CYBER RISK: INSURING THE DIGITAL AGE

Professor Philip Rawlings*

Abstract

The rapid rise of the digital economy presents enormous opportunities to the insurance industry but also brings huge risks, and it is the difficulty of defining those risks that has presented the greatest challenge to this sector of the market. This paper looks at the development of cyber insurance, the problems facing both policyholders and insurers, and the role that insurance can play in improving cyber security. It considers the questions of whether cyber losses fall within ordinary commercial insurance policies and the particular difficulties involved in drafting specialist cyber insurance.

Introduction

Successful businesses seek to develop products and markets, and for insurance companies and brokers this means identifying new risks and then designing and selling policies. The internet seems fertile ground for such expansion: over $8 trillion passes through the internet each year, and more than a third of the world's population is online with 5 billion networked devices and by 2018 this will have grown to half the population with 21 billion devices.[1] Networked computers are essential to most companies both in organising their businesses and as components in many products from smart phones to oilrigs.[2] But these opportunities mean that, alongside familiar risks arising from the breakdown of machinery and employee error or misdemeanour, the use of networked systems makes businesses and their products vulnerable to cyber attack. While training and cyber protection software will reduce this vulnerability, such precautions can never be entirely effective, and, in any case, the dependence on third-party software, the outsourcing of functions and the interconnection between computer systems (routed through third parties) means a company's cyber security is not completely within its control. All of which creates opportunities for the insurance industry. The problem for both policyholders and the insurance industry is that, while cyber risks are recognised as significant, they are not fully understood: what are the risks and how can they be insured?

What risk?

The types of loss that can arise from breaches of cyber security are potentially very broad.[3] The company which suffers such a breach might have to pay the cost of reconstructing a database, repairing or replacing damaged systems (such as the computers or machinery controlled by computers) and managing the response to an attack (such as investigating the problem, public relations to repair reputational damage, dealing with enquiries, notifying customers and payment providers, credit monitoring for customers whose accounts may have been compromised, and assisting with identity theft issues). Money may have been stolen or there may have been payment of a ransom for the return of data or access to data that has been encrypted by a malware programme.[4] Sales may fall as customers lose confidence in the company and the share price may drop, which, among other things, may make the company more vulnerable to takeover. There may be regulatory penalties (such as might

* Director of the Insurance Law Institute, Centre for Commercial Law Studies, Queen Mary University of London, 67-69 Lincoln's Inn Fields, London WC2A 3JB, United Kingdom. p.rawlings@qmul.ac.uk

[1] Cisco at http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html; *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (2011) at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[2] *Internet of Things: Security Stud: Home Security Systems Report* (Feb 2015) at https://www.hpfcd.com/docs/InternetOfThings.pdf.

[3] *McAfee Labs: Threats Report*, intel Security, Aug 2014 at http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf; Verizon, *2014 Data Breach Investigations Report* at http://www.verizonenterprise.com/DBIR/2014/.

[4] Swiss Re, *Is CGL Coverage Tonic for the Data Breach Blues?* (2014), p.2 at http://media.swissre.com/documents/ARM-14-04167-P1-Coverage_Tonic_Data_Breach_Blues-5-20-web.pdf.

arise from breach of data protection and anti-spam laws or regulations relating to particular industries, such as banking)[5] and associated defence expenses, and also damages arising from liability for losses suffered by third parties (such as actions for damage to customers' computer systems, or breach of contract or privacy rights, or expenditure and losses incurred by banks and credit card companies,[6] or arising from derivative actions by shareholders against directors and officers for failing to prevent or manage the problem[7]). This list is by no means closed. The continued impact of computers on product design and business organisation and personal lives means that new types of loss will emerge: the potential range of liability associated with the driverless car is only one obvious illustration – who (and whose insurer) is liable for damage caused by a driverless car (the car's owner, the designer of the software, the manufacturer of the car)?

These losses may arise in various ways. They may come from within the company through faults in the machinery or software, or the actions of naïve or corrupt insiders (such as inputting the wrong data, losing laptops or USB sticks loaded with data, opening an email attachment that contains malware, implanting malware or disclosing passwords to an outsider). They may be the result of the actions of outsiders, who want to steal money or data, spy on the company, or protest or disrupt its activities. The internet not only allows new methods of crime and mischief it is also a new way by which war and terrorism can be conducted. State security services have recognised the opportunities for spying on another country's state secrets or confidential commercial information, and for disruption, as happened with the attack in 2009 on Iran's nuclear industry.[8] A company may be targeted directly or through an employee or a third party with whom the company has close connections, or an attack may come from a "wild virus", that is, a virus released onto the internet which has no particular target but searches for vulnerable systems. All companies outsource at least some of their IT provision, including software, maintenance and data storage, and this creates vulnerability beyond the direct control of the company. Moreover, a company that provides outsourcing services is itself likely to outsource some of its work, and so on.[9] Rapid digital connections mean problems can spread to other computer users before any response is possible, and the sophistication of some hacks may make it difficult to detect when a computer system has been attacked: a breach of the payment system used by PF Chang's China Bistro chain of restaurants in the US went unnoticed for almost nine months in 2013-14.[10]

How big are the losses? The evidence is unclear as companies are reluctant to disclose breaches of security because of the impact on customer confidence and share value: for example, in spite of a report in 2015 by a leading cyber security firm that more than 100 financial firms in 30 countries had been affected by the Carbanak malware with total losses of at least $300 million, none of those firms appears to have disclosed an attack.[11] Some jurisdictions do require companies to notify third parties who may have been affected by attacks, but these laws do not usually establish arrangements for the

---

[5] FCA Handbook: Senior Management Arrangements, Systems and Controls (SYSC); Financial Conduct Authority, *Risk Outlook 2014* at http://www.fca.org.uk/your-fca/documents/corporate/fca-risk-outlook-2014. In the US, see Regulation S-P, Rule 30 (the Safeguards Rule) and SFC circular (at http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=14EC49), and Canada has the world's toughest anti-spam law, Controlling the Assault of Non-Solicited Pornography and Marketing Act (http://www.fca.org.uk/static/documents/corporate/risk-outlook-2014.pdf).

[6] In the US, Genesco, a retailer, was charged $13 million for failing to observer online security standards in breach of agreements with credit card issuers: S Kelly and V Pasquali, 'The untold cost of cybersecurity', *Global Finance*, 2 May 2013 at https://www.gfmag.com/magazine/may-2013/cover-growing-threat-the-untold-costs-of-cybersecurity-.

[7] There have been many such actions in the US, but the first to come to court was dismissed because the company had reasonable cyber security controls: *Palkon v Holmes* (US District Court, New Jersey), Civil Action 14-CV-01234 (SRC) (2014) at http://law.justia.com/cases/federal/district-courts/new-jersey/njdce/2:2014cv01234/300630/49/

[8] S Waterman, 'US-Israeli cyberattack on Iran was "act of force", NATO study found', *Washington Times*, 24 mar 2013 at http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all

[9] Eg *Recall Total Information Management, Inc v Federal Ins. Co.*, 83 A.3d 664 (Conn. App., 2014).

