Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Managing cyber risk

A client guide
the Netherlands

Contents

Essential steps for effective management of cyber risk

In this guide, we outline:

The growing threat that data breaches pose to organisations across the world

The importance of being prepared for a data breach

The steps that need to be considered as soon as a data breach occurs

The importance of making the necessary notifications relating to the data breach

The key considerations in terms of the ongoing management of the data breach

The importance of mitigating loss by implementing a recovery strategy

The growing threat of data breaches

'Many companies are incurring significant damage, but often suffer in silence and are keen on keeping the information to themselves. In addition, the amount of the damages incurred is rising at an explosive rate. Therefore, cyber criminality starts to effect the true economy and can negatively impact our growth and welfare.'

State Secretary Klaas Dijkhoff, Dutch Financial Times, April 11, 2015

'Cyber attacks are often carried out by countries in pursuit of intellectual property and confidential corporate information, such as blue prints of products. Such online criminal actions are nowadays carried out with such frequency that they are sure to cost Dutch companies money.'

Dutch Financial Times, June 2, 2014

'Companies and supervisory authorities around the globe must put more rigorous safeguards in place against a possible large scale cyber attack. According to Greg Medcraft, chairman of the overarching organisation of supervisory authorities Iosco, the next big financial shock will be caused by a cyber attack.'

Dutch Financial Times, August 26, 2014

Although data breaches are often considered against the backdrop of cyber crime, the scope of data breach risk is actually much broader, ranging from a sophisticated hacking of credit card details held by an online retailer to the consequences of an employee losing a laptop containing personal data belonging to third parties.

The fact is that electronic information has become one of the most valuable assets held by organisations. However, there are many ways in which the confidentiality, integrity or availability of electronic information can be compromised.

Awareness of the risk

These cyber incidents are posing an increasing threat to organisations across the globe, which are slowly coming to realise that cyber risk is a serious issue. In 2015, a global risk management survey found that global public and private companies considered cyber risk to be in their top ten concerns, placing it ahead of property damage, disruption of supply chain failure and directors and officers liability.

Data breaches, where personal data belonging to other individuals or organisations is compromised in some way, are among the most serious forms of cyber incident.

Multinationals and governmental organisations hold a vast quantity of personal data which, if it fell into the wrong hands, could cause serious harm, including considerable financial loss and distress to those whose data has been improperly accessed. This leaves organisations exposed to significant claims by the individuals affected.

Legal and regulatory developments

The protection of personal data has also become a high priority for lawmakers and regulators. From a European perspective, the proposed General Data Protection Regulation is a piece of draft EU legislation which seeks to harmonise data protection laws across the EU. Under this regulation, which is scheduled to take effect in 2016, organisations that control or process personal data within the EU may be fined as much as €1 million or two per cent of the organisation's global annual turnover (whichever is greater), if they suffer a data breach. In addition, the reputational and public relations damage and related financial consequences which a data breach can cause an organisation cannot be underestimated.

From a Dutch perspective, there will be a notification obligation of data breaches as of January 1, 2016. Under this obligation, a notification is required to the Dutch data protection authority if a breach results in a loss of personal data and such loss is likely to have a negative impact on the privacy of the person involved.

It should also be remembered that data breaches do not only affect large organisations with deep pockets. A recent survey found that over 72 per cent of all data breaches occurred in small and medium-sized organisations, many of which cannot afford the regulatory consequences, third-party claims and reputational damage that can arise out of a data breach.

Managing risk through cyber insurance

Conventional types of insurance, such as crime, civil liability, property or business interruption insurance, often do not cover the risks which are inherent in an organisation holding or using electronic information.

Cyber insurance essentially covers losses and/or liabilities that arise out of unauthorised access to, or use of, an organisation's electronic information, or the destruction or loss of that information. Although not all fines and penalties which may arise out of a data breach are insurable, cyber insurance can still offer cover for many of the losses and costs which a data breach can cause.

The cover offered by a particular policy can encompass diverse situations, from a sophisticated hacking to a lost laptop containing personal data belonging to third parties.

Stage 1 | planning for a data breach

'Fail to plan, plan to fail ...'

There are a number of important steps that an organisation should take to protect itself against a potential data breach. This will be essential, particularly in the EU where the General Data Protection Regulation will, when it comes into force, impose certain accountability requirements on organisations. In order to comply with those requirements, organisations will need to put in place preparatory measures to guard against the risk of a data breach. Those preparatory measures should include the following:

- Having a data map in place showing where and how data is stored and who is responsible for it. This allows the organisation to assess the potential scale of the problem quickly in the event that a data breach occurs.

