Analysis of the full costs of cyber security breaches

Literature review annex

Harry Heyburn, Andrew Whitehead, Leonardo Zanobetti and Jayesh Navin Shah, Ipsos MORI
Professor Steven Furnell, University of Plymouth

Ipsos MORI

Contents

1 Longlist of documents included in literature review

The following reports were highlighted for potential inclusion within the literature review that took place at the start of this study. They are all publicly available.

- Action Fraud (2019) Cyber Crime Dashboard
- CEBR/Veracode (2016) Business and Economic Consequences of Inadequate Cybersecurity
- Comparitech (2018) How data breaches affect stock market price
- Deloitte (2016) Beneath the Surface of a Cyber attack
- Department for Health and Social Care (2018) Securing Cyber resilience in health and care
- Detica (2011) The Cost of Cybercrime
- FBI Internet Crime Complaints Centre (2018) 2018 Internet Crime Report
- Home Office (2018) Understanding the Costs of Cybercrime
- Ipsos MORI (2019) Cyber Security Breach Survey 2019, DCMS
- Kaspersky (2016) Measuring the financial impact of IT security on businesses
- McAfee (2018) Economic Impact of Cyber Crime
- McAfee and CSIS (2014) Net losses: Estimating the Global Cost of Cybercrime
- NCC Group Whitepaper (2018) The Economics of Defensive Security
- OECD (2017) Enhancing the role of insurance in cyber risk management
- Online Trust Alliance (2019) 2018 Cyber Incidents & Breach Trends Report
- Oxford Economics (2014) Cyber attacks: Effects on the UK
- Ponemon Institute & Accenture Security (2019) The Cost of Cyber Crime
- RAND (2018) Estimating the Global Cost of Cyber Risk
- TalkTalk (2016) Annual report
- US Council of Economic Advisors (2018) The cost of malicious cyber activity to the US economy
- Verizon (2019) 2019 Data Breach Investigations Report

2 Literature summary table

This table summarises each of the 15 shortlisted reports (out of the longlist of 22 in the previous section) that we reviewed in detail.

Cyber Security Breaches Survey, Ipsos MORI, 2019	
Description of report contents and objectives	The Cyber Security Breaches Survey is a quantitative and qualitative survey of UK businesses and charities. Its aim is to help these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the government to shape future policy in this area.
Countries	UK
Type of cyber-breach (with definition)	▪ Fraudulent emails or being directed to fraudulent websites ▪ Others impersonating organisation in emails or online ▪ Viruses, spyware or malware ▪ Ransomware ▪ Unauthorised use of computers, networks or servers by outsiders ▪ Denial-of-service attacks ▪ Hacking or attempted hacking of online bank accounts ▪ Unauthorised use of computers by networks or servers by staff ▪ Any other breaches or attacks
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	There were two strands to the Cyber Security Breaches Survey: ▪ A random probability telephone survey of 1,566 UK businesses and 514 UK registered charities was undertaken from 10 October 2018 to 20 December 2018. The data have been weighted to be statistically representative of these two populations. ▪ A total of 52 in-depth interviews were undertaken in January and February 2019 to follow up with businesses and charities that had participated in the survey and gain further qualitative insights.
Sample size	1,566 businesses and 514 registered charities
Respondents characteristics (size and sector)	For businesses analysis by size splits the population into: ▪ Micro businesses (1 to 9 employees) ▪ Small businesses (10 to 49 employees) ▪ Medium businesses (50 to 249 employees) ▪ Large business (250 employees or more) For charities analysis by size is considered in terms of annual income bands: ▪ Low income (under £100,000) ▪ Middle income (£100,000 to under £500,000) ▪ High income (£500,000 or more)