[10] See http://www.pfchangs.com/security/; J Greenwald, 'Travelers sues PF Chang's to avoid paying breach costs', *Business Insurance*, 13 Oct 2014 at http://www.businessinsurance.com/article/20141013/NEWS07/141019957?template=mobileart

[11] *The New York Times*, 15 Feb 2015 at http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

central collection of information.[12] To fill the gap, research has been sponsored by cyber security firms or insurers, which may (often unfairly) cast doubts on the objectivity of the work.[13] According to these figures, the annual global cost of cyber crime is $375-575bn, with a cost to the UK economy of £20 billion.[14] In its 2014 report, the Ponemon Institute[15] estimated that the annualised average cost of cyber crime to each large US company was $3.5 million, which was 15% higher than 2013, and Norton, the computer security firm, has estimated that 431 million adults around the world have been subject to cyber crime, costing them $114 billion.[16]

It is hard to relate to such figures, and perhaps the regular flow of news stories about cyber security has had a more powerful impact. In 2008, information about 130 million customers was stolen from Heartland Payment Systems, Inc., a large US payment processing company, and by 2010 the company was reported to have set aside $139.4 million to deal with the problem, including $60 million to Visa, $3.5 million to American Express, $42.8 million to meet expected settlements with other litigants and $26 million in legal fees.[17] Just before Christmas 2013 malware installed on the payments system of Target, the large US retailer, enabled hackers to gather payment card information from 40 million customers – representing more than 8% of all US debit cards issued and 4% of credit cards – with an average loss of $331 for each debit card and $530 for each credit card. The costs to Target will probably exceed $235 million and might reach $1.1 billion. The company was hit with lawsuits from customers and banks, profits fell by 46%, transactions dropped and the company's CEO resigned.[18] Between June and August 2014 hackers accessed personal information relating to 83 million customers of JPMorgan Chase.[19] That year also saw perhaps the largest security breach in terms of people affected when the personal details of 233 million eBay customers, including 15 million in the UK (just under 1 in 4 of the entire population), were stolen,[20] and 2015 began with, among others, an attack by hackers on a database of 80 million customers held by Anthem, one of the US's largest health insurer, as well as the Carbanak attack which allegedly led to unauthorised transfers and ATMs dispensing

---

[12] The Notification Regulation, Commission Regulation (EU) No. 611/2013, art.3; ICO, *Notification of PECR Security Breaches* at http://tinyurl.com/lhdtx5h; PM Schwartz and EJ Janger, 'Notification of Data Security Breaches' (2007) 105 Michigan Law Review 913; J Christianson and G Brotz, *Laws Governing Data Security and Privacy – US Jurisdictions at a Glance* (2014) at http://www.cfjblaw.com/files/Publication/b6bd2fa2-e24b-4deb-8b7b-0c6b0663e94d/Presentation/PublicationAttachment/f0ffa7be-d766-4647-9e89-2328d3436838/Laws-Governing-Data-Security-and-Privacy-Table-CFJB-ExpectFocus-Summer-2014.pdf; DACbeachcroft, *International Data Breach Law: A Comparative Guide* (2012) at http://www.dacbeachcroft.com/documents/imports/resources/pdfs/brochures/international-data-breach-law-a-comparative.

[13] Lawrence A Gordon *et al*, *2006 CSI/FBI Computer Crime and Security Survey*, COMPUTER SEC. INST. (CSI), at 2, *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf. Reporting breaches is, or may become, mandatory in sectors such as finance, which could improve statistics.

[14] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (the McAfee Report) (Jun 2014) at http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf; Airmic, *Review of Recent Developments in the Cyber Insurance Market*, p.11 at http://tinyurl.com/lcn6r58.

[15] Ponemon Institute, *2014 Cost of Data Breach Study* at http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/. Survey sponsored by IBM.

[16] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport.

[17] J Vijayan, 'Heartland breach expenses pegged', *Computer World*, 10 May 2010 at http://tinyurl.com/mx6crdm.

[18] American Bankers Association, *Target Breach Impact Survey* (Sep 2014) at http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf; http://www.dwf.co.uk/news-events/legal-updates/2014/10/is-your-business-prepared-for-cybercrime/; S Weinstein, 'How Target became a target: massive cyber security breach creates legal and reputational risk for leading US retailer' (2013) Coventry Law Journal 11.

[19] 'Another cyber attack targets Wells Fargo website', *Los Angeles Times*, 26 Marr 2013 at http://articles.latimes.com/2013/mar/26/business/la-fi-mo-wells-fargo-cyber-attack-20130326; J Kirk, 'JPMorgan Chase Breach Affected 83 million customers', PCWorld (2 Oct 2014) at http://www.pcworld.com/article/2691452/jpmorgan-chase-breach-affected-83-million-customers.html.

[20] H Wallop, 'eBay hacking: online gangs are after you', *The Telegraph*, 23 May 2014 at http://tinyurl.com/qdd44dh.

cash.[21] Other stories highlight the problems caused by clumsy, naïve or incompetent employees and machinery malfunctions. The failure in June 2012 of cash machines operated by RBS in the UK arose from a software fault, but it led to compensation payments and administrative costs of £125 million and another £56 million in fines imposed by the financial regulators.[22] The UK government seems regularly to use laptops and memory sticks, often containing unencrypted data: in 2007 two CDs with details of 25 million people were lost by HM Revenue and Customs; in the following year the Ministry of Defence mislaid a computer hard drive that held data on 100,000 armed forces personnel and 600,000 potential recruits; and in 2015 CDs containing sensitive information relating to inquiries into the deaths of Mark Duggan, Azelle Rodney and Robert Hamill were entrusted to the mail system from which they never emerged.[23] There are stories of foolish, ill informed or spiteful people who are sacked, prosecuted and/or sued for what they post on social media sites.[24] Here the concerns for a company are its potential liability for such actions by employees and the impact on its reputation. Finally, a cyber breach attracts media attention when supposedly wrapped up in the world of spying. The US media seems particularly alert to any suspicion that an attack might have come from a rival power, such as China, while stories implicating Russia can seem almost nostalgic in their echoes of the more straightforward rivalries of the Cold War,[25] and the sense of national danger is underlined by mention of CIA or FBI involvement in the investigation. Yet, China has been the victim of significant attacks, and there have been plenty allegations about US involvement in cyber espionage and attacks on various targets. Indeed, the technical sophistication of computer users in the US has meant that the most dangerous cyber attacks have come from that country.[26]

Cyber space is an area in which national commercial and security interests are advanced, exposed, attacked and defended, making cyber security a matter for public policy. In the US, President Obama has been particularly active, issuing a directive in 2013 to advance "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure",[27] and criticising Sony Pictures in 2014 for initially yielding to hackers demands not to release *The Interview*.[28] Inevitably, there has been a flood of new laws and regulations. The UK government has also consulted on the issue, the Financial Crime Alerts Service has been established to share information between government, law enforcement agencies and banks, the Bank of England's Financial Policy Committee, which overlooks the financial system, has issued warnings about the risks posed by cyber attacks, and regulators have established or tightened their oversight of cyber security.[29]

---

[21] *The New York Times*, 5 Feb 2015, 14 Feb 2015 at http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0, and http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

[22] http://www.bbc.co.uk/news/business-30125728

[23] 'Timeline; child benefits records loss', BBC News, 25 Jun 2008, at http://news.bbc.co.uk/1/hi/7104368.stm; 'Previous cases of missing data', BBC News, 25 May 2009 at http://news.bbc.co.uk/1/hi/uk/7449927.stm; *The Independent*, 29 Jan 2015.

[24] http://www.theguardian.com/media/greenslade/2014/oct/20/medialaw-social-media

[25] Eg contrast: E Nakashima, 'Foreign hackers targeted US water plant in apparent malicious cyber attack, expert says', *The Washington Post*, 18 Nov 2011 at http://tinyurl.com/8458nks, with D Poeter, 'Illinois water utility "hacked" by vacationing contractor', *PC Mag*, 1 Dec 2011 at http://www.pcmag.com/article2/0,2817,2397140,00.asp. See also, NBC News, 'FBI warns US business of China-backed cyberattacks' at http://www.nbcnews.com/tech/security/fbi-warns-u-s-businesses-china-backed-cyberattacks-n226821; DE Sanger and N Perlroth, 'New Russian boldness revives a Cold War tradition: testing the other side', *The New York Times*, 30 Oct 2014 at http://tinyurl.com/l8mueed.

[26] Insurance Europe, *Terrorist Acts against Computer Installations and the Role of the Internet in the Context of International Terrorism* (Feb 2004), p2 at http://www.insuranceeurope.eu/uploads/Modules/Publications/1225358536_annexe180.pdf.

