UK

Nigel Parker Partner
nigel.parker@allenovery.com

Adam Smith Associate
adam.smith@allenovery.com

Allen & Overy LLP, London

Managing third party risks in cyber security

According to a recent survey conducted by the Department for Digital, Culture Media and Sport ('DCMS'), cyber security is viewed as an essential part of business management. With the proliferation of the Internet of Things ('IoT') and organisations outsourcing much of their cyber security protection, keeping track of third party activity can sometimes be problematic. With the coming into effect of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') earlier this year, priority into personal data management will undoubtedly change and tools and measures will also need to adapt to keep up-to-date with developments. Nigel Parker and Adam Smith, of Allen & Overy LLP, discuss the management of third party cyber security and the various remedial practices available.

The suggestion that cyber risk is a core business concern is no longer revelatory. The scale and range of threats originating from the connectivity of modern business processes and the rise in outsourcing, means an organisation that neglects cyber security, risks putting its future in jeopardy. According to a 2018 survey by the DCMS[1] ('the DCMS Report'), approximately four in ten businesses reported a cyber breach or attack in the preceding 12 months. Almost 40% of such incidents have resulted in financial or data loss.

In the same study, almost three quarters of directors, trustees and senior managers surveyed stated that cyber security is a high priority - and it is easy to understand why. Without implementing appropriate cyber security measures, businesses can compromise everything from their most important trade secrets to the welfare of the individuals they hold information about. While businesses are investing in cyber security risk management strategies and implementing measures intended to minimise exposure to cyber threats, most organisations focus on internal measures, ensuring that their computer systems have adopted up to date security measures, and that policies and procedures are introduced to make sure employees do not compromise data. While these measures do address certain major challenges for businesses, in reality, many of the organisation's biggest vulnerabilities lie outside the gates, namely with the third parties with whom data has been shared.

To state the obvious, mitigating cyber security risks with regard to data held or otherwise processed by business partners, service providers and other third parties is far more difficult than addressing internal compliance issues. As soon an organisation shares data with a third party, it loses full control of that data. It becomes reliant not only on its own measures but on those taken by the recipient, who may have a different risk profile and different threats to contend with. As a result, there is only so far that an organisation can go in mitigating third party risks. However, there are steps that can be taken to ensure that data is safeguarded when shared externally.

Dealing with third parties

Organisations continue to grow more reliant on data, resulting in vast arrays of commercially important information being exchanged between organisations and service providers of varying sizes and sophistication. Outsourcing and the rise of cloud-based third party applications and other online platform-based resources, means many organisations may struggle to keep track of all recipients of their data and the reasons for disclosure. This can be particularly difficult in large organisations where a number of different teams share different types of data with other companies.

In recent years, many organisations have adopted cloud computing services, often solely to outsource data storage. While the cost and resource benefits over maintaining internal capability are clear, moves to transfer data to the servers of service providers result in the organisation's data set becoming 'one of many' on shared servers, with availability and security determined by the cloud service provider. In the DCMS Report, businesses that used cloud computing were found to be 9% more likely to have encountered a breach (52% versus 42% overall). Although a number of companies operate within the cloud computing sector and have the resources to implement state of the art security measures, their scale and profile arguably make them priority targets for hackers.

As well as common service providers, organisations will occasionally need to share data with professional advisors such as law firms, accountants and management consultants, who will likely receive the organisation's most sensitive data. Again, this will mean that while they

continued

should be implementing strong cyber security measures, they will also be among cyber criminals' major targets.

The proliferation of the IoT and smart devices further complicates matters, potentially creating scenarios in which data is collected and transmitted to service providers without such transmission being obvious to employees. A more pressing issue, with respect to IoT devices, lies in the connected nature of the products and the fact that many devices may not offer the requisite level of protection from cyber security threats. Potentially, such devices offer cyber criminals a way into corporate networks, which in turn potentially allows the exfiltration of sensitive information.

It is important that organisations appreciate the level of priority each service provider gives to cyber security. They may not always be aligned with the approach the organisation takes. For example, in order to run a service at a marginal profit level, a vendor may have taken the strategic decision to implement only the bare minimum of security measures required to comply with law or to meet market standards. These standards may fall below those required for the organisation according to its own policies, procedures and guidelines. Any compromise suffered by a third party engaged by the organisation, is likely to tarnish the organisation's own reputation for data security.

Risks from cyber security incidents

Recent focus on the entry into effect of the GDPR, puts the protection of personal information to the forefront of many organisational decisions on data. Cyber security incidents can impact a much wider range of valuable and sensitive data, however, the compromise of which can be damaging. In addition to personal data, organisations hold or generate information that can be valuable or sensitive, such as data relating to their intellectual property, know-how and trade secrets, information in respect of their commercial strategies and positions, and confidential and/or privileged documents provided by professional advisers. Where any of this data is affected by a cyber security incident, the organisation may face a number of risks, including:

