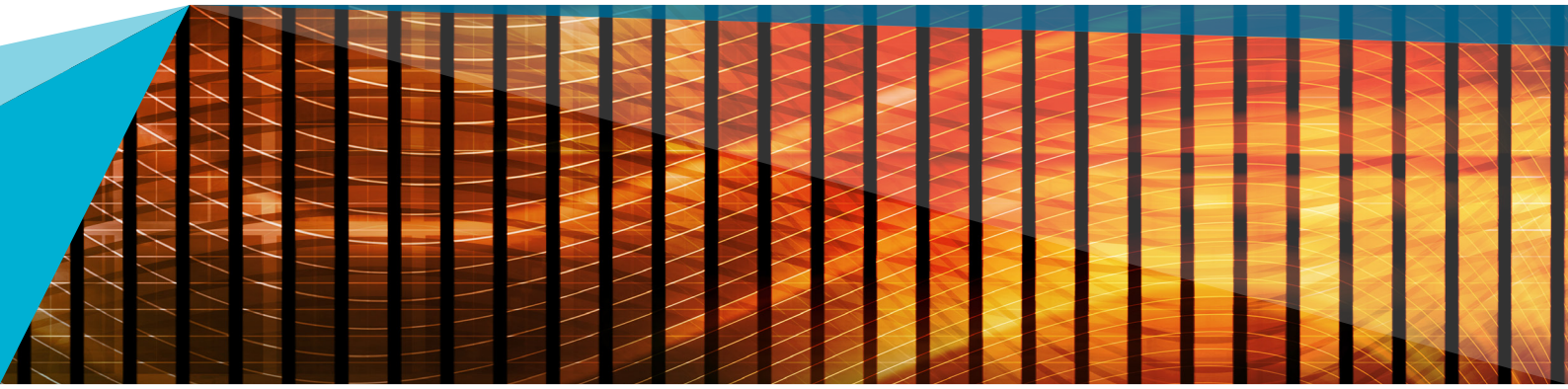
MARSH

October 2017

CYBER: CONVERTING RISK INTO OPPORTUNITY



There is little doubt that Irish businesses are becoming more concerned with the risk of a cyber-attack, but is there enough awareness of the true extent of the actual risk?

Marsh's Ireland office recently hosted an event, *Cyber: Converting Risk into Opportunity*, which examined how leading organisations are evolving their thinking in managing cyber risk. The event, in partnership with AIG and held in Dublin, was led by cyber insurance, risk management, and legal experts. It highlighted the growing cyber risks and regulations organisations now face and included speakers from Marsh, AIG, and Arthur Cox.

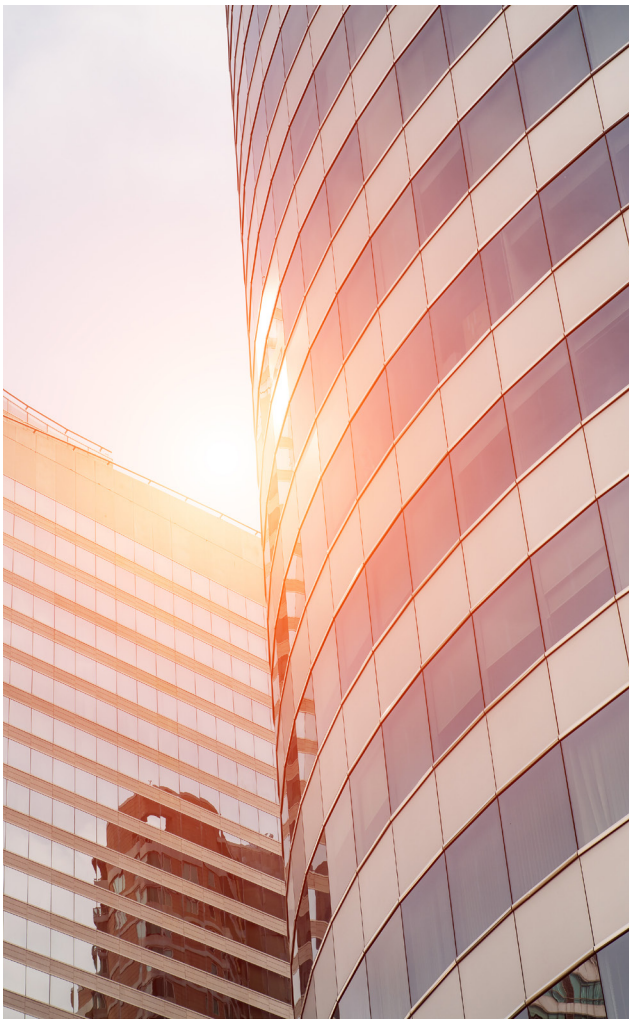
The event produced thought-provoking ideas around the way businesses in Ireland can better manage their cyber exposure, particularly given the recent increase in major cyber-attacks and the impact of the pending General Data Protection Regulation (GDPR).

BETTER UNDERSTANDING OF CYBER NEEDED AS RISKS INCREASE

"As the digitisation of business increases, there is a greater need for vigilance and discipline to navigate the cyber landscape. However, not all organisations are at the same level of maturity when it comes to managing cyber risk", Peter Johnson, Head of Cyber Advisory at Marsh, pointed out.

