, agreed at the end of 2015 and likely to come into force in 2017, introduces mandatory reporting of cyber security incidents in some circumstances, which will have wide-ranging impact. The directive had originally focused on ensuring the security of operators of essential services such as energy, water, telecoms and financial services. However, in its final form, it will extend to include providers of other digital service platforms, potentially catching a huge number of additional organisations in its net, depending on how member states choose to apply the directive.

On a related theme, new European General Data Protection Regulation is expected to be in force in Europe in 2018, with the aim of bringing the rules about how data can be stored and used into alignment across all member states. Among the features of the new regime is a significant increase in the maximum fine for losing data, with the likely fine being up to 4% of annual global revenue or €20 million – a further incentive, if any were needed, for organisations to ramp up data security.

## HIGHER FINES FOR HEALTH AND SAFETY OFFENCES

At the end of 2015, the Sentencing Council in the UK published new sentencing guidelines covering corporate manslaughter and health and safety offences. Under the new guidance, fines vary according to the size of the organisation involved, but large organisations in particular will face a significant increase. For example, an organisation with a turnover in excess of £50 million, convicted of a health and safety offence or corporate manslaughter in a fatality, can now expect a fine in the millions.

How well your organisation is set up to deal with the crisis that inevitably follows a serious health and safety failure may have a profound impact on how you eventually fare in court.

"One of the most important things to do in the immediate aftermath of a health and safety incident is to carefully consider what aspects of your crisis response activities should attract legal privilege" explains Howard Watson, a partner who specialises in health and safety claims at Herbert Smith Freehills. "Simply writing 'privileged' at the top of emails is not enough. Legal privilege where appropriate should be evoked more formally."

## HUMAN RIGHTS VIOLATIONS AS A SOURCE OF RISK

Media coverage linking organisations with the violation of human rights is now commonplace. Stories of environmental disasters, the intervention of security forces in community protests, the use of child labour and even human slavery/trafficking in the supply chain are not unfamiliar on the front pages – and they will continue throughout 2016.

These links arise in a number of ways. An organisation may cause or contribute to a violation of human rights either directly, through its action (or omissions), or through its business relationships, supply chain or customers. Whatever the link, crises of this type are always very sudden. If they cannot be anticipated and prevented, they must be dealt with rapidly to stop them escalating and causing calamitous financial and reputational damage.

When organisations do come under scrutiny in respect of human rights, the judges are no longer only those seated in the courts. The 'new' judges are the NGOs, civil society, banks, international financial institutions and stock markets. Aside from any legal sanctions that the organisation may suffer, these institutions can apply equally powerful reputational, operational and financial 'sanctions' for human rights violations.

"To minimise the risk of reputational damage stemming from involvement in activities that might become controversial from a human rights perspective, companies and their legal advisers must take the broadest possible view of how to protect the company's position right from the outset" says Stephane Brabant, who leads on business and human rights for Herbert Smith Freehills. "Where a crisis threatening reputational damage does occur, solutions need to be fast, pragmatic and effective. Attempting to resolve disagreements through conventional channels, such as the courts, can often amplify grievances and compound the damage."

## A CHANGING ROLE FOR LAWYERS

The issues around business and human rights perfectly illustrate the changing role of the lawyer in crisis prevention and management. The best lawyers will ensure their clients comply with the law on issues including health and safety, environmental protection and working conditions. In order to minimise the risk of crisis, they will go beyond the letter of the law and consider internationally recognised human rights in drafting contracts.

When a crisis does occur, outstanding lawyers will step up not only as technical lawyers but as trusted legal advisers. They will be able to counsel on the legal consequences of events and provide pragmatic advice on the right action to take in fast-moving situations where the stakes are high. We're certain that's the type of lawyer you'd like to have at your side.

# KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.


**DANIEL HUDSON**
PARTNER, LONDON

+44 20 7466 2470
Daniel.Hudson@hsf.com

**ANDREW MOIR**
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

**HOWARD WATSON**
PARTNER, LONDON

+44 20 7466 2088
Howard.Watson@hsf.com


# LEGAL NOTICE