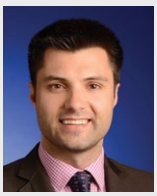
Reflections from AIG's Corporate Governance and Cyber Seminar

This year's cyber panel discussed:
Post GDPR - are data breaches on the rise?

Mark Camillo
Head of Cyber EMEA,
AIG



Konrads Klints
Director, Cyber,
KPMG

Steven Hadwin
Head of Operations -
Data Protection, Privacy
and Cybersecurity
Norton Rose Fulbright

Typhaine Beaupérin
Chief Executive Officer
FERMA - Federation
of European Risk
Management Associations

Nic Daley
Senior Consultant
Hill + Knowlton Strategies

Mark Camillo, EMEA Head of Cyber, AIG:
We're now more than a year in to the GDPR, which often weighs on a lot of our clients' minds. And we thought it would be useful to have a discussion about what we're seeing, how the policy is responding, what's going well, and what could be improved upon.

Konrads, let's start with you. Obviously KPMG is involved in doing work, almost on a daily basis, in responding to incidents and events.

Q. Can you give us a little bit of a background as to what you're seeing, and what are the most common incidents you and the team are responding to?

Konrads Klints, Director, Cyber, KPMG:
A. What we mostly see are cyber events that are directly from organised crime groups. And organised crime groups always are out there for one thing and one thing only - money. The thing we see as most common, in terms of cyber events that are inflicted by somebody else, is business email compromise. The bad guys are inserting themselves between communication streams, particularly looking for an opportunity where there's a money transaction involved, for example settling a supplier's invoice and saying 'Hey, we've just changed bank accounts. Could you please transfer this money to this account?' And as a result the client transfers the money and they've done their duty. 30 days later the supplier starts chasing for payments. There's an investigation and the money lost ranges somewhere from the low tens of thousands to the tune of, say, 16 million euros through the banking system. So that's the number one thing we're seeing.

And the other, especially in manufacturing companies right now, is around ransomware. Cyber criminals have figured out that actually large companies can offer much more money. They launch the ransomware and say 'If you don't want that to have to happen again, please pay us money' and the money ranges anywhere between £150,000 up to £1 million.

Mark Camillo:
Q. Steven, from a legal perspective, what are the latest in the GDPR developments? There seems to be a large number of notifications made to the ICO in the UK as well as other data protection authorities across Europe.

Steven Hadwin, Head of Operations - Data Protection, Privacy and Cybersecurity, Norton Rose Fulbright:
A. Yes, well there are a few trends we've seen since the implementation that are worth commenting on. The first one I'd mention is we've seen a real tendency of companies to over report and over notify personal data breaches (by reporting to data protection authorities and notifying that individual). The ICO has acknowledged that this is happening. They've said that around one third of all the incidents that are notified to them don't actually meet the thresholds that require incidents to be notified. They use the word inundated to describe how they feel about the number of notifications that are coming in. Equally on the data subject side, we see companies pushing to notify data subjects when they don't strictly have a requirement to do so. Now often what companies are trying to do there is just achieve optimal compliance with GDPR to comply with their obligations.

And in some circumstances that is of course, commendable behaviour, but there are also risks attached. One other point on this over notification trend is that it's particularly pronounced in North West Europe, so we're very much at the heart of it. UK, Ireland and the Netherlands are probably the three jurisdictions I'd focus on around this trend.

> " One of the risks with this approach is that there's been a real increase in the number of claims for compensation being brought by individual data subjects who have been affected by data breaches."

GDPR gives people the toolkit to bring those complaints and then it entitles them to compensation if they have suffered what's called material or non-material damage as a result of a breach of the regulation. You can bring a claim if you felt distressed or anxious or had any kind of negative emotional reaction. You don't have to have suffered financial loss. So what we tend to see now is whenever there is a large data breach that happens, it's notified to the affected population. In a way it is a good thing and it is one of the aims of the regulation that individuals can take advantage of their rights in this way. Partly though, I would comment that this is to some degree, the result of the emergence of a number of independent law firms that are looking to bring these claims and encourage people to bring them on a sort of quasi collective basis.

Mark Camillo:
We have now released our 2018 claims report on what we're seeing with respect to cyber notifications. It's interesting because in Ireland, over 40% of incidents are being reported to the regulator. Whereas in places like Spain, less than 10% are being reported, so there is this big divide.