Johnson identified four stages of cyber maturity into which organisations fall:

1. **Preventing attacks from happening:** The main focus for organisations at this stage is on cyber security, with the risk viewed as an IT problem. As tactics used by cyber attackers continue to evolve and major attacks become more frequent, prevention alone is not enough.
2. **Planning for what happens if an attack does take place:** At this stage, cyber starts to become a board level issue. These organisations have tested breach plans in place, have worked to become GDPR compliant, and have looked at transferring the risk through the use of insurance.
3. **Managing cyber as a quantifiable risk:** Organisations are using quantification to manage the risk and are looking at how to finance the loss, should they be hit by an attack.
4. **Turning risk into opportunity:** At the leading edge, a few companies are starting to see cyber as an opportunity, using the investments they have made in cyber to help enhance them to their client base.



Worryingly, some companies still sit at the first level of cyber risk management maturity. But this is not enough to effectively manage the risk. As recent press headlines have shown, with events such as the WannaCry and Petya/GoldenEye attacks, more companies are finding themselves victim to increasingly sophisticated attacks, which, in many cases, cannot be completely prevented.

To protect themselves, organisations need to:

- Understand the exposures they have across the organisation.
- Engage with experts to help them understand when a breach has occurred and the resulting reputational damage.
- Transfer the risk through the use of insurance.

THE INSURANCE MARKET IS MATURING

Once the cyber issues have been defined, companies must consider how to finance any losses. Cyber is an intangible risk that businesses are still struggling to grapple with. Insurance is a useful tool to systematically go through the problem as it turns cyber risk into a financial question. It provides strategic tools for managing it by:

- Defining the risk within the business in a systematic way using loss scenarios.
- Quantifying the risk by taking a data-driven view.
- Enabling rational financial decisions.

The insurance market for cyber risks has matured considerably in recent years. "A few years ago, the insurance market was quite immature from a cyber perspective with many exclusions," said Marsh's Johnson. "These days, policies are quite broad; however they need to be matched to the risk."

Some aspects of the broader cyber policies will also be covered under existing policies. Care should be taken to make sure that coverage does not overlap.

"We recommend looking at what the risks are and looking at what is already in place and then taking an objective view on what the most appropriate coverage is going forward and putting that in the context of the risk appetite of the organisation," Johnson added.

As the losses involved in a cyber-attack increase, (as attacks become larger and more sophisticated), the use of insurance for risk transfer will become more important. "If you're an organisation that holds and processes large amounts of third-party data and information, the cost of a data breach can quickly reach into the millions of Euro," said Ciaran Reddin, Senior Cyber & Professional Indemnity Underwriter at AIG.

NEW REGULATION WILL INCREASE CYBER COSTS FOR BUSINESSES

The GDPR will bring some significant changes to European data protection law when it comes into effect on 25 May 2018. For businesses in Ireland, this will mean:

- Less time between discovering the attack and notifying the regulator.
- Greater protection of personal data for customers including new rules around notifications.
- Bigger fines and clean-up costs.

"However, the regulation can be viewed as more of an evolution than a revolution. The security standards under the GDPR is similar to those already required in the industry", Colin Rooney, Partner for the Technology and Innovation Group at Arthur Cox, explained.

One of the biggest changes for businesses under the GDPR will be the fines that are imposed, which will introduce a maximum of EUR20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Costs for organisations will increase considerably following a breach under the GDPR rules and this will need to be considered when assessing the impact a potential cyber-attack could have.

The effect of the regulation will vary depending on the nature of the organisation. However, while there is no one-size-fits-all approach, all organisations need to be aware of the data they hold and the way the GDPR will change their cyber exposure, Rooney said.

The new notification rules will require organisations affected by a data breach to notify the regulator and affected data subjects within 72 hours of becoming aware of it. This will mean organisations will have less time to respond, and may find it challenging to gather the required information.

"In my experience a data breach really does shake an organisation. There's wide-spread panic. While there's often very good leadership at the top, people are very concerned about not only their own position, but what their obligations are, and that's not helped by the regulation being a little bit ambiguous at the moment," said Rooney.

"It is important that when you engage with the regulator, you do so with knowledge and confidence," he added.

> "In my experience a data breach really does shake an organisation. There's wide-spread panic."
>
> COLIN ROONEY, ARTHUR COX

CYBER AS AN OPPORTUNITY

Ultimately, cyber risk can be seen as an opportunity for those businesses that put themselves at the leading edge of managing the risk by using it as a way to differentiate themselves from their competitors.

According to Marsh's Johnson, organisations can use two potential business models to take advantage of the opportunities available under a mature management of cyber risk. The first is use of cyber to enhance the organisation's proposition and use that, as a means to offer its clients services such as:

- Cyber security.
- Breach services.
- Insurance.

The second is for organisations to capitalise on their cyber investments by increasing customer's trust of the organisation's service and product quality. This can be done by offering guarantees to their clients and backing that up with an insurance programme. In addition, while regulation such as the GDPR will provide an impetus to improve data security and controls around the use of personal information, it presents an opportunity for organisations to better understand their data and how it may be used to add value to their business.

Given the wide-ranging impact of the cyber-attacks over the past year, combined with the upcoming effects of the GDPR, organisations that improve their cyber maturity now will find themselves in a better position to not only face upcoming regulation but to put themselves ahead of their competitors.

GRAPHICS NO. 17-1022