[27] Presidential Policy Directive – Critical Infrastructure Security and Resilience, 12 Feb 2013 at http://tinyurl.com/aglp8qh; *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (2011) at http://tinyurl.com/ljj35rs; See Bank of England, Record of the Financial Policy Committee Meetings, 18 June 2013, and 8 and 15 Dec 2014, at http://www.bankofengland.co.uk/publications/.

[28] http://www.bbc.co.uk/news/entertainment-arts-30512032.

[29] British Bankers Association, News, 23 Sep 2014 at http://tinyurl.com/kusqn7w.

The media attention and the barrage of new laws and regulations puts pressure on the directors and senior executives of firms, although they may only come to realise what this means after a cyber attack when, alongside civil suits and awkward questions from shareholders and customers, they may find themselves subject to bad press and multiple investigations by law enforcement agencies and regulators, and the inability to prosecute the hacker may leave the company's directors and senior officers as the only real target for criticism.

Why don't companies take precautions?

There should be enough here to scare anyone who uses a computer, and, indeed, cyber security ranks high among those things that keep corporate risk managers awake at night – 84% of global financial institutions put it among their five highest risks in 2014, and it is top of the risk chart in Germany and second in the UK and France.[30] Some firms invest enormous amounts in security: the bank JPMorgan Chase reportedly spends $250 million a year,[31] and as early as 2011 global expenditure was said to be more than $95 billion.[32] Alongside this – although less impressive – has been the increase in spending on cyber insurance. US premium revenue for this sector rose 32% in 2014 and is approaching $2 billion, although this is still small when compared with a market total of over $1tn.[33] Elsewhere progress has been slower – UK premiums are around £150 million, but expectations are high with Allianz estimating that premium income across Europe will reach €700-900 million by 2018.[34] There is also potential for an international market like London to develop cyber products for Asia: in 2013, cyber crime was thought to have cost Japan $1 billion, Singapore $1.25 billion and China $37 billion.[35]

Yet, not everyone seems convinced about the value of insurance. A recent survey in the UK and Ireland revealed that less than a third of companies had assessed the financial impact of a cyber attack, and a mere 14% had cyber cover. More than half of the respondents did intend to buy insurance or, at least, obtain quotations in the next year, but this hardly suggests the sort of urgency that the statistics and the news stories might have been expected to generate.[36] That survey indicates a problem with ownership of the cyber risk issue. In 57% of companies anything to do with computers was regarded as a matter for whoever looked after IT provision. In other words, many firms regard computers like any other machinery or office equipment with which they carry on their business and that IT is a matter for middle management and junior employees to worry about it.[37] There are other explanations. Risk management is often seen simply as expenditure rather than as part of the assets it seeks to protect, and this makes it vulnerable to pressure on costs. Directors and risk managers may be reluctant to question IT provision because it is outside their expertise or because of resistance from IT staff, who may see it

---

[30] J Greenwald, 'Financial institutions identify cyber risk as major concern: Survey', *Business Insurance*, 23 Oct 2014. Also, *Post*, 24 Sep 2014, 15 Apr 2014; Marsh, 'Cyber gap insurance – cyber risk: filling the coverage gap' (2014) at http://uk.marsh.com/Portals/18/Documents/Cyber%20Gap%20Insurance%20Brochure_Final.pdf

[31] A Samson, 'Sophisticated bank cyber attack said to target core infrastructure', Fox Business, 28 Aug 2014 at http://www.foxbusiness.com/technology/2014/08/28/sophisticated-bank-cyber-attack-said-to-target-core-infrastructure/

[32] The value of this sector is indicated by reports that Intel paid $7.8 bn for McAfee, the security giant: http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

[33] PJ Beshar, 'Protecting America from Cyber-Attacks: The Importance of Information Sharing', testimony before US Senate Committee on Homeland Security & Governmental Affairs, 28 Jan 2015.

[34] *Cyber Liability Insurance: Market Trends Survey* (Oct 2014) at http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf; http://www.agcs.allianz.com/services/financial-lines/allianz-cyber-protect/

[35] Aon, *Cyber Exposures and Solutions in Asia: Risk Management and Insurance to Protect Your Financial Statements* (Mar 2014), p.9 at http://www.aon.com/attachments/risk-services/Asia-Cyber-Exposures-and-Solutions-032014.pdf

[36] UK & Ireland 2014 Cyber Risk Survey Report, see E Kenning, 'Marsh predicts cyber insurance rush', *Insurance Age*, 17 Jun 2014.

[37] Cited at http://tinyurl.com/l9ov7cu. See Bank of England, Record of the Financial Policy Committee Meetings, 8 and 15 Dec 2014, p10 at http://www.bankofengland.co.uk/publications/Documents/records/fpc/pdf/2014/record1412.pdf.

as a challenge to their skill and professionalism.[38] Research undertaken in the US (albeit in 2011, which is a long time ago in this area) suggested that directors were encouraged not to invest in cyber security because investors misunderstood the nature of the risk and saw security breaches as a nuisance rather than a threat to firms.[39] Of course, there is the possibility that the nature of their work leads risk managers to overestimate the risks involved in IT.[40]

Spending more on computer security is obviously one response to the threat of cyber attacks, but total security is not achievable, as JPMorgan Chase discovered. Indeed, Gordon and Loeb have argued that this is not a rational investment objective and that on average the best return involves pegging spending on cyber security at around 37% of expected losses.[41] In any case, taking out appropriate insurance cover seems sensible. Tougher regulatory regimes will help focus attention, and, in particular, changes to EU law on data protection that will broaden the category of those liable for data breaches and increase the penalties.[42] Bad news may be even more effective in promoting the purchase of better security and more insurance, which appears to have happened in the US following the losses at Target in 2013 and a ruling in 2014 that Sony's existing policy did not cover its losses. Such stories meant other companies recognised gaps in their coverage and the costs of cyber breaches.[43]

Much of the discussion around insurance leads to the conclusion, as one commentator put it, that "the biggest challenge for insurers is education and raising awareness of the risk exposures among the corporate insurance purchasing community".[44] But blaming companies for not taking out adequate cover is only one side of the story. It does not acknowledge the failure of insurers to provide suitable products at the right prices. The problem is that insurers are both excited and nervous about the opportunities. There is concern about the extent of their exposure to claims for cyber breaches under existing portfolios. Moreover, the lack of historical data means insurers (and reinsurers) face problems in determining the questions that should be asked in proposal forms, in drafting policies, in calculating premiums and in dealing with claims. There is legal uncertainty about where liability might fall. The problems posed over liability for accidents involving driverless cars have been mentioned, but these issues are already with us because modern cars are loaded with computer controlled devices – the Ford Fusion has more lines of code than the Boeing 777 Dreamliner.[45]

---

[38] Airmic, *Review of Recent Developments in the Cyber Insurance Market*, pp.4-5 at http://tinyurl.com/lcn6r58.

[39] LA Gordon, MP Loeb and L Zhou, 'The impact of information security breaches: has there been a downward shift in costs?' (2011) 19 Journal of Computer Security 33.

[40] J Adams, 'Cars, cholera, and cows: the management of risk and uncertainty', Policy Analysis, 4 Mar 1999, 335.

[41] LA Gordon and MP Loeb, 'The economics of information security investment,' *ACM Transactions on Information and System Security*, Nov 2002, 438.

[42] EU Data Protection Regulation (COM(2012) 11 final) extends liability to data processors: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. The proposed EU Network and Information Security Directive will also increase reporting requirements: Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (2013/0027(COD)), 13 Mar 2014 at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244. For EU strategy, European Parliament Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)), 12 Sep 2013 at http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2013-0386&language=EN; P Ryan, P Buckenham and N Donnelly, 'EU Network and Information Security Directive', The IT Law Community (24 Oct 2014) at http://www.scl.org/site.aspx?i=ed39127.