Q. Typhaine, what do you hear are the risks that the risk managers are most worried about when looking at this topic?

Typhaine Beaupérin, Chief Executive Officer, FERMA:
A. So first of all for the GDPR, I think it is fair to say that it's been a real challenge for companies to get through the implementation. It has involved a lot of resources and time. It has been costly. But one of the good things that we can see, and the feedback that we hear, is that it has been a catalyst to raise awareness about those issues. And we see once more that the corporate value of companies is based on intangible assets and data. The data protection that is security has definitely entered into the risk categories of many risk mapping exercises. And it has prompted discussions at the Board level. In addition, the GDPR has had a significant impact on data protection policy and enforcement beyond the EU. So we can see that there is really now a trigger towards normalisation of data protection globally thanks to the GDPR. In terms of managing cyber risk in general, of the two challenges that the risk managers are facing, the first one is about quantification. It's how you translate cyber risk impacts into business figures. And the second one is a governance issue.

> " We're seeing that it's a cross disciplinary risk and it needs a holistic approach. However this is not always the reality and the risk manager can sometimes feel that they are alone."

IT measures can take the larger parts of the discussion, whereas it should be a more rounded discussion on the overall exposure of the company led by the risk manager.

Mark Camillo:
So Nic obviously you're seeing a lot of these incidents as they happen and you're seeing them in the news.

Q. Can you spend a little bit of time talking about some of the breaches that you've seen and those handled well and maybe those that have not been handled so well and some of the lessons learned?

Nic Daley, Senior Consultant, Hill + Knowlton Strategies:
A. So cyber-attacks and data breaches are similar to other organisational crises in that yes, you will be judged on the fact that it happened, but you'll also be judged on how you respond. Considering all the different audiences and stakeholders that an organisation needs to think about and communicate with, it is really critical.

Where we have good case studies, I'll use the likes of British Airways last year and their speed of response, a highly visible CEO, and leadership was on display in terms of a strong voice. It was the same with Norsk Hydro, where there was speedy decision making and good communication from leadership.

What we have also seen post GDPR is that there can be a real freneticism within organisations to communicate very, very quickly after a breach. And the risk is that at any time you usually don't have all the information that you would like to have in order to communicate.

So there is an ongoing judgement to be made with the forensic data investigators, with a legal team, with a reputation management/PR side of things, to say okay, at what point do we need to be communicating and with whom?'

The way that we consider it is when we think about communicating with the different stakeholders - what do we want them to know and to think, and to feel and then to do?

> " If we just rush to notify and say this has happened, and move onto the next thing, we could actually escalate the initial breach by bringing clients a wave of additional enquiries and queries that actually we're not in a position to answer."

And so we've worked on a number of breaches where there's an ongoing period of engagement. You might do your initial notification within a week. It could take a couple of months, depending on the data investigation, for an ongoing dialogue with their different audiences and stakeholders, depending on what the forensic data investigation is unveiling.

Coupled with that, some of the other risks and pitfalls that we've seen are where you're not communicating internally in terms of your wider communications piece.

So you might be launching a new product or you might be engaging with your customers about another particular issue and those internal communications teams aren't talking to one another. The last thing you want is to post something very positive on social media without realising actually there's a storm that's developing on Twitter or LinkedIn or wherever it might be, that's highly critical of the organisation.

The crafting of the messaging and the engagement that we have with customers, with the shareholders, with staff and other partners, is critical to demonstrate that you are being genuinely transparent, that you are being authentic and that you are taking this seriously. It's an opportunity through your communication to demonstrate all of the things that your business or organisation has done, in order to bolster yourselves and protect, to the best of your ability. And then what you are going to do in the long term to try and ensure that this doesn't happen again.

Mark Camillo:
Thanks to our panellists. Our cyber claims intelligence series report can be found at www.aig.co.uk/insights/claims-intelligence-cyber-report-2019

Mark Camillo
Head of Cyber, EMEA
Tel: +44 (0)20 7651 6304
mark.camillo@aig.com

Mark Bannon
Head of Cyber, UK
Tel: +44 (0)20 7651 6317
mark.bannon@aig.com

Geraud Verhille
Head of Financial Lines, UK
Tel: +44 (0)20 3217 1840
geraud.verhille@aig.com