Cyber regulation: Cyber's new rules

The tightening of data regulation next year could drive demand for cyber cover and, with the reporting of breaches becoming compulsory, it may help underwriters price this new risk ever more accurately

After a sluggish start, the need for cyber insurance seems to have finally clicked with businesses, and the market is now growing in the UK, notes Andrew Lewis, cyber underwriter at QBE: "There has been a lot of change in buyers' habits. Clients are getting to grips with what they are buying and how it would affect their businesses. This has led to an increase in buying by all sector SMEs and large corporates, the latter with big deductibles."

The UK market is picking up from a low base, notes Graeme Newman, chief innovation officer at CFC Underwriting, observing that most cyber cover is still bought in the US. But the last 18 months has witnessed three times as many submissions as last year, reports Matthew Webb, head of cyber security at Hiscox. Newman says CFC handled more than 400 cyber-related claims in 2016, a 78% rise from 2015.

"In the UK, there is no legal obligation to report data breaches to the Information Commissioner's Office unless the firm is in the financial sector," underlines Laura Irvine, an associate with BTO solicitors. "However, there will be once the EU General Data Protection Regulation is in force, from 25 May 2018."

This will be a watershed for the cyber insurance market in Europe, comments Hans Allnutt, head of cyber and data risk at DAC Beachcroft. "Breach notification laws will be harmonised. Personal data breaches across Europe will need to be notified to regulators within 72 hours and affected data subjects without undue delay. Companies will face significant costs associated with breach investigation, reporting, heightened exposures to litigation and regulatory sanctions. Cover for these financial losses is a key selling point of a cyber insurance policy."

Lewis says the new regulations will support the message insurers have been giving clients: "They will make clients focus on their risk and have responses in place. The fines will be greater but it is more about educating on the exposure." Webb says they will be a shot in the arm, but not a silver bullet.

Ransomware

In ransomware attacks, hackers encrypt data and demand money to unlock it. Between April 2015 and March 2016, the total number of users hit by ransomware increased by 17.7% to 2.3 million users around the world.

Matthew Webb, head of cyber security at Hiscox, describes "a massive increase in claims around ransomware put in a phishing email. They open the file and encrypt the software, so the business can't access data. The hackers then sell the remedy in bitcoins."

Peter Hawley, cyber underwriter at HDI Global SE, notes that ransomware has become a business model, with a relatively low value demand so the policyholder will likely pay.

Many cyber policies cover reimbursement of such extortion payments, although Dr Mark Hawksworth, cyber and technology specialist for Cunningham Lindsey, expresses the view that perhaps insurers might consider refusing to insure any client who paid in response to such a demand or at least apply terms, given the risks inherent in capitulating to such demands.

While insurers seem acutely conscious of such risks, several stressed that it is a last resort, linked to securing and backing up the IT system so future exposure is mitigated.

"The idea behind the insurance is to secure the system to avoid paying a ransom," says Andrew Lewis, cyber underwriter at QBE, who confirms that ransomware and extortion are on the rise. He says victims should inform their insurers immediately and before negotiating, while Graeme Newman, chief innovation officer at CFC Underwriting, comments: "No insurer can tell their client not to pay a ransom, which is sometimes the only strategy. Ransomware is the lowest form of this crime, the junk mail of the cyber-crime world. They are not sophisticated and attackers are targeting low-hanging fruit, and basic preventative measures need to be in place."

Kyle Bryant, regional manager for cyber risk in Continental Europe at Chubb, predicts: "If the Dutch data privacy law – effective from 1 January 2016 – is anything to go by, we can expect significant growth in interest for cyber liability cover when the GDPR becomes law. This is mainly due to the potential financial and business reputation impact of the new regulations, which include public disclosure and hefty fines." The maximum fine will be raised to the higher of €20m (£17m) or 4% of a company's global turnover.

Mark Williamson, a partner at Clyde & Co, says the obligation to report data breaches will greatly increase notification costs and those associated with reputation damage protection, as well as potentially big financial penalties for inadequate steps to protect data. This should drive up demand for specialist cyber insurance cover and the industry may be expected to plug gaps in cover.

"We see commercial pressure in the market both to innovate new bespoke cyber covers and to extend wordings as part of traditional property and casualty policies," Williamson says. "Most of the legal tests of cover have been in the US, but this is an area where the opportunities and threats to insurers are abundant. Insurers face challenging times. Much has been said about silent exposures, thresholds required for reporting breaches and the new requirements on insurers to manage risk even while modelling lags. But the industry is well prepared and in a good position to write bespoke cyber prudently and to exclude cyber risk where needed from traditional P&C policies."