	Businesses are grouped according their respective Standard Industrial Classification (SIC) 2007 codes: ▪ Administration or real estate (L and N) ▪ Construction (F) ▪ Education (P) ▪ Health, social care or social work (Q) ▪ Entertainment, service or membership organisations (R and S) ▪ Finance or insurance (K) ▪ Food or hospitality (I) ▪ Information or communications (J) ▪ Utilities or production (including manufacturing) (B, C, D and E) ▪ Professional, scientific or technical (M) ▪ Retail or wholesale (including vehicle sales and repairs) (G) ▪ Transport or storage (H)
Costs identified (with definitions)	Direct cost ▪ Staff not being able to work ▪ Lost, damaged or stolen outputs, data, assets trade secrets or intellectual property (IP) ▪ Lost revenue or income if customer or donors could not access your services online Recovery cost ▪ Additional staff time to deal with the breach or attack, or to inform customer, beneficiaries, donors or stakeholders ▪ Costs to repair equipment of infrastructure ▪ Any other associated repair or recovery costs Long-term cost ▪ Loss of share value ▪ Loss of investors, donor or funding ▪ Long-term loss of customers (including potential new customers or businesses) ▪ Handling customer complaints or public relations (PR) costs ▪ Compensation, fines or legal costs
Comment on applicability of costs and ability to replicate	While to survey provides a useful framework for estimating costs the accompanying qualitative analysis suggests that it does not go far enough in estimating recovery and long-term costs and direct costs are also not fully captured, this suggests that it underestimates the full cost of a cyber incident for a firm. In addition, the cost categories provided do not have clear definitions that are mutually exclusive.
The Economics of Defensive Strategy, NCC Group Whitepaper, 2018	

Description of report contents and objectives	The report examines the costs of cyber defence in comparison to the costs and likelihood of a data breach. Varying breach costs and attack probabilities for different industry sectors are used to indicate the likely cost-effectiveness or overspend for different sectors and estate sizes in order to determine the cost or cost benefit of cyber defence
Countries	UK
Type of cyber-breach (with definition)	"Data breaches" as defined by the Ponemon Institute Study.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Breach costs ▪ Equal to the number of compromised records per breach x Ponemon Institute's average cost of a breach across all sectors. ▪ Alternative approach uses Cisco's model for breach costs as equal to 20% of revenue. In combination with the ONS figures for turnover of companies. ▪ In this case the loss equals turnover x 0.2 (20%). Prevention and defence costs ▪ This paper uses the SANS Institute security costing model, which estimates the cost of implementing operational security. ▪ In addition to this some annual costs have been included to take account of the costs of staffing and consultancy. ▪ The SANS model breaks operational costs down to sub costs: − Asset inventory database − Device scanners − Network access controls − Logging/alerting/analytics ▪ The SANS model then offers an estimate of each of these costs for small-medium businesses and medium to large businesses. Staffing and consultancy time is then added to the costs captured in the SANS model to give an overall "prevention and defence cost".
Sample size	N/A
Respondents characteristics (size and sector)	Estimates provided for all sectors, for UK business
Costs identified (with definitions)	Breach costs ▪ Direct costs: − Fines − Theft of credit or resources