[43] L Thomas and J Finkle, 'Insurers struggle to get grip on burgeoning cyber risk market', Reuters, 14 Jul 2014 at http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714; *Cyber Liability Insurance: Market Trends Survey* (Oct 2014) at http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf. For the Sony case, see below.

[44] N Burridge, 'Asian countries most at risk from cyber crimes', *Post*, 4 Jul 2014.

[45] http://www.roadandtrack.com/car-culture/a7114/the-business-end-raj-nair-ford/; E. Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drives at Risk* (Feb 2015) at http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

The rapid growth in this part of the insurance market seems to suggest that change is occurring. Companies are starting to recognise the need to respond to cyber risk, and this may indicate that insurers are offering cost-effective products which more closely meet customers' requirements,[46] although it may simply be that companies have become sufficiently concerned about an attack that they are buying products even though they are not entirely suitable or are too expensive.

Insurance of cyber risk in US

The broad nature of the losses arising from cyber risks means they may fall within a company's existing insurance. This will, of course, depend on the terms of the particular policies, but, while the principles of contract construction may be clear, they are not always easy to apply, and as yet there is little UK case law.[47] Litigants have been rather more active in the US, although reference to these cases comes with the usual health warnings associated with attempts to transpose judicial decisions from one jurisdiction to another. Aside from variations in policy wordings, the UK courts may use different rules of construction or apply similar rules differently from US judges, and each state has its own insurance law jurisdiction. In addition, many US cases involve the insurer's obligation under the policy to defend claims brought against the policyholder and a ruling that there is a duty to defend does not necessarily imply liability for a claim because it is triggered where there is the potential for coverage.[48] It should also be remembered that insurance cases are often fact specific.

Most US case law on cyber coverage involves Commercial General Liability (CGL) policies, which follow the model drafted by Insurance Services Office, Inc. (ISO), an industry body. Coverage A in CGL policies provides cover where the policyholder is legally obliged to compensate for injury or property damage suffered by third parties that arises out of the policyholder's business. Property damage includes "Physical injury to tangible property, including all resulting loss of use of that property" and "Loss of use of tangible property that is not physically injured" (CGL, Section IV, cl.17). The US courts have generally taken the view that electronic data is not tangible property because, "Alone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance."[49] Thus, the theft of email addresses or the corrupting of data is not tangible loss.[50] On the other hand, in *Retail Systems, Inc. v CNA Insurance Companies*,[51] it was held that a claim, which arose when the policyholder lost a client's computer tape, could include the full value of the data recorded on that tape because it formed part of the physical property. The Louisiana Supreme Court took an even broader view, ruling in *South Cent. Bell Telephone Co v Barthelemy* that "tangibility is not a defining quality of physicality", and, therefore, that electronic data is tangible because "it can be observed and altered through human action".[52] The other problem is to determine what constitutes physical injury. US courts have tended to take the view that this includes permanent or even temporary loss of access to computer services: "Because a computer clearly is tangible property, an alleged loss of use of computers constitutes 'property damage' within the meaning of plaintiff's policy."[53] In *Sony Computers Entertainment Am., Inc. v American Home Assurance Co*,[54] a CGL policy covered those sums Sony became legally obliged to pay as a result of "physical injury" to tangible property "including loss of use of that property", but excluded damage or loss arising from a defective Sony product. The insurer had no duty to defend when customers sued for losses arising from a design flaw that meant its

---

[46] Airmic, *Review of Recent Developments in the Cyber Insurance Market* at http://tinyurl.com/lcn6r58.
[47] See below for *Tektrol Ltd v International Insurance Co of Hanover* [2005] EWCA Civ 845.
[48] *Black v Goodwin, Loomis & Britton, Inc*, 239 Conn 144 (Conn, 1996); *Liberty National Enterprises, LP v Chicago Title Insurance Co*, 217 Cal App4th 62 (Cal App 2 Dist, 2013).
[49] *State Auto Property and Cas Ins Co v Midwest Computers*, 147 F Supp 2d 1113, 1116 (WD Okla, 2001), Alley DJ.
[50] *Liberty Corporate Capital Ltd v Security Safe Outlet, Inc*, 937 F Supp 2d 891 (ED Ky, 2013). Also *Magnetic Data, Inc v St Paul's Fire and Marine Ins Co*, 442 N W2d 153 (Minn 1989); *Cincinnati Ins Co v Professional Data Services, Inc*, 2003 WL 22102138 (D Kan, 2013).
[51] 469 NW2d 735 (Minn App, 1991).
[52] 643 So2d 1240 (La., 1994) at 1246. Also, *Landmark American Ins Co v Gulf Coast Analytical Laboratories, Inc*, 2012 WL 1094761 (M.D. La., 2012).
[53] *State Auto Property & Casualty Insurance Co v Midwest Computers*, 147 F Supp2d 1113, 1116 (WD Okla, 2001), Alley DJ. But see *Vonage Holdings Corp v Hartford Fire Ins Co*, 2012 WL 1067694 (D.N.J., 2012) where the issue was unresolved.
[54] 532 F3d 1007 (CA9 (Cal), 2008).

PlayStations would not play certain DVDs and game discs, contrary to advertising claims made by Sony. The court held that the policy only covered "loss of use" caused by a third party's product. The result would, therefore, have been different if defective DVDs supplied by a third party had damaged the units or the units had damaged the DVDs. In *Recall Total Information Management, Inc v Federal Ins. Co.*,[55] 130 computer tapes containing data relating to 500,000 IBM employees fell off the back of the truck on which they were being carried by the sub-contractor used by Recall, a data management company hired by IBM. IBM sued Recall for $6 million to cover the cost of notifying the employees as required by state law. Curiously, the court held that Recall could not recover this sum under its CGL policy because it was not compensation for loss suffered by the employees since the objective of the state law was to enable the employees to protect themselves against the risk of loss through, for example, identity theft and not to compensate them for such loss. One of the issues in *Eyeblaster, Inc. v Federal Insurance Co*[56] involved the way loss was inflicted. The policy did not cover liability arising from an "intentional wrongful act", but this did not exclude liability where the policyholder intentionally installed software on the third party's computer, which ultimately caused damage, as part of its ordinary course of business because this was not shown to be an "intentional wrongful act".

Coverage B in CGL policies covers liability for personal or advertising injury arising out of the insured's business. This includes defamation, disparaging someone's goods, products or services and violation of privacy rights. In *Netscape Communications Corp v Federal Ins Co*,[57] the insurers had a duty under the policy to defend where software used by the policyholder collected data from those accessing the policyholder's website in breach of their privacy rights, and in *Tamm v Hartford Fire Ins Co*[58] the duty was triggered where the policyholder was sued for breaching confidentiality in obtaining access to the emails of a company for which he had worked. Courts have tended to distinguish between secrecy and seclusion so that liability for breach of a third party's right not to have confidential information disclosed falls within Coverage B cover, but liability for breach of a statutory right not to receive unsolicited emails or faxes does not.[59] A key issue is often whether there has been publication,[60] but the courts have been generous in their construction of this requirement. There does not have to be disclosure to the public at large or even to a substantial group of people. The court in *Tamm* held that there would be publication even if the disclosure was only between employees at the same company, and in another case there was publication where the disclosure was to the person whose statutory right to privacy had been breached.[61] In *Travelers Indemnity Co of America v Portal Healthcare Solutions LLP*,[62] a health care company allowed public access to medical records held on a computer, but no one viewed them. The policy did not define "publication", and the court concluded that there was no need for the claimant to show that the records had been read by an unauthorised person:

> "Publication occurs when information is "placed before the public," not when a member of the public reads the information placed before it. By Travelers' logic, a book that is bound and placed on the shelves of Barnes & Noble is not "published" until a customer takes the book off the shelf and reads it. Travelers' understanding of the term "publication" does not comport with the term's plain meaning, and the medical records were published the moment they became accessible to the public via an online search."[63]

