MANAGING CYBER RISK IN THE THIRD SECTOR

Liam Greene of Markel explains why cyber risks should be high on the risk management agenda of third sector organisations as incidents hit the headlines with increasing frequency.

Cyber risk can be grouped broadly into two types:

- Operational cyber risk concerns the risk to business continuity if organisations are denied their electronic systems.
- Information cyber risk arises as a result of the digitisation of data and information. Never before have organisations been able to hold and transfer so much data with such speed and ease. A significant part of information cyber risk relates to the growing legal regulations and sanctions associated with data.

It is important to note that neither operational nor information cyber risk are limited to hacking incidents. Exposure to such risks can arise from employee and software errors. Nowadays, virtually every organisation operates electronically in some way and therefore faces a cyber exposure; charities and not-for-profit organisations are not exempt from this trend.

The Information Commissioner's Office recently announced an investigation into claims that an 87-year-old man's personal details were sold or passed on by charities up to 200 times. Although many people might not consider this to be a "cyber" incident, because of the digitisation of data in the modern world, it is becoming increasingly difficult for organisations to keep track of the transfer speed and volume of individual data records.

Digital data therefore comes with increasing legal and reputational exposure. Commenting on this incident, the Prime Minister, David Cameron, said that some fundraisers were "damaging the reputation of the charity sector", and the ICO noted that the incident "suggests not only a disregard for the law, but also a disconnect with the supporters whose generosity they rely on".

Case study

The financial, reputational and legal exposures of digital data to charities were highlighted when the ICO fined the British Pregnancy Advice Service £200,000 on 28 February 2014. Like many charities, the BPAS held personal and sensitive data and information belonging to 9,900 people who had approached the charity for advice.

The BPAS was not aware it was storing the information, highlighting the difficulty that organisations face in tracking and controlling the information they process. Unfortunately, the data was stolen by a hacker activist who threatened to release the information.

The ICO found that the BPAS had failed to adopt appropriate technical and organisational measures to prevent the loss of the data. It was deemed unacceptable that the BPAS was unaware that personal data held was unprotected and, because of the nature of the data, it should have been afforded the highest standards of security. This example highlights just how easy it is for organisations to unwittingly collect digitised data and attract the associated risks.

Accordingly, organisations should ask themselves what they would do when and if they suffered a similar incident and should prepare accordingly. Despite the fine, the BPAS's actions were commended by the ICO. The BPAS voluntarily reported the incident and cooperated with the ICO, and it took steps to protect potentially affected data subjects.

Health & social care providers

Hans Allnutt, partner specialist at the solicitors DAC Beachcroft, explains that "further legal requirements for organisations providing or supporting health, public health and adult social care services arise out of the Health & Social Care Information Centre's checklist, published in May 2015".

This includes guidance for reporting, managing and investigating cyber security incidents requiring investigation (Cyber SIRIs) and information governance incidents (IG SIRIs). "Level 2" incidents must be reported to the Department of Health, the ICO and other regulators as soon as possible (usually within 24 hours of a breach being notified or identified locally).

Managing cyber risks

The operational, financial, legal and reputational exposures arising out of cyber risks are becoming clearer by the day, fuelled by publicity and a compensation culture around privacy.

Organisations should look into which preventive measures (risk management) measures they can use and how well equipped they are to react to an incident. At Markel we have recently enhanced our specialist cyber risks insurance cover to assist policyholders with the management of cyber risk. We now include immediate access to specialist legal and cyber experts in the event of a claim.

Alongside this, we have created a helpline that offers expert legal and technical IT security guidance on issues arising from cyber and data protection risks. Not all cyber risks can be anticipated or prevented, so an effective insurance policy will help charities, not-for-profit and care organisations to respond to cyber incidents and should form part of any risk transfer exercise.