CYBER SECURITY IN 2017

Data breaches in 2016

2016 was considered to be a terrible year, by many people, for many reasons. One area said to have endured a particularly troublesome 12 months was network security. According to Lewis Morgan of IT Governance, the total number of reported data breaches in 2016 was 1.6 billion. This was nearly three times the amount reported in 2015.

The substantial increase in data breaches and the changing landscape in reporting regulations suggest that 2017 is going to be a particularly significant year for cyber security.

Where is the threat?

As a society, we are becoming more and more connected. The Internet of Things means that we rely on technology for everything from storing our life savings to controlling the temperature of our kitchen. At a national level, everything from power grids and water supplies to our traffic lights are linked to a system which has the potential to be breached. Although this is of concern at an individual or company level, cyber crime is increasingly becoming a threat on a global scale.

Although most experts consider it very unlikely that any group or individual could bring about a total internet failure, there have already been examples of whole areas or countries being cut off from the internet for a period of time. This has an instant impact not only on that area, but on how that area deals with the rest of the world. Such an interruption can take days for businesses and the economy to recover.

Although a desire for financial reward is still the main motivation for cyber criminals, they are becoming increasingly aware of the value of the information that can be stolen. For example, stock markets could easily be manipulated if their data is compromised. The effect of a cyber attack may not always be instantly apparent. The alleged involvement of Russia in the recent US Presidential election is an example of the discreet, but globally significant, impact of what was reported to be state-sponsored interference. The potential levels that could be reached and the impact it could have is unprecedented. Last week, BBC news reported that Professor Richard Benham, Chairman of the National Cyber Management Centre, gave a particularly stark prediction that “in 2017 a major bank will fail as a result of a cyber attack”.

One rapidly-evolving area anticipated to see a huge increase in 2017 is ransomware. This is a very effective way for cyber criminals to make a lot of money very quickly. Data is encrypted and withheld until the victim pays the criminal a ransom. As the amounts requested are traditionally rather small, companies would often rather pay than lose access to their data. Due to their success, criminals are now increasing their demands and becoming more indiscriminate in choosing their victims. In the US, schools, hospitals and charities have all been targeted.

Why are breaches increasing so significantly?

One of the difficulties faced by those working to prevent cyber breaches is the incredibly fast pace with which cyber crime is developing and evolving. Year on year, criminals are becoming more sophisticated in the way in which they target their victims and carry out their crimes. Money that is made through cyber crime is invested back into evolving and improving the way the criminals operate. The money is used to develop the ways in which recently protected systems can be once again infiltrated and controlled. Similar to a marketing department, criminals use analytics to observe which campaigns are most successful and follow resultant trends. Once criminals have access they do everything they can to protect themselves, such as using the dark web and laundering money through bitcoin wallets.

The evolution of cyber crime is outsmarting even the most up to date firewalls. Viruses are becoming more difficult to detect and criminals are targeting those least likely to be aware of them; churches, government agencies and even police stations. Often companies or individuals do not know about a breach until it is far too late. The information that has been obtained – not only by way of stolen data but also intelligence through the successful breach - is then shared throughout the criminal network. The ease with which information can be exchanged anonymously, and the ability of groups to connect and communicate with each other across the world, means that the hackers become even better; they are quicker, more informed and generally one step ahead of those trying to stop them.

A particular example of this was provided by Raj Samani, CTO at Intel Security. When Intel Security traced back Cryptowall 3.0 - a particularly destructive form of ransomware - they discovered that the ultimate payment into just two bitcoin accounts was US $325m. Three days after the results of Cryptowall 3.0 were published, the criminals had developed Cryptowall 4.0 which was more sophisticated, more advanced and free from many of the bugs of 3.0.

Impact on the insurance industry

An increase in cyber breaches has led to an increase in the cyber insurance market. As reported in the Financial Times, the cyber insurance industry is ballooning globally. Allianz estimate the total written premium to be US$2.5 billion globally, which could reach US$20 billion by 2025. The London market

especially has predicted a big surge in cyber insurance in 2017. Inga Beale, Chief Executive at Lloyd's of London said at the end of last year *"at Lloyd's we are seeing huge cyber insurance uptake and last year we introduced 15 different types of cover just for cyber in anticipation of this demand rising in 2017*."

Although cyber risk is an emerging market, outside the USA, the market is still relatively small. With the General Data Protection Regulation coming into force in 2018 – at which time the UK will still be in the EU and therefore it will still apply - it may be that this will increase demand even further, as Europe falls more in line with the reporting obligations of the US.

The industry will face many difficulties in trying to keep up with the growing demand.

A **Lack of Data** due to under-reporting and information becoming quickly out of date makes it very difficult to analyse risk from a statistical point of view.

Coverage limits are difficult to assess. Upper limits are unpredictable and indirect losses, such as reputational loss, cannot be measured and are therefore often excluded.

The **Specific Requirements** of corporations are often unique to a specific industry, or even perhaps the company themselves, which means that the products require a great deal of customisation.

The independence of the products, the unpredictability of losses and the lack of data means losses are difficult to measure so **Pooling** is not currently available though it could be a sensible way forward.

Pooling of the risk has been considered and it would be a very effective way of sharing the data. At the moment the industry would not be able to cope with a 'cybergeddon' attack. As existing coverage is limited there would be a proportion of risks in the economy that are uninsured. The UK government is not currently able to back up what could potentially be unlimited liabilities in the event of a catastrophic cyber event that could threaten the whole economy. A combined initiative between the insurance industry and the government as they did with Flood Re (for more information please see our previous article on this topic) means the insurers' funds would be exhausted before the government is required to step in.

How to be prepared in 2017

Insurers need to be continuously refining their products to keep up with the demand for ever-changing coverage in the face of an ever-changing risk. A product will only be useful to a client if it will effectively cover them in the event of a breach. Policies that are currently in place need to be reviewed, updated and

adapted and new products need to be continuously developed to make sure they respond to the changing demands.

The market cannot predict where the new cyber threat will come from or whether it will impact at an individual, national or global level. The cyber crime marketplace is growing; it is improving and it is taking less skill and less equipment to achieve results. No company is protected. Although criminals may initially attack larger organisations with more to offer, this will eventually trickle down to businesses that are less prepared to handle the attack. Companies need to protect themselves by ensuring they have effective procedures in place in terms of staff training / awareness to prevent attacks and a suitable policy of insurance available should such preventative measures prove insufficient.

Not all policies are created equal. The insurance industry will need to continue to work hard to deliver effective solutions for policyholders faced with such repeated and varied attacks.

Samantha Wilson
Associate
T: 0203 697 1906
M: 07780 221676
E: samantha.wilson@cpblaw.com