On the other hand, publication of confidential information by a hacker rather than the company or its employee may not be covered. In *Zurich American Insurance Co v Sony Corp of America*,[64] the policy

---

[55] 2012 WL 469988 (Conn Super, 2012), 83 A3d 664 (Conn App, 2014).
[56] 613 F3d 797 (CA8 (Minn), 2010). But, *Union Pump Co v Centrifugal Technology, Inc*, 2009 WL 3015076 (W.D.La., 2009).
[57] 2007 WL2972924 (ND Cal, 2007).
[58] 16 Mass L Rptr 535 (Mass Super, 2003).
[59] *Resource Bankshares Corp v St Paul Mercury Ins Co*, 407 F3d 631 (4th Cir 2005); *Cynosure, Inc v St Paul's Fire & Marine Ins Co*, 645 F3d 1 (ist cir., Mass., 2011); *Owners Ins Co v European Auto Works, Inc*, 695 F3d 814 (C.A.8 (Minn.), 2012).
[60] *Recall Total Information Management, Inc v Federal Ins Co*, 83 A3d 664 (Conn App, 2014).
[61] *Zurich American Ins Co v Fieldstone Mortgage Co*, 2007 WL 3268460 (D Mid, 2007).
[62] 2014 WL 3887797 (ED Va, 2014). See also, *Hartford Casualty Insurance Co v Corcino & Associates*, 2013 WL 5687527 (US Dist Ct, Calif, 2013).
[63] *Ibid* at 5, Gerald Bruce Lee DJ.
[64] No 651982/2011 (NY Sup Ct, 2014).

covered "oral or written publication, in any manner, of material that violates a person's right of privacy", but this was not triggered when hackers stole private data of around 100 million customers of Sony, leading to 64 class actions, because the policy only covered publication by Sony. The phrase "in any manner" referred to the medium of publication, not its origin. Moreover, in *Creative Hospitality Ventures, Inc v United States Liab. Ins.*,[65] it was held that the issue of a credit card receipt, which showed more than five digits of a credit card number or the expiry date, was not a publication.

Cyber losses may fall within the terms of other types of US policy. First-party insurance should cover damage to the policyholder's computers, while business interruption insurance is usually triggered where property damage has caused a loss of earnings. In *American Guarantee & Liability Ins Co v Ingram Micro, Inc*,[66] the policy relating to property and business income insurance covered "all risks of direct physical loss or damage from any cause", and the issue was whether this included loss when the policyholder's computers crashed because of a power cut. The judge concluded, consistently with the view taken in cases on CGL policies. "that 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[67] Similarly, in *NMS Services, Inc v Hartford*,[68] deletion of data held on a computer constituted property damage. In *Lambrecht & Associates, Inc v State Farm Lloyds*,[69] the court decided that loss of revenue was covered when a virus meant the computer had to be replaced and data re-entered. The policy covered, among other things, loss of business income caused by "accidental direct physical loss" to the policyholder's business property, and the court held that, although the introduction of the virus was the deliberate act of a hacker, from the policyholder's point of view it was "an unexpected and unusual occurrence" and, therefore, an accident. A crime policy was the subject of the decision in *Retail Ventures, Inc v National Union Fire Ins Co of Pittsburgh, Pa*.[70] Hackers gained access to a retailer's computer system and downloaded the bank account and credit card details of more than 1.4 million customers, which were then used for fraudulent transactions. As a result, the retailer notified customers, paid their losses and those of Visa/MasterCard, met legal fees arising from investigations by various state attorneys general and the Federal Trade Commission, and hired public relations consultants. Although a first-party policy, the court held that it covered these third party liabilities because it was expressed to include losses arising "directly from… [t]he theft of any Insured property by Computer Fraud". Some policies contain exclusion clauses that, while not specifically referring to cyber risk, will, nevertheless, prevent claims for such losses. D&O insurance typically excludes losses from privacy breaches and, therefore, may create difficulties for directors facing a derivative action for losses suffered by the company through a cyber privacy breach. The decision in *Tagged, Inc v Scottsdale Ins. Co.*,[71] involved a D&O policy that did not cover the provision by the policyholder of professional services. This excluded liability where a social networking site falsely advertised features to protect teenage users from sexually explicit content because, as operator of the site, Tagged provided professional services in determining its content, since this required the exercise of skill, and, even though users did not pay expressly for this service, advertising by the company of it efforts to protect against certain content was done to attract users and thus increase revenues.

US insurance companies resist strongly the idea that CGL policies are intended to cover cyber risk.[72] While perfectly reasonable if based on the wording of the policies, a less convincing argument has been made that policies were not intended to cover risks which were not foreseen at the date the ISO models were drafted or the policies themselves were entered into. The purpose of insurance is to cover unforeseen risk and that must include types of risk that are unforeseeable at the time of the policy. The fact that these risks were not priced in may have a serious impact on the insurers, but this is irrelevant to a court seeking to determine the meaning of the policies.

---

[65] 444 Fed. Appx. 370 (11th cir., Fla., 2011).
[66] 2000 WL 726789 (D Ariz, 2000).
[67] *Ibid*, at 2, Marquez SDJ.
[68] 62 Fed Appx 511 (CA4 (Va), 2003).
[69] 119 SW3d 16 (Tex App,2003). Contrast with *Union Pump Co v Centrifugal Technology, Inc*, 2009 WL 3015076 (W.D.La., 2009), discussed above.
[70] 691 F3d 821 (CA6 (Ohio), 2012).
[71] 2011 WL 2748682 (S.D.N.Y., 2011).
[72] J Greenwald, 'Insurers fight to bar cyber coverage under commercial general liability policies', *Business Insurance*, 26 Oct 2014 at http://tinyurl.com/m2ygpfl.

Excluding cyber risk

CGL policies now exclude damage "arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data" (Coverage A, Exclusions cl p).

> "For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment" (CGL, Sec IV, cl 17).

The decision in *Zurich American Insurance Co v Sony Corp of America*,[73] although favourable to the insurer, led the ISO to clarify these provisions by expressly excluding loss arising out of "any access to or disclosure of any person's or organization's confidential or personal information", which is defined broadly as non-public information, including personal data, trade secrets, customer lists and payment data.

Policies in the London market also routinely exclude liability for cyber risk. For example:

> "1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
>
> 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile."[74]

The exclusion clause developed by the Non-Marine Association focuses on damage or loss of data:

> "This Policy does not insure, loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss"[75]

Of course, the effectiveness of policy exclusions and limitations depends on the drafting. In the US case, *Eyeblaster, Inc. v Federal Insurance Co*,[76] the policy excluded losses of "software, data or other information that is in electronic form", and this denied cover for liability when a customer's personal computer was damaged after a visit to Eyeblaster's website, but the insurer was liable under another term relating to "loss of use of tangible property that is not physically injured", which did not exclude cyber losses. The changes to CGL policies mentioned above should prevent a repeat. The effect of exclusion clauses was the main issue in *Tektrol Ltd v International Insurance Company of Hanover Ltd*,[77] which was that rare animal, an English case on whether cyber losses were covered by an insurance policy. T had sensibly made five copies of a source code used in their computer-controlled energy saving devices: at their premises, the code was stored on two computers and in hard copy; it was on the managing director's laptop; and it was on a computer at a remote site operated by an independent company. In a coincidence of circumstances that is not adequately described by calling it unfortunate, all the copies of the code were lost within a period of a few days: the laptop and remote computer were infected by the Christmas Card virus, and the two computers and the hard copy were

[73] No 651982/2011 (NY Sup Ct, 2014).
[74] Institute Cyber Attack Exclusion Clause (CL380 clause).
[75] Electronic Data Endorsement A (NMA 2914).
[76] 613 F3d 797 (CA8 (Minn), 2010).
[77] [2005] EWCA Civ 845. Thanks to Professor Rob Merkin QC for drawing this to my attention.

stolen. Whether or not T could claim depended on the meaning of a clumsily drafted all-risks policy. It had a short insuring clause and a long list of exclusions, prompting Carnworth LJ to remark, "Although it is described as an 'all risks' policy, one has to search long and hard, through a bewildering and apparently comprehensive list of exclusions, to discover the extent to which any risks are in fact covered."[78] The case demonstrates how this method of drafting can backfire. Carnworth LJ took the view that, "One should start from the presumption that the parties intended an 'all risks' policy to cover all risks",[79] and this led the court to construe the exclusion clauses narrowly. One of these excluded "erasure loss distortion or corruption of information on computer systems… or software caused deliberately by rioters strikers locked-out workers persons taking part in labour disturbances or civil commotion or malicious persons". The computer virus was a wild virus and the court held that it was not excluded because the reference to "rioters" and so forth and also to deliberate actions indicated an intention to exclude only attacks directed at the computer.

