In April, we saw another large scale network security breach involving the uncovering of 11.5 million documents, referred to as the “Panama Papers”. The documents contained sensitive information on the creation of offshore entities on behalf of individuals, including high profile public figures. They were obtained by a hacker who exploited vulnerabilities in the Panamanian law firm’s computer systems.

There has been an international focus in recent years on tax havens with companies like Google and Starbucks coming under scrutiny for their tax arrangements. The breach therefore has ignited politically fuelled debates around public interest vs privacy and legality vs morality. The costs incurred by Mossack Fonseca, not only of dealing with the aftermath of the breach but also in potential liabilities and reputational damage, have the potential to be huge. This creates an excellent opportunity for contemplating how recoveries may have been possible under various insurance policies, most notably (given the nature of the event) under a cyber policy.

Many of the individuals whose files were disclosed are high profile public figures and celebrities. They presumably have the means to bring large professional negligence and privacy liability actions against the firm, which could make such actions more likely. A firm’s clients may allege that the firm was in breach of its duties and was negligent in allowing their information to be compromised. Both a professional liability policy and the privacy liability module within a cyber policy could be triggered by those suits.

Similarly, regulatory investigations may trigger coverage under both professional liability and cyber policies.

The ‘Panama Papers’ have created an interesting angle, given the potential for involvement of the legislature in various territories, for example public inquiry in the UK or a congressional investigation in the US. Under a professional liability or cyber policy it’s worth thinking about whether the legislature would be deemed a regulator within the context of the insurance. Also, to what extent resultant fines and penalties may be recoverable. Professional liability policies will generally exclude coverage for those but most cyber policies will address this exposure, where insurable by law.

Questions have also been raised as to whether Mossack Fonseca were used to facilitate illicit activities. Although there is not yet any evidence of any of the uncovered activities being illegal, the firm and its staff may be exposed to allegations of misconduct and helping to facilitate illegalities. The Panama police reportedly searched the headquarters of Mossack Fonseca during a raid that lasted for over 8 hours and the US Department of Justice has confirmed that a criminal investigation has been opened into the legality of the various schemes. Under a professional liability or cyber policy criminal proceedings against the firm itself will be excluded but under a Directors’ & Officers’ policy recoveries could potentially be made for the costs of defending criminal proceedings against individual directors.
In addition to the possible liability and regulatory issues, the direct costs incurred by Mossack Fonseca after the leak was discovered will be considerable and could be recoverable under a cyber policy. In summary, a standard policy would provide for:

- Obtaining legal advice from a specialist data breach lawyer
- Engaging an IT forensic expert to investigate the cause and scope of the breach
- The costs associated with notifying the individual clients whose files had been exposed. A good quality cyber policy should extend to voluntary notification rather than just notification that is mandatory by law or regulation
- Offering credit monitoring services or ID theft protection to affected customers
- Setting up and operating a temporary call centre to deal with the inflow of client queries after notification and engaging a crisis management or public relations firm to help deal with the press and mitigate reputational damage

Cyber insurers not only provide a means of recovery for these costs but also provide access to a panel of service providers who are expert and experienced in the various breach response fields and who may be engaged at competitive, pre-agreed rates. This includes 24/7 access to a breach reporting hotline for immediate guidance from a specialist legal advisor.

Perhaps the most financially damaging effect of the ‘Panama Papers’ breach on Mossack Fonseca is the reputational harm that the firm may suffer as a direct consequence of the adverse media coverage. The breach has led to very public discussions on the morality of the work that Mossack Fonseca were carrying out. It has been suggested that high net worth individuals were using them to benefit from secrecy and discreet arrangements. It’s therefore easy to see how the data leak could have a dramatic effect on client trust and ultimately impact the firm’s client retention, revenues, and profits.

Reputational damage can be mitigated by the post-breach services provided by cyber insurers. Experience shows that those services can significantly reduce consequential losses to a business that has been affected by a breach, whether those losses arise from civil suit, regulatory actions or customer desertion.

There are also dedicated reputation harm insurances available which can be tailored to the individual needs of a firm like Mossack Fonseca. Those policies address the loss of net income triggered by adverse media activity following a defined reputational harm event, not necessarily limited to a privacy or security breach. The reputational harm event scenarios can be based on what the specific client deems relevant in their own commercial context. This may include perils such as data breach, disgrace of a celebrity endorsing products, senior executive/partner disgrace, environmental damage, product safety failure and food contamination.

To truly meet a firm’s needs, a dedicated reputation harm policy must be a bespoke product that is tailored to the firm’s business and risks. This requires a collaborative and consultative process with the insurance underwriters. Firms and companies interested in such a product should ensure that they are represented by a broker that has experience in this area.

Lucy Scott - Global Cyber & Technology
Tel: +44 (0)20 7933 2382
Mobile: +44 (0)75 0694 3276
E-mail: lucy.scott@uk.lockton.com