	− System down time and associated revenue loses. such as staff call out costs for incident response ▪ Indirect costs: − Staff costs: any extra payments, overtime, etc. involved in restoring systems from backups, associated testing etc. − Reputational impact: lost business, cancelled business and loss of both existing and potential customers − Compensation − Reduction in company value Prevention and defence costs ▪ Operational costs: − Asset tracking, whereby an organisation must list both the data assets to be protected and the software which interacts with the data and must consequently be patched or updated − Security related hardware and software such as firewalls, anti-virus etc. − The cost of any additional staffing to handle the increased workload of updating software etc. ▪ Development costs (would only apply to an organisation developing its own software)
Comment on applicability of costs and ability to replicate	Top down costing. Using only secondary data from other sources. Namely the Ponemon study, Cisco study and SANS Institute study. The proposed cost structure is much more detailed than the estimates, i.e. the breach costs cannot be broken down by sub cost. Useful for validation and refinement of cost mapping, however costing methodology is weak as it simply sticks other study's cost estimates together.
Annual report, TalkTalk, 2016	
Description of report contents and objectives	TalkTalk, Annual report for 2016 – financial statement includes "exceptional costs" which are inclusive of the one-off exceptional costs associated with the cyber attack.
Countries	UK
Type of cyber-breach (with definition)	The specific 'cyber attack' experience by TalkTalk in 2016. The attack was an SQL injection. SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	The method for calculating the loss is not referenced. We might assume that the losses reported where directly observable and quantifiable from primary data owned and managed by TalkTalk. E.g. TalkTalk will directly measure the loss resultant from offering free upgrades, as the number of upgrades initiated multiplied by the market value of the upgrade.
Sample size	1 specific cyber attack.
Respondents characteristics (size and sector)	Communications (broadband)
Costs identified (with definitions)	The one-off exceptional costs associated with the cyber attack were £42m for FY2016 which includes the direct incident response costs and the following customer management costs: ▪ Additional call centre agents ▪ Communication and marketing costs incurred during October and November ▪ the costs of restoring our online capability with enhanced security features ▪ The increased retention costs including the cost of providing free upgrades to those customers who chose to take one One-off exceptional costs related to the cyber attack are also expected to accrue in FY2017 due to the timing differences between the incurrence of the provision and the resulting cash outflow. “The provision in FY16 for cyber attack related technology costs and surplus property costs, will be incurred in FY17 and beyond.”
Comment on applicability of costs and ability to replicate	Very little applicability. Costs are not broken down to an appropriate level of detail. We can use the types of costs highlighted to sense check the cost mapping, not much more than this.
Understanding the Costs of Cybercrime, Home Office, 2018	
Description of report contents and objectives	Home office cost of crime structure (anticipation, consequence and response costs). This is a consistent structure used to capture the costs of all crimes. The method used attempts to capture costs to society as a whole (not just costs to business). This is an important distinction because for example repaid, in this methodology are consider transfers with a net economic cost to society of Zero. Where as in a structure looking at costs to business this would be a direct financial cost equal to the amount of the fine. This paper provides a framework for capturing costs and does not attempt to estimate those costs.

Countries	UK
Type of cyber-breach (with definition)	For consistency this paper uses the definitions provided In the Serious and Organised Crime Strategy (Home Office, 2013a), the government highlighted some of the issues arising from cybercrime, which it explained could be broken down into two types of criminal activity: ▪ "Cyber-dependent crimes – those which can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage." ▪ "Cyber-enabled crimes – those which can be conducted on or offline, but online may take place at unprecedented scale and speed." This definition excludes cyber terrorism, online hate crimes, cyber bullying, digital piracy or online sexual crimes. The paper acknowledges other taxonomies and definitions of cybercrime which have been used include: ▪ Anderson et al. (2012) who used a definition that incorporates traditional forms of crime, publication of illegal content, and crimes unique to electronic networks ▪ Wall (2007) who defined cybercrime as: crimes against the machine, crimes using machines and crimes in the machine
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	As this is only a framework no methodology for calculating the proposed costs is provided. We might imagine the cost framework provided would be populated via survey of a random probabilistic sample of SME and LBE's across all sectors.
Sample size	N/A
Respondents characteristics (size and sector)	N/A
Costs identified (with definitions)	Costs in anticipation ▪ Tech costs: – Computer security protection software/products (e.g. anti-virus) – Introduction of new additional technologies ▪ Training: – Cyber security training/education

- Training for law enforcement investigators and officers
- Training of court and legal personnel

- Security practices/behaviours:
  - Implementing cyber security practices
  - Usability/user impact as a result of increased security procedures
  - Switching internet service providers (ISPs), security providers or products to increase security
  - Vetting staff or contractors for security purposes
  - Monitoring third parties' security
  - Checking credit histories/scores
  - Avoidance of the internet and/or other technologies (among non-users

- Government activities:
  - Drafting and creating new legislation
  - Efforts to educate public on new legislation
  - Implementation of national awareness raising/protection campaigns

- Other:
  - Cyber insurance administration
  - Consumer credit/identity protection services (for example,
  - CIFAS, a fraud protection organisation)
  - Fear/worry about cyber crime
  - Collection and compilation of cybercrime statistics

Costs as a consequence

- Costs of fixing an attack:
  - Equipment/infrastructure damage
  - Clean-up expenditures
  - Rectifying credit histories/scores

- Financial losses:
  - Business disruption (including lost outputs)
  - Online theft/fraud of funds
  - Lost value of IP/commercially sensitive information
  - Damage to reputation or brand value
  - Disputed transactions

