LEWIS SILKIN

Data breach and cyber attack in the EU: the insurance factor

Introduction

Dr. Nathalie Moreno, considers the risks associated with some of the new data security requirements and examines the role of insurance cover in managing the risks posed by potential data breaches and cyber attacks

Data breaches and cyber attacks are now part of the new norm any organisation needs to contend with in an evermore interconnected world. It is therefore no surprise that businesses increasingly have turned to cyber liability insurance to protect and mitigate exposure to such risks. Interestingly, the Aon Global Risk Management Survey 2015 identified cyber risk as a severe risk for organisations of all sizes and, according to Pricewaterhouse Coopers, some 117,000 cyber-attacks were anticipated each day in 2015. The Aon survey cites the Washington think tank, the Center for Strategic and International Studies which claimed that the estimated annual cost of cyber crime to the world economy is US$ 445 billion (almost 1% of global income), not including the intangible damages to an organisation.

While there is no panacea or magic wand to prevent unavoidable business disruption caused by such borderless and unpredictable incidents, the combination of a sound and effective data compliance framework and appropriate insurance coverage are the two main defences against data security risks.

EU organisations are given useful guidance on data risk management in both the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive). In particular, the GDPR sets out new rules in relation to data management and security control and the NIS Directive helpfully recommends appropriate steps to manage security risks. Both pieces of legislation come into force from May 2018 and require mandatory notification of data breaches or incidents to the relevant national competent authority; albeit the 'authority' may be different under each piece of legislation depending on the nature of the incident.

For many businesses, the question is whether their current general liability policy caters for such incidents or if they should obtain policies that specifically insure against data breach claims.

In this article, we analyse the new data security requirements under the GDPR and the NIS directive and evaluate the role that insurance can play as an effective risk mitigation tool.

Data security requirements under GDPR and the NIS Directive

In the European Union, the Data Protection Directive (Directive 95/46/ EC) set out well known principles in relation to data security which organisations have now learned to live with. These include the obligation for data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Except for Germany and the Netherlands, EU data protection laws do not mandate an organisation to inform its national Data Protection Authority (DPA) if a personal data breach occurs. However, under Directive 2002/58/EC on Privacy and electronic Communications,otherwise known as the E-Privacy Directive, EU providers of electronic communication services are legally required to report cyber breaches to their national DPA within 24 hours, or face a fine.

Other sector regulations may affect the security requirements for certain industries. For example, in the UK, organisations regulated by the Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) are required to comply with the data security obligations set out in the Financial Services and Markets Act 2000 (FSMA) in addition to those in the Data Protection Act 1998. FSMA says that organisations must have in place adequate systems and controls to monitor, detect and prevent financial crime and in the case of a breach, organisations are required to notify the FCA and PRA under Chapter 15 of the Supervision Manual.

Under the current EU data protection regime, the level of fines and sanctions has failed to be deterrent enough to create a general culture of compliance. For instance, on 5 October 2016, the Information Commissioner's Office (ICO), the UK DPA, issued its largest fine to date, landing Talk Talk Telecom Group Plc with a record breaking £400,000 fine for security failings which allowed a cyber-attacker to access customer data. However, the total cost of the data breach to the company, taking into account the reported loss of new customers and exceptional costs, was reported to

be in the region of £42 million.

In France, the CNIL, which is the French DPA, issued its highest fine of €150,000 against Google in January 2014 for reaches of French data protection law and has an ongoing dispute over the right to be forgotten which could see Google faced with an additional fine of €300,000 for non-compliance. Spain also imposed its maximum fine of €900,000 on Google for the same breaches in December 2013. Germany saw its highest data breach fine issued in December 2014 by the regional DPA of Rhineland- Palatinate which imposed a record fine of €1.3m on insurance group Debeka Krankenversicherungsverein a.G.