Insuring cyber risk in the UK

Cover for cyber risk may be offered by an extension to an existing policy, although the benefits are likely to be limited, or a policy that fills gaps in existing cover created by exclusion clauses, [80] or a standalone policy. Cyber insurance may cover first-party and third-party risks. First-party risks include damage to, or loss of, the policyholder's digital assets, such as data and software programs, revenue loss caused by interruption of service, extortion, reputational damage, and theft of digital assets, such as computer equipment, or money. Third-party risks include liability arising from harm to digital assets, defamation and privacy breaches and where the policyholder has a contractual duty to indemnify against losses caused by an outsourcer.

The US has a fairly well developed range of policies, but other markets are beginning to catch up. Increasing numbers of UK and European insurers now offer small businesses a relatively low cost, standardised product for first-party losses with low limits on claims and no cover for reputational damage and crisis management, or third-party liability. Medium and large companies, in particular those holding large amounts of personal data on third parties or employees will need broader cover. There has been a tendency to draft policies in vague language, or to omit clear definitions, or to narrow the scope of liability by using wide exclusion clauses and low indemnity limits.[81] This may lead the unwary or poorly advised to take out coverage that has significant gaps, making it important to use a specialist broker.

The first issue is whether the policy is appropriate for the way in which the policyholder conducts its business. Where employees work away from the office, the policy might need to cover data storing on mobile devices.[82] Outsourcing activities, such as the use of data storage companies and IT contractors, can present difficulties because insurers may be unwilling to cover risks that fall outside the control of the policyholder. This means the company must be confident that the outsourcer has adequate security[83] and insurance cover that will respond to the losses that might arise. If the policy covers business interruption, does it include interruption of service caused by any criminal or regulatory investigation that follows a cyber breach? Policies often cover only attacks directed at the policyholder by hackers and, therefore, not losses caused by the failure of an internet service provider or by "wild viruses". There will be exclusions for the criminal or intentional actions of "the insured". The "insured" may be defined narrowly as senior executives and directors, but some policies use a very wide meaning that includes all employees, current and former, which severely limits their value.

The policy may indemnify the policyholder for payments made to a hacker in order to prevent an attack, restore a damaged system, or recover or unencrypt data, as long as the insurer has given prior

---

[78] *Ibid*, at [20].
[79] *Ibid*.
[80] Eg Cyber gap policies developed by Marsh, 'Cyber gap insurance – cyber risk: filling the coverage gap' (2014) at http://tinyurl.com/o7yjumv.
[81] *Tektrol Ltd v International Insurance Co of Hanover* [2005] EWCA Civ 845.
[82] For failings of UK companies regarding personal devices: B Norris, 'Majority of UK companies failing to manage BYOD and cloud computing risk', *Commercial Risk Europe*, 26 Jul 2013.
[83] Data Protection Act 1998, Pt II, para 7(a); Data Sharing Code of Practice at http://tinyurl.com/qy2kkmb.

consent.[84] But is this enforceable? The payment may be characterised not as responding to a ransom demand or extortion but as a fee to someone who is negotiating with the criminal.[85] Yet, even ransom payments are not illegal at common law. In a case involving maritime pirates, Rix LJ said, "there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages."[86] That was so even though he acknowledged that such payments encouraged and funded further acts of piracy. He did, however, qualify this by adding that, "It may be that the position with regard to terrorists is different."[87] Legislation has made the position less clear. The Proceeds of Crime Act 2002, s328(1), makes it an offence for someone to become involved in an arrangement that they know or suspect facilitates the acquisition, retention, use or control of criminal property by another, and criminal property is property that is, as the defendant suspects, a benefit from crime (s340). A ransom payment is criminal property in the hands of the criminal, but probably not when being collected together by the payer. Collecting the money without consent from the appropriate authority could constitute money laundering, but the Crown Prosecution Service might not regard it as in the public interest to prosecute where the only failure was not obtaining consent.[88] The law on terrorism is stricter. Under the Terrorism Act 2000, s17, it is an offence to make a payment where there is reasonable cause to suspect the money may be used for terrorism. That act has been amended by the Counter-Terrorism Act 2015, which makes it an offence for an insurer to make a payment "in respect of any money or other property that has been, or is to be, handed over in response to a demand made wholly or partly for the purposes of terrorism" (s42(1) inserting s17A(1)(c)). Criminal liability extends to any director or senior employee where the payment is made with his or her consent or connivance or is attributable to his or her neglect (s 42(1) inserting s17A(2)). Commercial property insurers offer limited terrorist cover,[89] but it is clearly important that any cyber policy does not include ransom payments to terrorists; indeed, since it can be difficult to identify who is making the demand, the legislation may make insurers more cautious about providing such cover.

A policy may cover fines imposed on the policyholder and costs arising from prosecution or an enforcement action, but is such insurance lawful? A properly drafted policy will only provide cover if it is legal to do so in the relevant jurisdiction, and will usually refer only to fines imposed by a regulatory authority rather than a court. In English law, financial firms cannot obtain indemnity against penalties imposed by the Prudential Regulation Authority or the Financial Conduct Authority.[90] Aside from this, whether it is possible in English law to indemnify someone against the consequences of their criminal act depends on the nature of the crime and the connection between that act and the loss. In *Gray v Thames Trains*,[91] Lord Hoffmann referred to the *ex turpi causa non oritur actio* defence as "a special rule of public policy".

> "In its wider form, it is that you cannot recover compensation for loss which you have suffered in consequence of your own criminal act. In its narrower and more specific form, it is that you cannot recover for damage which flows from loss of liberty, a fine or other punishment lawfully imposed upon you in consequence of your own unlawful act. In such a

---

[84] The policy will allow the insurer to revoke cover for extortion if the policyholder discloses that such cover exists.

[85] This issue arose during negotiations by the Tate Gallery for the return of two paintings by Turner. Indeed, the High Court held that as trustees of the paintings the Tate had a legal obligation to effect their recovery, which might include paying the criminals: http://www.tate.org.uk/about/press-office/press-releases/consent-order-enables-tate-put-documents-relating-stolen-turners; S Nairne, *Art Theft and the Case of the Stolen Turners*, London: Rektation Books, 2012.

[86] *Masefield AG v Amlin Corporate Member Ltd* [2012] 1 WLR 2012 at 2033-34.

[87] *Ibid* at 2034.

[88] See the discussion on 'The law in the UK on ransom payments' in *Money Laundering and the Financing of Terrorism* (2009), appendix A at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/9031112.htm.

[89] Under Pool Re, the insurer covers losses up to a threshold and beyond that cover is provided by the scheme: http://www.poolre.co.uk/. For an early discussion of the issues, Insurance Europe, *Terrorist Acts against Computer Installations and the Role of the Internet in the Context of International Terrorism* (Feb 2004), p2 at http://www.insuranceeurope.eu/uploads/Modules/Publications/1225358536_annexe180.pdf.

