Cyber Update:
Byte-Sized Regular Updates on Cyber Liability Issues

ICO fines insurer for loss of customer personal data

The Information Commissioner’s Office (ICO) has fined online travel insurer Staysure.co.uk £175,000 after it failed to keep customers’ personal information secure.

Over 5,000 customers had their credit cards used by hackers who potentially had access to over 100,000 credit card details, as well as customers’ medical details.

The ICO investigation found the company had breached the Data Protection Act by failing to keep the information secure. It had no policy or procedures in place to review and update IT security systems, and had twice failed to update database software, which could have prevented this incident. This left security flaws in the system, some for as long as five years, which hackers ultimately exploited to gain access to customer information.

The ICO’s Monetary Penalty Notice and decision is available at: https://ico.org.uk/media/action-weve-taken/mpns/1043368/staysure-monetary-penalty-notice.pdf

ABI says cyber insurance to become business essential in next decade

The Association of British Insurers (ABI) believes that cyber insurance will become as common for UK businesses as property insurance by 2025.

Huw Evans, Director General at the ABI, said:

“Cyber risk is growing rapidly. At the moment, despite more than 80 per cent of large businesses suffering a cyber security breach in a 12 month period, only around 10 per cent have any form of cyber insurance.”
Online breaches can cost millions, and would threaten the viability of many businesses, so the stakes are high. Cyber insurance is an increasingly important way for businesses of all sizes to manage this threat.

The UK insurance industry is already providing cover for cyber risk to customers around the world. More British firms are now taking advantage of this expertise and by 2025 this type of cover will be seen as an essential business purchase.

CII launch data protection best practice guide

The Chartered Insurance Institute (CII) has launched a Best Practice Guide relating to requests made under section 29(3) of the Data Protection Act (which allows organisations to share data with a third party in order to prevent and detect crime in the insurance industry).

Companies that embrace the model are obliged to:

+ Ensure their employees make requests only where it is appropriate and necessary;
+ Ensure that due consideration is given to requests received by them;
+ Provide a detailed reason to the requester in the event that they are unwilling to disclose personal data;
+ Ensure their staff are appropriately trained in the use of section 29(3);
+ Ensure their Single Point of Contact (SPOC) details are kept fully up to date with the Insurance Fraud Bureau (IFB); and
+ Ensure a representative attends and fully participates in the IFB’s regular forums.

The CII’s guide is available at: https://www.insurancefraudbureau.org/media/1091/best-practice-guidance-version-5-0.pdf
ICC launches cyber security guide

The International Chamber of Commerce (ICC) has launched a new plain English guide to help companies of all sizes manage cyber security and mitigate the threat posed by cybercrime.

The guide has been prepared for management and information technology teams to aid discussions within a company. It includes:

- A security self-assessment questionnaire;
- A set of five principles to reduce the risks associated with cyber security incidents; and
- A checklist of six steps every company should take.

ICC Secretary General John Danilovich said:

"The digital economy is playing an increasingly important role in opening up new markets and opportunities for global business. But in today's global economy many businesses adopt modern information and communications technologies without fully realizing the new types of risks to be managed as a result. ICC's guide offers a way to recognize these risks and map out a process to deal with them."

A copy of the ICC’s guide is available at:

Speech by Bank of England focuses on cyber insurance

Paul Fisher, the Deputy Head of the PRA and Executive Director of Insurance Supervision, gave a talk to the Economist's Insurance Summit in which he considered how societal changes could drive change to an insurer’s business model.

He thought the digitisation of consumer insurance is a double-edged sword. Technological advancements bring new opportunities to businesses but cyber-risk is a great concern. He said:

"As with the other risks, insurers are affected for both good and ill: with ever more frequent and increasingly sophisticated cyber-attacks on businesses and individuals, insurers are being relied upon more
and more for protection. A new business opportunity for sure. But, unlike most other insured risks, insurance firms could themselves be significant victims.

It is difficult to predict how cyber-crime – or even cyber accidents – will evolve, and it is very challenging to obtain data for losses that arise out of cyber-events. This makes it all the more difficult to quantify reserves, models and prices as well as develop operational safeguards internally.

An Insurer wishing to expand into any new business area needs to demonstrate to the PRA that new risk exposures are well understood and that the required capital for an altered risk profile has been fully considered.”

The full text of his speech is available at:

BIS updates cyber security guidance for business

The Department for Business, Innovation and Skills (BIS) has updated its cyber security guidance for business.

The advice is from security and intelligence experts across government about how to prevent the majority of cyber attacks and how to manage common cyber risk.

The guidance repeats the results of the BIS 2014 Information Security Breaches Survey, which reported that 81% of large organisations had experienced a security breach of some sort. The average cost per organisation was between £600,000 and £1.5 million.

The guidance consists of nine documents; including:

+ 10 Steps: Summary;
+ 10 Steps: Board Level Responsibility
+ 10 Steps: Executive Companion;
+ 10 Steps: Ten Critical Areas;
+ 10 Steps: Advice Sheets;
+ 10 Steps: Infographic; and

As with the other risks, insurers are affected for both good and ill: with ever more frequent and increasingly sophisticated cyber-attacks on businesses and individuals, insurers are being relied upon more and more for protection. A new business opportunity for sure. But, unlike most other insured risks, insurance firms could themselves be significant victims. - Paul Fisher, the Deputy Head of the PRA
Common Cyber Attacks:  Summary;
Common Cyber Attacks; and
Common Cyber Attacks: Infographic.

The BIS guidance is available at:

May 2015

For further information please contact:

James Hutchinson
Partner
T: +44 (0) 20 7469 0408
E: j.hutchinson@beale-law.com

Follow our cyber team on twitter @cyberclaims