- Establishing a risk map, showing the sectors and jurisdictions in which the organisation is active and highlighting any activities or locations which pose a high risk in terms of data breaches. This allows the organisation to understand better the risks it is facing and put in place tailored measures to mitigate these risks.

- Ensuring that any outsourced service providers which have been engaged by the organisation are taking all necessary precautions and not exposing the organisation to an unnecessary risk of a data breach.

- Establishing a data breach management team, with a senior management lead and deputy, to allow the organisation to move quickly and decisively in the event that a data breach occurs.

- Devising an incident management plan, setting out how the organisation will respond to a data breach. The plan should be tested to ensure it will work when a data breach strikes. This plan should be drafted with the terms of the organisation's cyber insurance policy (if it has one) in mind to ensure that effective notifications are made to insurers when a claim arises (see 'notifications' below).

- Knowing in advance when regulators will need to be notified about a data breach and what form this notification should take. In particular, organisations which are active in a number of jurisdictions should be aware of the notification

requirements which apply to them in each jurisdiction. Expert advice on this issue, setting out the notification requirements for each jurisdiction, will make notification much more straightforward when the time comes.

- Making sure that the required internal and external resources are in place to deal with a data breach adequately. For example:
  - Identifying suitable legal counsel to provide privileged advice in the event of a data breach.
  - Having experts on hand to deal with the IT forensic issues and public relations difficulties which a data breach can cause.
  - Having a system in place to ensure that the organisation is capable of contacting every affected customer who that might need to be contacted when a data breach happens (bearing in mind that the means of communication may be different for different types of customer).
- Considering the benefits of cyber insurance and reviewing the terms of the cyber insurance policy to ensure it covers the particular risks faced by that organisation. Not all policy wordings are the same and some contain exclusions which could leave an organisation with unexpected gaps in cover.

Stage 2 | discovering a data breach

An organisation's executives and employees should always be vigilant to the risk of a data breach and should be aware of the warning signs which may indicate that a breach has occurred, such as unusual patterns of access to the organisation's databases or unusual patterns of customer behaviour. In this regard, appropriate systems and controls should be put in place to act as an early alert system for potential data breaches.

Once a data breach has been identified, the breach management team should take urgent steps to implement the organisation's breach management plan. A swift and comprehensive response to a data breach will help to minimise its consequences, reducing the overall financial cost and reputational damage to the affected organisation.

Stage 3 | responding to the data breach

Within a short time-frame, an organisation's data breach management team will need to take a number of steps in accordance with its breach management plan to assess and mitigate the effects of the data breach.

These include informing the organisation's legal advisers of the data breach and obtaining preliminary legal advice as to immediate next steps, including:

- Advising on the potential consequences of the breach, including whether at this stage the organisation's insurers should be notified about the breach and whether there are any obligations on the organisation to notify its regulators or the owners of the data which has been compromised.
- The co-ordination of a crisis response team, which may involve:
  - forensic IT experts, to assess the type and volume of data affected and the risks involved, with a view to limiting the spread and effect of the data breach
  - PR experts to deal with the reputational and brand risk arising from the data breach.

The importance of involving legal advisers

Involving the legal advisers at this early stage and co-ordinating the crisis response team through the legal advisers will ensure that the organisation is protected to the maximum extent possible as far as sensitive communications are concerned. The aim will be to ensure that communications regarding sensitive information are (as far as possible) covered by legal privilege, to limit the extent to which such communications must be disclosed in any legal proceedings that are issued against the organisation, thereby limiting the organisation's exposure to loss.

Stage 4 | notification

When a data breach occurs, there are three types of notification which an organisation will need to consider making:

- First, if it has cyber insurance, it will need to notify its insurers of a potential claim.
- It may also need to notify its regulators.

Notification to insurers

The provisions in a cyber insurance policy which require an organisation to notify its insurers of a potential claim are very important. When a data breach occurs, notification will most likely need to be made promptly and could be required within a particular number of days. Notifications may also need to include certain information in order to be effective. As well as details of the breach itself, this may include information on the regulatory or financial consequences of the breach, so an assessment of these issues will need to be made at a very early stage. An effective notification is therefore key if an organisation wishes to recover its losses under the policy.

In terms of making notifications to regulators, the requirements can differ depending on the type of organisation and the regulated sector in which it operates. Furthermore, where a data breach affects individuals or entities in different jurisdictions, the trigger points and requirements can multiply. The requirements may also depend on the type or volume of the data concerned or on the potential of the data breach in question to cause harm. The formalities of a notification to a regulator must also be considered.

Most regulators will require a notification to be made within a certain number of days and to contain certain types of information on the nature of the breach and the steps that are being taken to remedy it. The organisation will need to take care in ensuring that all necessary notifications are made and meet the required standard. Therefore, as previously mentioned, it is important to be familiar with the various notification requirements in advance of a data breach occurring.