- Other:
  - Emotional/physical harms
  - Victim support services

Costs in response

- Law enforcement (law enforcement disruption and investigation activities)
- Courts (Prosecuting cyber cases)

	▪ Prisons and probation: − Additional costs to the probation system − Incarceration of cybercriminals ▪ Non-criminal justice system responses: − Reporting/documenting incidents − Legal, PR advice and similar expenses − Increased/improved IT spending as a direct response to victimisation − Training/education put in place as a direct response to victimisation − Switching ISPs, security providers or products as a direct response to victimisation − Reduction in research and development expenditure
Comment on applicability of costs and ability to replicate	None
The Cost of Cyber Crime, Ponemon Institute & Accenture Security, 2019	
Description of report contents and objectives	Study on the economic impact of cyber attacks. The objective of the study is to estimate the global cost of cybercrime, estimation of the cost-opportunity of preventive measures, estimation of the uptake of preventive measures.
Countries	Australia, Brazil, Canada, France, Germany, Italy, Japan, Singapore, Spain, United Kingdom, United States
Type of cyber-breach (with definition)	Cyber attacks: criminal activity conducted through the organization's IT infrastructure via the internal or external networks or the Internet. Cyber attacks also include attacks against industrial controls. A successful cyber attack is one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defences.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Cost of cybercrime: in-depth interviews in which organisations were asked to report amount spent on dealing with cybercrime over a period of four consecutive weeks. The cost was then validated and used to determine an annualised cost to detect, recover, investigate, and manage the incident. Value at risk: expected cost of cybercrime expressed as a percentage of revenue by industry, which was then multiplied by the total industry revenues. Limitations: ▪ Costs are not based on accounting information ▪ Non-representative sample ▪ 4-week period surveyed ▪ Unspecified checks and balances applied ▪ Extended timespan of interviews

Sample size	2,647 senior leaders (IT and compliance and information security) from 355 large-size companies (different sample every year).
Respondents characteristics (size and sector)	Banking, utilities, software, automotive, insurance, high tech, capital markets, energy, US Federal, consumer goods, health, retail, life sciences, communications and media, travel, public sector.
Costs identified (with definitions)	Internal costs ▪ Discovery: activities that enable an organisation to detect and possibly deter cyber attacks or advanced threats, including allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection. ▪ Investigation: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents. The escalation activity also includes the steps taken to organize an initial management response. ▪ Containment: Activities that focus on stopping or lessening the severity of cyber attacks or advanced threats. These include shutting down high-risk attack vectors such as insecure applications or endpoints. ▪ Recovery: Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and other IT (data centre) assets. Ex-post response activities are also included in recovery to help the organization minimize potential future attacks. These include containing costs from business disruption and information loss as well as adding new enabling technologies and control systems. External consequences Costs related to results of cyber attack (information loss/theft, business disruption/ damage to equipment, revenue loss). ▪ Cost of information loss or theft: Loss or theft of sensitive and confidential information as a result of a cyber attack. Such information includes trade secrets, IP (including source code), customer information and employee records. This cost category also includes the cost of data breach notification in the event that personal information is wrongfully acquired. ▪ Cost of business disruption: The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements. ▪ Cost of equipment damage: The cost to remediate equipment and other IT assets as a result of cyber attacks to information resources and critical infrastructure. Costs are further broken down in to: ▪ Direct cost – the direct expense outlay to accomplish a given activity ▪ Indirect cost(s) – the amount of time, effort and other organizational resources spent, but not as a direct cash outlay