- **Commercial**: depending on the nature of the cyber incident, denial of service or the exfiltration of information that is necessary for the commercial operations of the organisation, may prevent it from carrying on business as usual;
- **Competitive**: the exfiltration and subsequent disclosure of intellectual property or other sensitive commercial data could potentially erode competitive advantage, rendering worthless knowledge that has taken substantial time and effort to develop. This may be particularly hazardous in market sectors where organisations in other jurisdictions are able to produce products at greatly reduced cost, where innovation represents the organisation's key point of differentiation;
- **Legal and Regulatory**: depending on the nature of the data and the industry sector in which an organisation operates, cyber incidents may result in regulatory action. The biggest regulatory risks relate to personal data. The UK Information Commissioner's Office ('ICO') has previously fined organisations for the infringements of their service providers, and such fines may rise significantly under the GDPR, which allows regulators to levy fines of up to the higher of €20 million or 4% of the previous year's total worldwide turnover. In the financial services industry, the Financial Conduct Authority has the power to take action against financial institutions for their implementation of inadequate cyber security controls. Where individuals suffer damage as a result of a cyber security incident, they may take civil action against the organisations responsible. In circumstances where intellectual property is shared with or licensed from another organisation, civil legal proceedings may also result where relevant information is compromised;
- **Reputational**: involvement in a cyber incident can have a major impact on an organisation's reputation. At the very least, it calls into question the quality and integrity of the measures taken to safeguard data, while cyber attacks, such as that launched by Fancy Bears on the Team Sky cycling franchise, demonstrate how the publication of confidential and sensitive information by attackers and hacktivists may lead to questions regarding the broader ethics of an organisation. Where incidents affect personal data, the reputational damage can be heightened in an era where personal data has become a crucial asset for many businesses, especially where the harvesting of such data requires the confidence of the individual to whom it relates.

Key aspects of remediation

Tools and measures designed to counter cyber security risks are, by necessity, often reactive in nature. They are designed to counter known threats, yet the continuing advancement

Image: Hal Gatewood / Unsplash.com

Tools and measures designed to counter cyber security risks are, by necessity, often reactive in nature. They are designed to counter known threats, yet the continuing advancement of information technology and cyber criminals' ability to harness that new technology means that they are always one step ahead.

1. UK Government Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey 2018: Statistical Release (2018).

of information technology and cyber criminals' ability to harness that new technology means that they are always one step ahead. In turn, this means that it is not possible to completely eradicate cyber risks. It is even harder adequately to mitigate the risks posed by the vulnerabilities of third party data recipients.

That said, there are a number of measures that organisations can implement to minimise the risks that exist. These include:

- **Assess internal security measures**: vulnerabilities in vendor devices or systems may provide a pathway through which hackers and cyber criminals will look to exploit vulnerabilities in vendors' systems to access the organisation's own network. Investment in cyber security tools and measures is necessary to minimise the risk of damage from such attacks. Up-to-date software should be maintained to ensure that the most recent anti-virus and other security tools are applied to the organisation's own system.
- **Establish data flows to recipients**: it is important to establish precisely which third parties are holding the organisation's data and what data they hold. Where processes and procedures in respect of cyber security and third party arrangements are not already in place, this may necessitate a project to update contractual arrangements to address cyber security.
- **Develop due diligence procedure and document results**: where vendors rely on the organisation's data in order to perform services, they should be subjected to due diligence procedures in order for the organisation to get comfortable with the level of protection afforded to data. This will allow the organisation to establish a risk profile that considers the vulnerabilities, the type and sensitivity of the data provided, and the assessed level of security provided.
- **Ensure contractual protections**: in respect of third party management, the service contract is perhaps the main tool an organisation has to address cyber security concerns. Through the contract, an organisation can seek to impose its own security standards on its vendors, require notifications of security breaches and cooperation in these circumstances, limit the use of data and require its destruction, and allocate liability. Where a vendor operates as a data processor in respect of personal data, certain contractual clauses will need to be included as a matter of law. Existing contracts should be reviewed for cyber security concerns and may require refreshing in order to provide sufficient protections. Where other third parties receive data, the organisation should look to secure reassurances that adequate security measures will be implemented.
- **Build cyber security into internal procedures for third party management**: organisations should consider how relationships with third parties are managed where the relationship requires them to disclose data. Ideally, organisations should have guidelines in place for third party relationships that address cyber security, and the ability to enter into arrangements should be limited to certain employees whose signoff is required. Such individuals should receive training on the issue.
- **Monitor and review third party compliance**: ideally, the organisation should have authority contractual right to require audits in order to monitor compliance with cyber security standards periodically. This is necessary so that vulnerabilities and other problems can be flagged and solutions can be developed to the satisfaction of the organisation. Even where auditing is not addressed in the contract, the organisation may seek to audit a vendor prior to renewing commercial terms. More broadly, where large volumes of data or sensitive data (i.e. personal data or commercially important data) are handled by particular third parties, their general compliance should be monitored, for example by reviewing media reports.
- **Plan PR responses**: consumers and the general public are increasingly sensitive to cyber security risks and involvement in a cyber security incident may compromise its reputation. Organisations should assume that a cyber security incident will at some point affect them, and should plan the public relations response to ensure that reputational damage is minimised.
- **Take out insurance**: cyber risk insurance policies are increasingly popular tools for addressing cyber security threats. Most policies not only protect against financial loss but provide full professional support in the immediate aftermath of an attack, often before the organisation has the opportunity to assemble an external response team.

Remediation programmes encompassing the above measures may not fully eradicate risks, but they certainly strengthen protections, and will serve to mitigate any enforcement action from regulatory authorities, as well as minimising reputational damage.