Rules under the GDPR

The GDPR was adopted by the European Parliament on 27 April 2016 and will come into force on 25 May 2018 to implement its principles into their national laws. With its introduction, EU businesses will need to contend with extended data security requirements and sanctions not only for data controllers but also for data processors.

This is a major new feature of the GDPR which requires, on one hand, data controllers to only mandate those processors that provide "sufficient guarantees to implement appropriate technical and organisational measures" in order to meet the GDPR's requirements and protect data subjects' rights, and on the other hand, requires data processors to comply with the measures set out by Article 32, which identify the GDPR's "security of processing" standards. Article 32 of the GDPR requires both data controllers and data processors to assess the appropriate security measures in light of the identified risks, the context and purposes of the processing as well as the potential risk for the rights and freedoms of individuals. By way of guidance, it lists the following as 'appropriate security measures':

- pseudonymisation and encryption;
- ability to ensure confidentiality, integrity, availability and resilience of processing systems and services;
- ability to restore availability and access to personal data in a timely manner in the event of an incident; and
- the regular testing and evaluating of technical and organisational measures for ensuring security of data processing.

Both protections are required to ensure that anyone accessing personal data under their authority does so only under their instructions. Compliance may be demonstrated by adherence to newly introduced mechanisms such as an approved code of conduct or a certification mechanism.

In order to force businesses to take a more pro-active approach to data security, the GDPR introduces a general data breach reporting obligation requiring businesses in all sectors to inform the competent DPA and, in certain cases, affected data subjects.

The GDPR requires the data controller to notify the relevant DPA within 72 hours of becoming aware of such breach (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons). Notification under the GDPR must include details of the nature of the breach, the number of data subjects and data records concerned, likely consequences, the contact details of the data protection officer and how the data controller proposes to deal with the breach, including, where appropriate, measures to mitigate its potential adverse effects. Any delay in reporting must be explained and the data controller must keep a record of the data breaches and the actions taken in relation to them.

If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, such as discrimination, identity theft or fraud, financial loss, breach of pseudonimity, damage to reputation, loss of confidentiality or any other significant economic or social disadvantage, the controller must also communicate the personal data breach to the data subject without undue delay. The communication should be in clear and plain language describing the nature of the personal data breach.

Businesses will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. Information security measures should be re-assessed to ensure that data breaches can be detected and managed promptly. Businesses should also consider implementing measures to ensure that any data that are subject to a breach are unintelligible to any person who is not authorised to access them (e.g. by encrypting data wherever possible), as this may exempt the business from the obligation to report the breach to the affected data subjects, and may help prevent harm to the business's reputation. Indeed, these notification requirements mean that companies' misdemeanours can no longer go under the radar and public awareness of failings to protect data adequately will be raised meaning increased reputational risk for companies.

Finally, non compliance under the GDPR will not only attract regulatory scrutiny, cause reputation damage and potentially loss of business, but also financial penalties. In line with current anti-bribery and anti-trust laws, sanctions for breaches could represent up to 2% of annual global turnover or €10 million, whichever is higher, and in the case of serious breaches, up to €20 million or 4% of annual global turnover for the preceding financial year, whichever is the greater.

Rules under the NIS Directive

The NIS Directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. EU/EEA member states have been granted 21 months until May 2018 to implement its principles into their national laws.

As part of the cyber security strategy for the European Union, member states are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. They will need to establish a national competent authority for information security and set up a computer emergency response team (CERT) that will be responsible for handling incidents and risks.

The NIS Directive and the GDPR are actually two complementary EU legislations which constitute the new EU security breach regime. They both have significant overlaps in so far as they require the implementation of risk -based security measures and they mandate notification in the case of incident. Moreover, they both have some extra-territorial effect as they apply to EU organisations as well as organisations which are established outside the EU but which offer

services within the EU.

However, they differ in the type of organisations targeted, the nature of breach and the types of incidents involved.