[90] General Provisions, GEN 6.1.5R.

[91] [2009] 1 AC 1339.

> case it is the law which, as a matter of penal policy, causes the damage and it would be inconsistent for the law to require you to be compensated for that damage."[92]

Recently, in *Les Laboratoires Servier v Apotex Inc*,[93] Lord Sumption explained that the narrower form operates automatically where the loss is either a penalty imposed by a criminal court or a consequence of that penalty and that application of the broad or narrow form does not depend on "the court's assessment of the significance of the illegality, the proportionality of its application or the merits of the particular case."[94] In *Safeway Stores Ltd v Twigger*,[95] which involved a breach of competition laws, the Court of Appeal rejected the argument that the rule could not apply to a company because it acts through human agents.[96] However, the *ex turpi causa* rule "only applies where the illegality is personal to the company, not vicarious", [97] and it was significant, therefore, that the relevant legislation placed liability on the company and not on those employees or directors who decided to break the law. This would lead to the conclusion that a company could not insure a penalty imposed for an offence under the Data Protection Act 1998 because liability is fixed on the controller of that data, which would be the company.[98] On the other hand, the company can insure against penalties arising as a result of vicarious or strict liability because, although it might be assumed that the purpose of attaching strict liability is to encourage companies to organise their affairs in ways that avoid liability and that, therefore, the lack of intention is unimportant, this is not the case.[99] Lord Sumption explained that the *ex turpi causa* defence will apply to "a limited category of acts which, while not necessarily criminal, can conveniently be described as 'quasi-criminal' because they engage the public interest in the same way."[100] This includes cases of "dishonesty or corruption" and breaches of "statutory rules enacted for the protection of the public interest and attracting civil sanctions of a penal character", such as competition rules,[101] but not situations where "the claimant was not aware of the facts making his conduct unlawful" because these are not acts of moral turpitude.[102] In *Osman v J Ralph Moss Ltd*, [103] a motorist was able to recover from his insurance broker the fine imposed when he was convicted of the strict liability offence of driving without insurance where this was the consequence of the broker's gross negligence in recommending a policy issued by a company whose finances were known in the market to be fragile. Phillimore LJ emphasised that the motorist "incurred that liability through no fault, no negligence or dishonesty on his part."[104] The *ex turpi causa* rule will not apply if there is no causal connection between the expenditure and the criminal or quasi-criminal act. In *Safeway Stores Ltd v Twigger*,[105] the company could not recover costs incurred in relation to the investigation by the Office of Fair Trading because these were a direct consequence of the offence. A cyber policy could, however, cover the costs of an unsuccessful prosecution or expenses arising as the result of a penalty. A driver, who may not be able to insure against a motoring fine, can take out a policy that provides a chauffeur if the driver is disqualified – if this were not the case the motorist would not be able to travel by bus. A company could insure for the costs associated with responding to the impact of a prosecution on its reputation, or investigating the source of the problem.

---

[92] *Ibid* at [29].
[93] [2014] 3 WLR 1257.
[94] *Ibid* at [19].
[95] [2010] EWCA Civ 1472. Also, *Askey v Golden Wine Co Ltd* [1948] 2 All ER 35.
[96] See *Meridian Global Funds Management Asia Ltd v Securities Commission* [1995] 2 AC 500.
[97] See *Stone & Rolls Ltd (in liquidation) v Moore Stephens* [2009] 1 AC 1391 at [27], Lord Phillips.
[98] Eg Data Protection Act 1998, ss1(4), 4(4), 55A. Individuals may commit an offence where the data breach is committed with the consent or connivance of, or is attributable to any neglect by, any director or senior officer of the company: s60(1). The proposed EU Data Protection Regulation (COM(2012) 11 final) extends liability to data processors: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[99] *Arab Bank plc v Zurich Insurance Co* [1999] 1 Lloyd's Rep 262. For the US, see *American Family Mut. Ins Co v CMA Mortg, Inc*, 2008 WL 906230 (SD Ind 2008); *Hartford Casualty Insurance Co v. Corcino & Associates*, 2013 WL 5687527 (CD Cal, 2013).
[100] *Les Laboratoires Servier v Apotex Inc* [2014] UKSC 55 at [25].
[101] *Ibid*.
[102] *Ibid* at [29].
[103] [1970] 1 Lloyd's Law Reports 313.
[104] *Ibid* at 320.
[105] [2010] EWCA Civ 1472. Also, *Askey v Golden Wine Co Ltd* [1948] 2 All ER 35.

The cyber security measures the insured has in place will influence a decision to offer cover, and, if cover is granted, liability will normally be contingent on the policyholder maintaining security. The proposal for insurance will doubtless ask about existing arrangements and any history of security breaches, and the premium may be reduced where the company has either met certain standards or, on renewal, has not claimed. The insurer may require a security audit before granting cover or after a breach, although this could present difficulties if it involves giving access to confidential data relating to third parties. What constitutes adequate security? There may be terms requiring regular data back-ups, data encryption, changes of passwords (particularly, where there has been unauthorised access), anti-virus protection and proper firewalls. The policyholder may be required to vet staff carefully, provide training, have arrangements for staff that leave the company, and plan for security incidents, including disaster recovery and business continuity arrangements. The difficulty in drafting such terms with any real precision is the lack of a universally accepted industry standard for cyber security.[106] This means insurers tend to fall back on vague language under which the insured is required, for example, "to take all reasonable steps to use and maintain data security". Presumably, this involves asking what a reasonable person in the position of the insured would have done. What if security is breached at a time when the policyholder knows the relevant virus software has a vulnerability which the supplier has not been able to address? This would depend on whether it is reasonable for the insured to continue using the software and would include consideration of issues such as the consequence of shutting down the insured's system and the difficulty of replacing the security system. One variant of this problem arises from the way non-security software companies seek to encourage the purchase of new software – and avoid the expense of maintaining earlier versions – by withdrawing support from the existing product. Microsoft's decision to discontinue support for the Windows XP operating system created significant difficulties for Lloyds and HSBC because it ran their ATMs so these machines became more vulnerable and their continued use may have breached cyber policies.[107] Cyber policy wording that refers to "any program that protects" might be construed as meaning only a program dedicated to security rather than one with another function because the protection in non-security software is designed primarily to ensure the smooth operation of that software and not to protect a computer system.

In respect of claims for third-party liability, the policy may be written on an occurrence basis, which requires only that the incident happened during the policy period and means the claim may be made after the policy has expired. Normally, it will be on a claims-made basis, that is, the policy responds only if a claim is known to the policyholder and reported to the insurer during the policy term. The concealed hack, such as the Red October malware,[108] which was undetected for five years, will be covered if it first comes to the attention of, and is reported by, the insured during the policy period. The obligation to notify will usually arise only if the insured has actual (rather than constructive) knowledge of a problem, but what does the policy say about the person within the company who must have this knowledge? The policy may oblige the insured to report if a "loss is likely" or a "loss may arise" and these wordings will usually broaden the incidents that must be reported beyond those triggered by the word "claim".[109] The policy will normally state that the obligation to fulfil this notification requirement is determined by the standard of the reasonable person engaged in a similar business. There may be a provision which allows notification after the policy has expired of an incident that occurred during the period of cover, although such extensions are usually relatively brief. Another possibility is retroactive or prior acts coverage under which the policy covers events occurring (but not known to the insured) during a stipulated period before the commencement of the policy. The insured must observe notification requirements. Notification is often required to be "promptly" or "as soon as practicable", and this may be combined with a specified maximum time period, such as 14 days. The insurer might argue that what constitutes such a period should be assessed in light of the security

---

[106] BIS, *UK Cyber Security Standards: Research Report 2013* (2013) at http://tinyurl.com/nn73sss; *Cyber Essentials Scheme: Assurance Framework* (2014) at http://tinyurl.com/mo5zr6w; Industry standards may be enforced through contract: eg Payment Card Industry Security Standards Council at https://www.pcisecuritystandards.org/organization_info/. In 2011, the Information Commissioner's Office (UK) warned that retailers not observing these standards risk enforcement action: http://www.bryanandarmstrong.co.uk/ard/enews_article.asp?ID=2646&AID=1437&CID=2

[107] Around 10% of UK businesses use XP: K Marriner, 'Caution urged against widescale exclusions in cyber policies', *Post*, 16 Apr 2014.