	▪ Opportunity cost – the cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident
Comment on applicability of costs and ability to replicate	Develops a largely replicable methodology for bottom-up costs. Data from interviews or surveys can be used to estimate costs, providing sense checks are performed.
Economic Impact of Cyber Crime, McAfee, 2018	
Description of report contents and objectives	The report provides a mapping of cybercrime cost across countries with a focus on IP theft.
Countries	Argentina, Australia, Brazil, Canada, China, Colombia, EU, France, Germany, India, Indonesia, Ireland, Italy, Japan, Kenya, Korea, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Norway, Russia, Saudi Arabia, Singapore, South Africa, Turkey, UAE, United Kingdom, United States, Vietnam, Zambia
Type of cyber-breach (with definition)	Cybercrime, defined as criminals gaining illicit access to a victim's computer or network, including: ▪ Loss of IP and business confidential information ▪ Online fraud and financial crimes, often the result of stolen personally identifiable information ▪ Financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports of publicly traded companies ▪ Opportunity costs, including disruption in production or services, and reduced trust for online activities – this includes the effect of ransomware ▪ The cost of securing networks, buying cyber-insurance, and paying for recovery from cyber attacks ▪ Reputational damage and liability risk for the hacked company and its brand
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Replicated from previous wave of study (2014), see below.
Sample size	Representatives from 51 countries

Respondents characteristics (size and sector)	Government officials
Costs identified (with definitions)	▪ The loss of IP and business confidential information ▪ Online fraud and financial crimes, often the result of stolen personally identifiable information ▪ Financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports for publicly traded companies ▪ Opportunity costs, including disruption in production or services, and reduced trust for online activities – this includes the effect of ransomware, which involves both payments to redeem encrypted data, and, more importantly, serious disruptions to services and output ▪ The cost of securing networks, buying cyber insurance, and paying for recovery from cyber attacks ▪ Reputational damage and liability risk for the hacked company and its brand, including temporary damage to stock value
Comment on applicability of costs and ability to replicate	The methodology, as well as the data sources used are not clearly expounded.
Net losses: estimating the global cost of cybercrime, McAfee and CSIS 2014	
Description of report contents and objectives	The report aims to calculate the overall cost of cybercrime to the global economy.
Countries	World
Type of cyber-breach (with definition)	Though there is no clear definition presented the report focuses on two particularly costly types of cybercrime: **IP theft**, **financial crime** (the theft of financial assets through cyber intrusions), as well as **theft of confidential business information** and **market manipulation**.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	The report uses a survey and existing sources to aggregate costs in the individual countries and extrapolate to calculate the global cost. Due to limits in reporting and data collection the report does not find a satisfactory approach to extrapolation and finds that sources report widely different costs for countries and regions. This study assumes that the cost of cybercrime is a constant share of national income, adjusted for levels of development. The likely global cost is calculated by looking at publicly available data from individual countries, buttressed by interviews with government officials and experts. Confirming evidence for these numbers is sought by looking at data on IP theft, fraud, or recovery costs.

	In addition to anecdotes, aggregate data for 51 countries in all regions of the world is used to estimate the global cost, adjusting for differences among regions. Methodological challenges for estimating cost of IP theft Calculations used in pricing a company for sale or merger can be based on a prediction of how much future income the IP will produce or how much it would fetch if offered for sale. These estimates provide a guide for estimating loss, but companies may not know what has been taken and the cybercriminals may not be able to make full use of what they have taken. Other intangible losses Along with the difficulty of valuing IP, other intangible losses are not easily measured. In addition to losses in business and consumer confidence, the effect of cyberespionage on national security is significant, and the monetary value of the military technology taken likely does not reflect the full cost to the nation. Underreporting and the difficulty of valuing IP are the most significant problems for estimating the cost of cybercrime. Theft of financial assets The theft of financial assets can be easiest to monetise, particularly when a criminal can transfer funds directly to an account they control. Opportunity cost For companies, the largest opportunity cost may be in the money spent to secure their networks. While companies would always spend on security even if risk in the digital environment was greatly reduced, there is a “risk premium” that they pay for using an inherently insecure network. The rate at which spending on cyber security increases reflects not only an increased use of network technologies, but also an increased awareness of the threat. The rate of change in cyber security spending can be used as an indicator of opportunity cost and a “risk premium”. Another way to look at the opportunity cost of cybercrime is to see it as a share of the Internet economy. The report estimates that cybercrime extracts between 15 per cent and 20 per cent of the value created by the Internet.
Sample size	Not stated
Respondents characteristics (size and sector)	Sources range from the Constitution, the Netherlands Organisation for Applied Scientific Research (TNO), China’s Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, Malaysia’s Chief Technical Officer and estimates by government agencies in other countries and consulting and cyber security companies around the world.
Costs identified (with definitions)	▪ Value of stolen IP ▪ Value of financial assets through stolen cyber intrusions