Unlike the GDPR, the NIS Directive only applies to two types of organisation: (1) operators of essential services such as banking, health, energy and transport and (2) digital service providers with 50 or more employees and an annual balance sheet turnover of over €10 million, As part of the cyber security strategy for the European Union, member states are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. They will need to establish a national competent authority for information security and set up a computer emergency response team (CERT) that will be responsible for handling incidents and risks.

The NIS Directive and the GDPR are actually two complementary EU legislations which constitute the new EU security breach regime. They both have significant overlaps in so far as they require the implementation of risk -based security measures and they mandate notification in the case of incident. Moreover, they both have some extra-territorial effect as they apply to EU organisations as well as organisations which are established outside the EU but which offer services within the EU.

However, they differ in the type of organisations targeted, the nature of breach and the types of incidents involved.

Unlike the GDPR, the NIS Directive only applies to two types of organisation: (1) operators of essential services such as banking, health, energy and transport and (2) digital service providers with 50 or more employees and an annual balance sheet turnover of over €10 million, e.g. an online marketplace, an online search engine or a cloud services provider.

In terms of scope, while the GDPR focuses solely on the protection of personal data, the NIS only tackles network security. The NIS Directive requires both operators and digital service providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their networks and to the information services which they use to deliver their networks.

They are also required to take appropriate measures to protect against the impact of any breakdown in the security of the network, with a view to ensuring continuity of service. In terms of breach notification requirements, the GDPR notification is only applicable where personal data are compromised. Instead, the NIS Directive introduces a reporting requirement which is unrelated to personal data and differs slightly between operators and digital provider breach claims.

On the one hand, operators of essential services must notify the CERT of incidents having a significant impact on the continuity of the service they supply. Notifications must be made without undue delay and must contain enough information to allow the competent authority or the CERT to determine any cross-border impact of the incident. In order to assess the nature of the incident, a number of factors will need to be considered including the number of affected users, the duration of the incident and the geographical impact of the incident. In case of a serious incident, the public may be informed of an incident by the competent authority or the CERT.

On the other hand, notification by digital service providers must include any incident having a substantial impact on the provision of a service that they affer in the EU and must be made without undue delay to the competent authorities. Such notification will have to include information to enable the competent authorities to determine the significance of any cross-border impact. Likewise, in order to assess the nature of the incident, a number of factors should be considered including the number of affected users, particularly those relying on the service to provide their own services, the duration of the incident, its geographical impact of the incident, the extent of the disruption to the service and the extent of the impact on economic and societal activities.

Under the NIS Directive, organisations are subject to administrative penalties if they fail to implement appropriate security measures or fail to notify the competent authorities of an incident.

They are only required to notify the competent authorities and not any data subjects who could be impacted by the breach. With respect to enforcement, member states will have the powers to legislate on penalties for non-compliance.

Although the GDPR and the NIS Directive provide different definitions of "appropriate technical and organisational measures", they aim to fulfil the same security objective. Organisations are required to undertake risk assessments and take all appropriate measures to prevent risk and mitigate any potential damage. In practice, it is expected that a majority of organisations will be subject to both the security and breach reporting requirements under the GDPR and the NIS Directive.

Clearly, the overlap between the two pieces of legislation could mean that organisations may face conflicting obligations, multiple notification requirements and liabilities in cases where an organisation has violated the provisions of both laws.

The penalties imposed on the one hand by the NIS Directive, which may include onerous administrative sanctions which are required to be "effective, proportionate and dissuasive" and on the other hand, by the GDPR which could be up to €20 million or 4% of annual global turnover for the preceding financial year, whichever is the greater, are a game changer for the insurance industry and its customers.

Will your general insurance policy cover cyber incidents?

It is widely accepted now that, alone, even the most sophisticated security infrastructure cannot entirely address the issue of cyber-attacks or breaches. In this context, boardrooms of companies of all sizes need to come to the realisation that insurance can play a vital role as part of their strategy to mitigate cyber risk.

