Group Briefing

July 2015

Understanding Cyber-Risk: Our 10 Key Takeaways

ARTHUR COX - KEY CONTACTS

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

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

This document contains a general summary of developments and is not a complete or definitive statement of the law. Specific legal advice should be obtained where appropriate.

All the experts say, there are two kinds of business: those which have been subject to a cyber-breach, and those which do not know they have been subject to a cyber-breach. Which business are you?

We were privileged to moderate a very insightful cyber-security discussion in Dublin on 30 June in association with the Embassy of the United States of America. The speakers were The Honorable John P Carlin, Assistant Attorney General for the National Security Division of the US Department of Justice, Sean M Joyce, Principal Advisor to PwC, from McLean, Virginia and Jenny Durkan, of Quinn Emanuel, Seattle, Washington State.

Here are their 10 key tips on managing cyber-risk.

1. ***Do not delay:*** There is no greater threat to business than cyber-threat. Doing nothing is not an option. Do not put this to the bottom of your 'To Do' list. Start dealing with it today. Remember, cyber-threat is not an IT problem: it is an enterprise risk. The operating assumption should be that no business/organisation is immune from attack.
2. ***Planning is key:*** A cyber-breach is not just 'a breach': it is a crisis. It can mean life or death for a business/organisation. While you cannot eliminate the threat, you can plan how to respond to a breach. Do this now. In the middle of a storm is not the time to ask where is the shelter.
3. ***Road-test the plan:*** Planning on its own is not enough: You need to road-test your plan. How will it work in practice? Have you thought through all the various contingencies? How will a breach affect the business/organisation? Can you shut down your information and communication systems safely? How will you deal with regulators? Who will be your spokesperson? What will you do to minimise litigation risk?
4. ***Get everyone around the table:*** Everyone who will be involved in responding to an attack should be involved in planning for an attack. Get the right people around the table. The day of the crisis is not the day you should be meeting your advisors for the first time.
5. ***Be clear on who you can contact in Government and An Garda Síochána:*** In the event of an attack, you may need to liaise with Government and An Garda Síochána. Make sure you have the correct contacts. If you do not have this, you will not have an effective plan.

6. ***What is of most value to the business/ organisation?*** The Board and senior management need to identify what needs to be protected. What is of most value to the business/ organisation? Is it intellectual property? Is it confidential business information? What are you doing to protect this information? Where is it stored? Is it in a folder named 'Crown Jewels'? Consider putting in place a naming convention only understood by limited internal personnel.

7. ***Conduct a review of all third party suppliers/service providers:*** Everyone you do business with is part of your business eco-system. Your business eco-system is only as strong as your weakest link - find this link. Compile a complete list of all your third party suppliers and service providers and carry out a comprehensive due diligence exercise.

   Review all contracts: do you have the right to carry out an audit on your suppliers/service providers? Are your suppliers/service providers required to follow a cyber-security framework? What are they required to do to protect your information? Are they required to inform you if their systems have been breached?

8. ***Raise awareness of the threat:*** Ensure all personnel in the business/organisation understand the scale of the threat and are alive to the most common forms of attack. Do they know what 'spear-fishing' is? Do they know who to contact if they receive a suspicious email? Roll-out training across all sectors of the business/organisation.

9. ***Print out the plan and a list of key contacts:*** All key personnel should have a hard copy of the plan and a laminated card of key contacts and their contact details. Remember, when you are in crisis mode, you may not be able to use your information and communications systems. Make sure this plan and your key contacts are reviewed and updated regularly. An out of date plan in a crisis will hamper your rescue.

10. ***Be open about the breach and learn from it:*** You should treat a breach in the same way as you would any criminal act: report it. Talk to your Government and Garda contacts immediately. Information sharing is critical to protecting not just your business, but the economy in general and Ireland's reputation abroad as a great place to do business. Finally, learn from the breach. If you do not learn lessons from a breach, you are opening the business/organisation up to potential liability in the event of a further attack.