	▪ Opportunity cost: Opportunity cost is the value of forgone activities – opportunities or benefits that cannot be realized because resources have been expended elsewhere. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in research and development (R&D), risk averse behaviour by businesses and consumers that limits Internet use, and increased spending on network defence
Comment on applicability of costs and ability to replicate	Does not provide sufficient detail on the methodology to be replicable. The methodology is not relevant for calculating costs at firm level.
Estimating the Global Cost of Cyber Risk, RAND, 2018	
Description of report contents and objectives	The objective of the study is to provide a transparent and adaptable methodology for estimating present and future global costs of cyber risk that acknowledges the considerable uncertainty in the frequencies and costs of cyber incidents. This report has a companion Excel-based modelling and simulation platform that allows users to alter assumptions and investigate a wide variety of research questions.
Countries	Netherlands
Type of cyber-breach (with definition)	
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Four sets underpinning model: ▪ countries ▪ industry sectors ▪ economic exposure ▪ perils Incident cost is related to GDP and output loss within specific industrial sectors, by country. In the model, **direct costs** are calculated based on the share of value added related to a sector i of a given country c, as well as the output value of that sector i in that country c. Alongside this, the model incorporates the unitless value representing the fraction of output of an industry i that is at risk from each type of exposure type, in addition to a unitless value representing the fraction of the exposure at risk of a country c, for an industrial sector i that will be destroyed or stolen due to a peril p. The direct cost to sector output will be then determined by the sum of the product of the unitless values for each type of peril and exposure – multiplied by the output of a certain sector in a certain country. This can be used to find the change to sector Gross Domestic Product (GDP) by relating in the changes in output to equivalent, linear changes in GDP.

	The resulting estimation clearly depends on inputs of perils, exposures, sectors, and the inter-sectoral links of a country. **Systemic costs** are determined using a Leontief Inverse Matrix; changes in output are related to changes in demand, and thus changes in one industry's output change the output in another. The **total output cost** due to cyber risk in a country is the sum of the direct and systematic costs. However, limitations of this approach are evident when considering: ▪ data sources availability ▪ cross-country comparability of data sources and sectoral definitions ▪ uncertainty relative to the weight of perils and expenditures
Sample size	Not stated
Respondents characteristics (size and sector)	Not stated
Costs identified (with definitions)	**Direct costs:** Output losses experienced by each sector in each country. These includes costs that are directly paid by a sector before, during, and after an event, including attests, fines, extortion, and investigative costs, and business interruptions that occur in the sector that was attacked, as well as litigation costs that may be incurred by third parties but are compensated by the firm that was attacked. **Systemic costs:** Macroeconomic impacts to output experienced by other sectors because of the direct damages by each sector in each country.
Comment on applicability of costs and ability to replicate	The model illustrates costs (expressed as output and GDP losses) from cyber attacks at the international level, without solving the issue of how to choose weights values within countries.
Deloitte: Beneath the surface of a cyber attack, 2016	
Description of report contents and objectives	The report provides an overview of costs related to tangible (above-the-surface) costs and hidden costs. Two case studies (health insurance, technology manufacturer) are the focus of the research.
Countries	US
Type of cyber-breach (with definition)	
Methodology (including methodological challenges, strengths/weaknesses and overall	**Valuation and financial quantification:** at a specific point in time (when the attack was discovered). Calculated through Discounted Cash Flow Method under the Income Approach, which broadly entails estimating the present value of the projected economic benefits to be derived from the use of the asset.