An aggravating risk factor is the increasing use of cloud services by governments, businesses and individuals, creating an aggregation risk difficult to measure due to shared infrastructure, services and networks, says Rafael Sanchez, international breach response manager for Beazley. Research by Oxford University, sponsored by insurer Novae, found organisations' cyber controls not fit for purpose, including those recommended by government. This has set alarm bells ringing, and Dan Trueman, Novae's head of cyber, says much more needs to be done to understand the risk environment and prevent damage to organisations from this threat.

In denial

Small businesses seem in denial. The Hiscox 2017 Cyber Readiness Report found that, while big firms incur the highest costs in nominal terms, the financial impact of cyber attacks is disproportionately high for the smallest companies. Despite this, small businesses seem more complacent, with 29% saying they changed nothing following a cyber incident compared to 20% of larger firms.

Insurers are keen to help clients identify and manage their risks, although defining and measuring them is tricky, says Sanchez. "The attack vectors, motivations and even the threat actors are fluid and impossible to predict. Security by design is not a concept embedded in most companies' operations, so they are often reacting to these changes in the threat environment. The lag between the two leads to constantly changing risk profiles."

Webb says the key thing is to have policy wordings that pick up different industry sectors with different exposures. "For example, hotels handle personal data and credit cards, and one hotel hacker locked guests out of their rooms."

Newman says: "The technology revolution has been so fast, and we have over-complicated the message. Because it is a US-dominated market, we have marketed the cover as for data breaches whereas most issues in the UK are about ransomware." According to him, US businesses are generally more regulated and aware than those in the UK, so British companies make a proportionately greater number of claims: "We get twice as many claims per policies sold in the UK as in the US."

Until now, there has been little litigation following scandals because victims have had to show financial loss resulting from the breach. However, in Vidal-Hall v Google [2015], the Court of Appeal ruled that they could claim compensation for distress without needing to show pecuniary loss. Awards of up to £250,000 have been made, and Allnutt expects this trend to be replicated across Europe once the new GDPR rules are in force.

Lack of transparency

Irvine says lack of transparency is a big issue, and that many banks under-report data breaches. "In the US they are better at reporting and no stigma is attached," she says.

So will the new reporting duty normalise being a victim and remove the stigma that triggers the desire to cover up? "I don't think a breach will ever be normal," replies Allnutt. "They are just lose-lose situations. The trouble is that under the new rules just the act of covering up a breach can incur a sanction of up to 2% or €10m irrespective of its nature. Therefore, how a company responds to a breach will be critical in the eyes of the law and the court of public opinion."

The complexity of some attacks demands a multi-faceted incident response, which can require calling in specialists in areas like security, data forensics, public relations, reputation management and law, notes Dr Mark Hawksworth, cyber and technology specialist for Cunningham Lindsey. He describes the cyber risk as a constantly moving target.

Covering up

Is there a tendency for companies to cover up data breaches, perhaps for fear of reputational damage? Some breaches might have been concealed from insurers, and the adjuster feeds that back, but dealing with IT personnel can sometimes be tricky, Hawksworth says: "If there has been an issue with a network, the temptation for the IT team is to install the security updates, which destroys the evidence by overwriting, and makes forensic investigation difficult. They try to look at the computer before the loss adjuster gets there, and might not want to cooperate."

The adjuster has to minimise the risk for the insurer, but the IT worker could fear being in the frame and not want the adjuster to tell the boss, or it might be an outside IT contractor, who fears loss of a contract.

Peter Hawley, cyber underwriter at HDI Global SE, observes that one misconception following a cyber attack is that there has been terrible IT failure, which is often less than would be expected. "It's an attack on the company and even brilliantly advanced hi-tech companies are under threat. It does not mean the systems are sloppy because the attacks change, and the insider threat is the biggest as employees have access."

Bryant also notes the dynamic nature of cyber risk. He says Chubb works with IT security vendors to create prevention and response capability for clients, as well as advising them on how to spend their IT security budgets on 'difference-making' activity, and ensuring risk management procedures are in place in case of a data breach or cyber attack.

Nigel Teasdale, president of the Forum of Insurance Lawyers and partner at DWF, comments that covering up a breach might have been the case a couple of years ago, but the reputational risks of being seen to have engaged in a cover-up are far worse than the breach itself: "Trust is at the centre of most of the relationships a company has with its stakeholders."

The ICO's pledge to pursue non-compliant companies will help insurers, predicts Hawley. "Most breaches have third-party consequences but first-party losses, like intellectual property, fly under the radar although they affect the companies' bottom line. It's grossly under-reported. This will give a better picture of the state of the market and the value of the losses, and help insurers underwrite at a proper price, matching the cover to the risk."

Lewis agrees: "Year on year, it is becoming easier, with more data and speaking to clients. Five or six years ago, there was not much consistency across the market on pricing, but premiums are now closer."