Group Briefing

May 2015

# Cyber-Security & Minimising Litigation Risk

ARTHUR COX - KEY CONTACTS

JOANELLE O'CLEIRIGH
PARTNER, LITIGATION & DISPUTE RESOLUTION
+353 1 618 0402
joanelle.ocleirigh@arthurcox.com

GREGORY GLYNN
PARTNER, LITIGATION & DISPUTE RESOLUTION
+353 1 618 0470
greg.glynn@arthurcox.com

PEARSE RYAN
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0518
pearse.ryan@arthurcox.com



The Government's Draft National Risk Assessment 2015 names cyber-security as one of the potential risks for Ireland in 2015. Cyber-security is not *'just an IT issue'*. It is a business critical issue that cannot be ignored and should be viewed as part of an organisation's overall risk management strategy. Regulators, particularly in the financial services industry, are increasingly asking whether organisations are 'cyber-attack' ready. The Central Bank recently commenced cyber-security inspections as part of its enforcement priorities for 2015. Organisations subject to inspection will face questions about their cyber-security risk assessment, business continuity plan, insurance, network controls and so on.

A key part in any cyber-security strategy is understanding the legal implications of a cyber-security breach. There is the obvious cost in terms of reputational damage and business disruption, but there is also the cost of exposure to litigation. The tips set out below will help reduce litigation risk and minimise the value of any potential claims.

## BE INFORMED

Cyber-security is a relatively 'new' area and one that is constantly evolving. Keep yourself informed. Be aware of the most common types of security breach, e.g. systems failures and data corruption; viruses and malicious software; theft or fraud involving IT systems; incidents caused by staff; and attacks by hackers. Keep up-to-date with new initiatives to counter cyber-security threats.

## UNDERSTAND THE LITIGATION RISKS INVOLVED

Most organisations will understand the reputational damage that can be caused by a cyber-security breach and will be familiar with the possible data protection issues that can arise. However, they may not have considered the potential exposure to litigation. As a result of a cyber-security attack, an organisation may find itself in breach of an express or implied term to store customer data securely, or it may be liable in tort for failure to take reasonable security precautions when storing customer information. In addition, data subjects may take direct action under data protection legislation.

## DO NOT BURY YOUR HEAD IN THE SAND

Cyber-security cannot be regarded as *'just an IT issue'*: it is a business-critical issue that cannot be ignored. Cyber-security should be a priority for any organisation. Managing cyber-security risk needs to be driven from the top down.

## UNDERTAKE A SECURITY RISK REVIEW

Ensure the IT department, the compliance officer, the legal department in your organisation and other business-services functions conduct a review of existing security processes. Identify what your organisation needs to protect (e.g. IP, customer details, etc) and identify potential areas of weakness. Consider instructing an external information security consultant to assess the effectiveness of existing security processes.

#### PUT IN PLACE COMPREHENSIVE POLICIES, PROCEDURES AND PLANS

Ensure the IT department, the compliance officer and other external experts (e.g. IT/ legal) put in place a set of comprehensive policies and procedures, e.g. an information security policy and a home and mobile working policy. Ensure these policies accord with recognised best practice. This should help minimise the risk of claims in tort. It is also extremely important to put in place a comprehensive cyber-incident response plan.

#### CREATE A CULTURE OF CYBER-SECURITY AWARENESS

Implement a training programme right across your organisation. Raise awareness of all policies. Ensure all employees are trained to identify, mitigate the risk of, and respond to cyber-security threats. Make employees at all levels aware of their obligations and responsibilities.

#### REVIEW YOUR ORGANISATION'S INSURANCE POLICIES

Confirm whether your organisation's overall insurance policies cover losses arising from a cyber-security attack. If not, consider taking out a cyber-insurance policy. It is advisable to ensure that any such policy makes provision for incident response assistance. Check also that you have adequate cover for business interruption services.

#### CARRY OUT AN AUDIT OF KEY SUPPLY AGREEMENTS

Check whether your organisation's key supply agreements address liability as a result of supplier failure to fulfil express contractual obligations due to a cyber-attack. Check also whether there is a threat to your organisation where a supplier which has access to your system is compromised.

#### CONFIRM WHETHER SUPPLIERS TO YOUR ORGANISATION ARE OBLIGED TO PROVIDE SUPPORT IN THE EVENT OF A CYBER ATTACK

Review key agreements to determine whether business suppliers are contractually obliged to provide business continuity support in the event of a cyber-attack on your organisation. Check also supplier ongoing supply obligations in circumstances where they are the subject of a cyber-attack.

#### CONFIRM WHETHER YOUR ORGANISATION IS OBLIGED TO CONTINUE ITS CONTRACTUAL OBLIGATIONS IN THE EVENT OF A CYBER-ATTACK

In the case of agreements where your organisation is the supplier, check whether there is an obligation to continue supplying goods/performing services where your organisation is subject to a cyber-attack.

#### ENSURE ALL IP IS ADEQUATELY PROTECTED

Some cyber-attacks may be specifically targeted at an organisation's intellectual property, particularly in cases where this is the organisation's most valuable asset. Ensure all IP is properly registered and protected. Ensure policies are in place to deal with an attack on your IP.

#### ASSESS YOUR ORGANISATION'S REGULATORY OBLIGATIONS

Confirm whether your organisation is subject to any specific cyber-security regulations. For example, a listed company will need to consider whether the event of a breach constitutes inside information/ price sensitive information which needs to be disclosed. This is an issue which may require input from your external lawyers.

#### BE AWARE OF ANY NOTIFICATION/REPORTING REQUIREMENTS

The Data Protection Commissioner (DPC) has issued a Code of Practice for dealing with Personal Data Security Breach. The Code recommends (except in cases of telcos and ISPs, where it requires) that all incidents in which personal data has been put at risk be reported to the DPC as soon as the data controller becomes aware of the incident. Anyone affected by the incident should also be notified. Familiarise yourself with this Code of Practice and ensure that all policies and procedures are aligned with it.

#### HAVE STRATEGIES IN PLACE TO MANAGE ANY REPUTATIONAL DAMAGE

Be prepared for negative publicity in the event of a security breach and know how to manage this. If criminal proceedings are taken against the perpetrator, expect the case to get media attention and your organisation to be named, even though it will not be a party to the proceedings. Have 'Guidelines' in place to assist those who may be responsible for issuing press releases and ensure that particular care is taken where court proceedings are in being or where your organisation is a listed company. In such circumstances, your external lawyers should review any proposed public comment.

#### KEEP RECORDS OF ALL CYBER-SECURITY INCIDENTS

Ensure someone in your organisation is responsible for keeping records of all cyber-security incidents and the measures taken to deal with these.

#### WORK WITH YOUR LAWYERS TO MAXIMISE PRIVILEGE

In the event of a cyber-attack, consult your lawyers immediately. Lawyers can assist with incident management and advise on the legal implications of the breach and any specific obligations on your organisation. The involvement of lawyers is also crucial to attract legal privilege, which may prove to be extremely important in the event of litigation.

#### LEARN FROM EXPERIENCE

If a security breach occurs, learn from this. Review and update any policies and procedures accordingly.

**arthurcox.com**

**Dublin**
+353 1 618 0000
dublin@arthurcox.com

**Belfast**
+44 28 9023 0007
belfast@arthurcox.com

**London**
+44 207 823 0200
london@arthurcox.com

**New York**
+1 212 782 3294
newyork@arthurcox.com

**Silicon Valley**
+1 650 943 2330
siliconvalley@arthurcox.com