As recommended by both the GDPR and the NIS Directive, any business' risk assessment should aim to get a thorough understanding of a company's insurance programme so as to maximise protection against cyber risk. As there are various types of cyber risks, it is advisable to consider first the adequacy of existing insurance policies held by the organisation, and then consider new insurance products which may be appropriate for the business, and acquire such new policies if needed.

For many companies contemplating the cost of specialist cyber insurance policies, the first question will be whether or not their existing general insurance policies will provide cover for cyber-attacks and data breaches in any event. In many cases, the wording of a general insurance policy may be considered by the policyholder to be drafted in such a way as to cover any damage that it may suffer from a cyber-attack or security breach. However, in the absence of specific wording referring to loss and damage caused by cyber-attacks and breaches, there is a serious question as to the extent to which insurance providers will be prepared to stretch their cover.

Whilst this question has yet to be played out in the European courts, there have been some recent US cases which have tested the wording under general commercial liability policies with regard to their applicability to cyber breach scenarios.

An unpublished opinion of the federal appeal court in Virginia (Travellers Indemnity Co. of America v. Portal Healthcare Solutions LLC, case number 14-1944 in the U.S. Court of Appeals for the Fourth Circuit) issued on 11 April 2016 has been widely heralded as a positive development for policyholders as it upheld a lower federal court in ruling that a commercial general liability policy may cover a data breach. The court found that the availability of data subjects' medical records online (due to the policyholder's failure to adequately secure its server) amounted to 'publication' and therefore fell within the scope of the personal or advertising injury provision of the policyholder's insurance cover.

This case was in contrast to some slightly earlier cases which seemed to swing more in the favour of the insurers. In the case of Recall Total Information Management Inc et al v. Federal Insurance Co. et al. (case number SC19291) a Connecticut appeals court found that a general commercial liability policy did not provide coverage for the loss of personal data (including social security number, birth dates and contact information) when tapes storing personal information fell out of the transportation contractor's van. The insured made a claim under a provision that defined personal injury as "injury, other than bodily injury,property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person's right to privacy" and the insurer denied that this covered the facts of the case claiming that there hadn't been any 'publication'. The court found that the policy did not cover the incident because, despite the theft of the information, there was no evidence that any of the information on the tapes was published. Although this case was good news for insurers, the case is very specific to the facts (and a very 'low tech' example of a data breach) and so would probably have limited application in other cases.

The final case of substance when considering this issue is the now settled dispute between Sony and its insurers, Zurich, over the liability for the PlayStation network cyber-attack which occurred in 2011 and saw hackers accessing the personal data of tens of millions of PlayStation users (Zurich American Insurance Co. v. Sony Corp. of America et al. case number 651982/2011 in the Supreme Court of t he State of New York). A New York trial court issued a bench ruling in January 2014 that the hacking did constitute a "publication" under a commercial general policy which covered "oral or written publication in any manner of [the] material that violates a person's right of privacy".

Though the trial court found that the hacking was a publication, it also found that for any publication to be covered by the policy, it had to be a publication by the insured itself meaning the act of the hackers wouldn't qualify. Sony appealed but the New York Supreme Court also found that Sony's insurance cover did not include the actions of third parties and therefore the acts of the hackers were not covered by the policy.

This is a particularly interesting case as it could potentially rule out cover for a cyber-attack where the policy requires the insured to publish the information as, by its very nature, a cyber-attack will be made by a third party.

These cases serve to highlight how the wording of any insurance policy should be carefully considered to determine whether or not it may be relied upon to offer adequate protection in a data breach scenario. Whilst there are certainly arguments to be made that general insurance policies held by businesses, such as professional indemnity insurance and directors and officers liability insurance may offer some cover for cyber-attacks, these issues are highly likely to be the subject of litigation in the coming years as the cost of cyber data breaches continue to rise and insurers push back on paying out.

Specialist cyber insurance – is it worthwhile?