[108] http://tinyurl.com/buo6ttz.

[109] *Rothschild Assurance Plc v Collyear* [1998] C.L.C. 1697 at 1717-1720; *Barnes v QBE Insurance (International) Ltd* [2011] NZHC 285.

measures a reasonable policyholder would have had in place, although compliance with a term on security would presumably be sufficient, and, as has been mentioned, liability will usually be contingent on reasonable security. What is the consequence of the failure to notify?[110] This will depend on whether the policy stipulates that liability is contingent on notification. This is a matter of contract construction, but if there is no express provision to this effect, the court is likely to take the view that the insurer must perform its obligation, which is to pay claims, subject to any counterclaim for losses caused by the policyholder's breach of contract.[111]

Beyond notification provisions the policy will oblige the policyholder to cooperate with the insurer in defending any action and asserting any rights the insurer acquires, such as rights of subrogation and contribution. There is some evidence that US insurers, who are anxious to promote the benefits of cyber insurance, are pursuing actions against those alleged to be responsible for security breaches, such as website designers, rather than defending claims by policyholders.[112] The terms of the policy will, usually, allow the insurer to settle a claim and require the policyholder not to admit liability or disclose the amount of cover or incur defence costs without the consent of the insurer. Such prohibitions may be contrary to the best interests of the policyholder, who may be anxious to inform customers, and may be ineffective as in breach of a legal obligation to inform customers or a regulatory authority.[113] Policies will have deductibles and a limit on the indemnity. These could lower the premium or be all that is on offer, but may leave the policyholder with inadequate cover, and, indeed, one reason some US companies turned to their general commercial insurers following a cyber breach was not because they failed to take out specialist cover but because it was rapidly exhausted.[114] As well as an overall limit to cover, there are likely to be sub-limits for particular losses or expenses, such as defence costs, investigation, public relations and crisis management, and, since the need for these seems so much more remote at the time of the policy than loss of computer service, policyholders may accept those limits without realising that such costs can be substantial. There is also the problem of how deductibles and limits are applied. Where the hacker accesses confidential data relating to 10,000 customers, is this one loss or 10,000 separate losses? The policy will normally seek to link events that have the same cause or that lead to a single loss or that form a continuous series of related losses.[115]

Ensuring cyber security?

The market for cyber insurance is developing rapidly, but it is experiencing the problems associated with a new product. Some insurers have been rightly cautious. They are aware of the difficulty of determining the extent of liability and fearful of repeating the experience of employers' liability insurers in relation to asbestos-related diseases. As a result, those customers that recognise the need for insurance can struggle to find a product that is suitable and affordable or that will keep pace with the rapidly changing nature of cyber risks and security.

Nevertheless, as with previous economic revolutions, insurance has a fundamental role to play in developing the digital economy. It is often assumed that the issues of cyber security and cyber insurance are separate – that cyber insurance is no substitute for proper cyber security – but in truth the two are intertwined. The questions insurers ask prospective insureds and policy terms may be more effective than exhortation or regulation in making directors think carefully about the risks facing the business. Insurers have a vested interest in providing expert advice to policyholders and have a long history of improving practice in various areas from establishing modern fire brigades to workplace

---

[110] *Kosmar Villa Holidays plc v Trustees of Syndicate 1243* [2008] EWCA Civ 147; J Lowry and PJ Rawlings [2009] JBL 275.
[111] *Friends Provident Life & Pensions Ltd v Sirius International Insurance* [2005] 2 Lloyd's Rep 517.
[112] *Travelers Casualty and Surety Company of America v Ignition Studio, Inc*, Complaint No. 1:2015cv00608 (Ill. N Dist. Ct., 2015).
[113] Eg ICO, *Notification of PECR Security Breaches* at http://tinyurl.com/lhdtx5h.
[114] This underpinned *Zurich American Insurance Co v Sony Corp of America*, No. 651982/2011 (NY Sup Ct, 2014). See, A Pearce, 'Allianz unveils cyber product suite', *Insurance* Age, 16 Sep 2013; Airmic, *Review of Recent Developments in the Cyber Insurance Market*, pp.11-12 at http://tinyurl.com/lcn6r58.
[115] *United Westlabs, Inc v Greenwich Ins. Co*, 2011 WL 2623932 (Del.Super., 2011), aff'd on different ground, 38 A.3d 1255 (Del.Supr., 2012).

safety.[116] The US government certainly subscribes to the view that insurance has an important part to play. At the end of 2014, Sarah Raskin, Deputy Secretary at the Department of the Treasury, "Ideally, we can imagine the growth of the cyber insurance market as a mechanism that bolsters cyber hygiene for banks across the board."[117] US regulators routinely insist on insurance as part of a package of security measures.[118] The UK government seems to have been a little slower to recognise this potential,[119] although this may be a consequence of a relatively weak cyber insurance market.

Of course, there are limits. Stephen Catlin, CEO of Catlin, owner of the largest syndicate at Lloyd's, recently warned that cyber risks present the "biggest, most systemic risk" he has encountered in an insurance career of more than 40 years.[120] Similarly, Axel Lehmann, Zurich's group chief risk officer, has warned, "The internet is the most complex system humanity has ever devised. Although it has been incredibly resilient for the past few decades, the risk is that the complexity which has made cyberspace relatively risk-free can – and likely will – backfire."[121] The problem is that no one knows the exact extent of the risks involved. A recent survey by Zurich revealed that even cyber security professionals were uncertain as to how a systemic risk might develop out of some issue at a particular company or a piece of technology,[122] and attacks such as on Anthem, the US health insurer, suggests that insurance companies may have much to learn about cyber security. At the same time, there is legal uncertainty as to the extent that insurers are liable. All of which calls to mind the situation just before the financial crisis in 2008 without even the – admittedly rather limp – protection and response strategies of the banking system. Not surprisingly, insurers are anxious to limit their risks and this may leave serious gaps in cover. In short, there is reason for concern that the industry cannot cover a "backfire". It may be that, as Catlin has suggested, government needs to think about organising support for this vital part of the economic and social structure, perhaps along similar lines to those offered in respect to flooding and terrorism.

---

[116] P Rawlings, '"Without Feeling and Without Remorse?": Making Sense of Employers' Liability and Insurance in the Nineteenth Century' (2013) 126 BILA Journal.

[117] S Raskin, 'Remarks of Deputy Secretary Raskin at The Texas Bankers' Association Executive Leadership Cybersecurity Conference' (Dec 2014) at http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx. See also, L Clinton, *Cyber-Insurance Metrics and Impact on Cyber-Security*, Internet Security Alliance at http://cyber.law.harvard.edu/cybersecurity/Cyber-Insurance_Metrics_and_Impact_on_Cyber-Security; *Treasury Department Report to the President on Cyber Security Incentives Pursuant to Executive Order 13636* (2014) at http://tinyurl.com/ksnfct7.

[118] Eg New York State Department of Financial Services, "New Cyber Security Examination Process" (Dec 2014) at http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf.

[119] Eg Department for Business Innovation & Skills, *Call for Evidence on Preferred Standard in Cyber Security: Government Response* (Nov 2013) at http://tinyurl.com/lzdjjnl.

[120] *Financial Times*, 5 Feb 2015.

[121] F Nyman, 'Interconnected cyber risks could cause global crisis', *Post*, 22 Apr 2014.

[122] *Ibid*.