Notifications to regulators

Failure to make a timely and effective notification to the relevant regulators is likely to exacerbate any sanction which the regulator eventually imposes in relation to the data breach. It should be noted that, in addition to regulators, in many cases it is possible that law enforcement agencies may need to be notified about a data breach, particularly if the breach is a result of fraud, theft or cyber-crime.

Notifications to affected individuals

Notifications to affected individuals should be made with a view to minimising the risk of those individuals bringing claims against the organisation. When it is necessary to notify the affected individuals of the data breach, the organisation may wish to offer, free of charge to the individuals concerned, the services of a competent ‘identity theft protection service’ to assist the individuals in mitigating the harm they may suffer.

Stage 5 | continuing to manage the data breach response

The initial response to a data breach is vital. However, ongoing management of a data breach and planning for the future in light of it is just as important. In the period following the organisation's initial response, it will be important to do the following, in conjunction with the organisation's legal advisers where possible:

- Engage in continued co-operation and dialogue with regulators, including preparing responses to any enquiries which regulators might have.
- Engage in dialogue with the owners of the compromised data, if appropriate, and respond to any complaints made or claims relating to the data breach.
- Keep insurers updated with any relevant information that may emerge following the data breach, with a view to obtaining insurers' agreement to the strategy adopted by the organisation in responding to the data breach.
- Continue to engage with third parties who are managing the consequences of the data breach, including any IT consultancies and PR agencies.
- Make further investigations to understand fully the extent, causes and implications of the data breach, with a view to minimising the risk of a similar breach happening in future. This process can be an invaluable means of reducing the risk faced by an organisation and will help to ensure that an organisation has the necessary systems and controls in place following a data breach.

Stage 6 | where appropriate, take action against those responsible

A very large proportion of data breaches are caused by an organisation's outsourced service providers mis-handling the personal data entrusted to them by the organisation.

When an organisation suffers loss as a result of a data breach which was caused, for example, by the negligence or wilful misconduct of the employees of a service provider, it may wish to hold that service provider accountable for the loss suffered. Advice should be obtained on whether a third party service provider could be held accountable for loss and damage caused by the data breach.

Insurance requirements

Organisations should also be aware that, to the extent there is insurance in place to cover the loss in question, it is likely to be a condition of the policy that nothing should be done by the organisation to prejudice the insurer's right to recover the loss from any third party (including service providers).

Conclusions

The scale and severity of cyber risk are enormous and continue to grow. This trend looks set to continue as economies across the world become increasingly reliant on electronic data.

It is vitally important that organisations holding, using or relying upon electronic data are prepared for data breaches and respond to them appropriately.

This includes considering the benefits of cyber insurance, which is an important tool in safeguarding an organisation's future against the threat posed by cyber risks.

Our Amsterdam team

We have a full-service data protection practice with extensive data breach response and management experience.

We have advised major banks, building societies, insurance companies, asset management companies, professional service firms and major corporations in respect of serious data breaches and their consequent correspondence and resolution with relevant regulators. This has included advising on a major multinational breach involving a co-ordinated response in 16 jurisdictions, which required detailed advice from a number of our international offices and with a number of correspondent local counsel.

Contacts

Jan Duyvensz
Of counsel
Data breach and Insurance coverage, Amsterdam
Norton Rose Fulbright LLP
jan.duyvensz@nortonrosefulbright.com

Floortje Nagelkerke
Senior associate
Data privacy and Data breach, Amsterdam
Norton Rose Fulbright LLP
floortje.nagelkerke@nortonrosefulbright.com

Global resources

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Our office locations

People worldwide

7400

Legal staff worldwide

3800+

Offices

50+

Key industry strengths

Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

Europe

Amsterdam
Athens
Brussels
Frankfurt
Hamburg
London
Milan
Moscow
Munich
Paris
Piraeus
Warsaw

United States

Austin
Dallas
Denver
Houston
Los Angeles
Minneapolis
New York
Pittsburgh-Southpointe
St Louis
San Antonio
Washington DC

Canada

Calgary
Montréal
Ottawa
Québec
Toronto

Latin America

Bogotá
Caracas
Rio de Janeiro

Asia

Bangkok
Beijing
Hong Kong
Jakarta[1]
Shanghai
Singapore
Tokyo

Australia

Brisbane
Melbourne
Perth
Sydney

Africa

Bujumbura[3]
Cape Town
Casablanca
Dar es Salaam
Durban
Harare[3]
Johannesburg
Kampala[3]

Middle East

Abu Dhabi
Bahrain
Dubai
Riyadh[2]

Central Asia

Almaty

1 Susandarini & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright US LLP
3 Alliances

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com