In light of the forthcoming security obligations imposed by the GDPR and the NIS Directive, it is no surprise that organisations are increasingly considering taking out cyber-security insurance policies. Insurers may require precise standards of security and may be unable to provide cover if the organisation is not able to demonstrate a satisfactory security framework.

In terms of insurance coverage, a £5 million indemnity limit is usual in practice. However, it remains to be seen if the insurance industry will increase it to cover the potential €20 million fines that the GDPR will be able to impose from 2018 and potentially even higher fines under the NIS Directive. It is also worth noting that even if a policy is approved, it may not pay out if an incident was caused by failed controls, such as a defective firewall.

The Aon Global Risk Management Survey 2015 indicated that only 10% of European companies surveyed had purchased cyber insurance. Cyber (Liability) Insurance, also known as Data Breach insurance or Data Compromise Coverage (depending on the insurance company) generally provides protection against both first party losses and claims by third parties. Whilst policies will differ and few insurers have a standard format, insurance could cover:

First party losses – which could include:

- the cost of investigating the breach in order to identify how it occurred, how to repair the damage caused and how the business might go about preventing such a breach happening again in the future;
- the costs of notifying the regulator and data subjects;
- business losses caused by the breach;
- PR and legal fees incurred in trying to manage how the business responds to such a breach.

Third party liabilities including:

- possible compensation claims by individuals affected by the breach. In the UK Section 13 of the Data Protection Act 1998 (DPA) enables individuals to seek compensation in the event that they have suffered loss and damage as a result of a data breach. Following a 2015 Court of Appeal decision [Google Inc v Vidal-Hall and others [2015] EWCA Civ 311] compensation can now be claimed purely for distress, there is no need for any economic damage to have occurred. Where a data breach may involve large numbers of individuals this could result in a significant amount being paid to individual data subjects.
- possible tortuous claims for damages on the part of data subjects where their personal information has been misused.

Cyber insurance is a developing product and insurers have yet to adopt standard forms, therefore the terms of cyber policies are often the result of negotiations between the insurer and the policyholder.

When entering into any negotiations with an insurer it is imperative to have a clear understanding of the risks faced by your business and ensure that those risks are being insured.

One such example may be if there is a risk that a business may be exposed to a data breach by a malicious employee. Most insurance policies will contain an exclusion for the deliberate, intentional or criminal acts of the policyholder which may then include the acts of a disgruntled employee. Such wording would need to be carefully crafted to provide the intended protections.

Insurers will want to see detailed information from anyone applying for cyber insurance, including a full risk assessment of the possible risks faced by the business and the systems and operations that are in place to minimise those risks. Organisations may be required to provide information regarding prior data security incidents and specific information regarding its data security practices and many insurers require applicants to attach relevant company policies, including internal and external privacy and data use policies, network security and training policies, records and information management compliance policies and incident response plans.

The GDPR and the NIS Directive have simply transposed such requirement for comprehensive risk assessments into the obligation for organisations to conduct data protection audits and privacy impact assessments (PIAs) in many instances. Insurers may expect applicants to reduce or limit their breach risk through implementing encryption, engaging in security audits, deploying specific technical, administrative or other security enhancements.

Once coverage is in place, organisations must understand any conditions of coverage and the claims process. The coverage should also be periodically monitored and evaluated in light of business needs and the changing cyber insurance market.

The implementation of the GDPR and NIS Directive and the increased focus on cyber security is likely to have a big impact on the cyber insurance market in the EU and insurers will be responding to an increased demand for specific cover. They are yet to educate organisations on what their requirements are; such as getting the first call when a qualifying incident occurs so as to ensure that organisations may benefit fully from their insurance policies and develop trust with their insurers. Companies should be acting now to assess their cyber security, identify their risk areas and seriously consider putting in place specific insurance policies to protect against the seemingly ever increasing cost of data breaches.

This article was first published in PDP journals http://www.pdp.ie/journals

For further information on this subject please contact:

Dr Nathalie Moreno
Partner
T + 44 (0) 20 7074 8461
nathalie.moreno@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com