assessment of its robustness)	**With-and-without method:** Involves estimating the value of an asset under two scenarios: one, with a certain asset or situation in place (the "situation," in this context, being the occurrence of a cyber attack); and the other without the asset or situation in place (in this case, the absence of a cyber attack). The difference in these value estimates yields the isolated value impact that can be attributed to the situation.
Sample size	2 companies
Respondents characteristics (size and sector)	Technology and healthcare sector organisations.
Costs identified (with definitions)	**Technical investigation:** the costs associated with technical investigations are direct expenses for analysis to determine what happened during a cyber incident and who was responsible. **Customer breach notification:** customer breach notification costs include the direct expenses associated with informing and advising individuals whose data has been compromised, as typically mandated by state or federal law or industry regulation. These can include printing, mailing, and call centre services, among others. **Post-breach customer protection**: post-breach customer protection costs are direct costs associated with services to detect and protect against potential efforts to use an individual's compromised personal data for unauthorized purposes. **Regulatory compliance:** regulatory compliance costs are fines or fees levied as a result of non-compliance with federal or state cyber-breach related laws and/or regulations. **Public relations**: PR costs are the direct costs associated with managing external communications or brand monitoring following an incident. **Attorney fees:** attorney fees and litigation costs can encompass a wide range of legal advisory fees and settlement costs externally imposed and costs associated with legal actions the company may take to defend its interests. **Cyber security improvements:** the costs associated with cyber security improvements are direct expenses for technical improvements to the infrastructure, security controls, monitoring capabilities, or surrounding processes, specifically to recover business operations after an incident or to prevent a similar occurrence in the future.
Comment on applicability of costs and ability to replicate	Low replicability. Methodology requires access to accounting information (sensitive data, especially for firms that have been the subject of a breach).
The Cost of Cybercrime, Detica, 2011	

Description of report contents and objectives	In the National Security Strategy, the UK Government recognised cyber threats as one of four "Tier One" risks to the UK's security. However, estimates of the impact of cybercrime have until now been no more than "best guesses". Therefore, the Office of Cyber Security and Information Assurance (OCSIA) worked in partnership with Detica to look more closely at the cost of cybercrime in the UK to gain a better appreciation of the costs to the UK economy of IP theft and industrial espionage. The aim of this study is to understand which types of cybercrime have the largest economic impact, and the relative risk faced by different industry sectors. This will aid further developments of cybercrime policy, strategies and detailed plans.
Countries	UK
Type of cyber-breach (with definition)	Cybercrime is defined as illegal activities undertaken by criminals for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the government. It does not include crimes that lack an overriding financial motive, or attacks of cyber terrorism or cyber warfare. It focuses on identity theft and online scams affecting UK citizens, IP theft, espionage and extortion targeted at UK businesses; and fiscal fraud committed against the government. The following definitions are used: **Identity theft:** cyber criminals obtain personal data from individuals (such as address, date of birth or bank account details) and exploit this online by opening bogus accounts (for example, bank accounts and mortgage applications). In many cases, the victims of identity theft are not even aware of a problem until the impacts become severe. **Online scams:** cyber criminals obtain financial or other valuable information by fraudulent means, usually by tricking individuals through scams such as purchase frauds (such as making people pay for goods they do not intend to despatch), 'phishing' (for example, sending bogus money-transfer requests from foreign countries to thousands of e-mail accounts), 'spear phishing' (highly personalised bogus e-mails targeted at a single individual), 'spoofing' (fooling people into entering details into a counterfeit website) and 'pharming' (redirecting website traffic from a legitimate website to a fraudulent website). **Scareware:** cyber criminals mislead individuals into downloading software onto their computers (for example, fake anti-virus software) by using fear tactics or other unethical marketing practices. The software downloaded is often ineffective or may appear to deal with certain types of virus before infecting the computer with its own viruses. Individuals may then have to pay the cyber criminals to remove the viruses and their impacts. **Fiscal fraud:** cyber criminals can withhold taxes due or make fraudulent claims for benefits by attacking official online channels (such as online self-

	assessment forms). The loss of tax revenue directly affects public-sector spending and the government's ability to invest in UK infrastructure. **Theft from business:** cyber criminals steal revenue online directly from businesses, which usually involves fraudulently obtaining access and looting company accounts and monetary reserves. In some instances, this cyber-criminal activity is greatly assisted by an "insider". **Extortion:** cyber criminals hold a company to ransom often through deliberate denial of service (for example, by using malware to flood a company server with erroneous internet traffic) or by manipulating company website links, which can lead to extensive brand damage (for example, by redirecting links for a retailer website to an online pornography website). **Customer data loss:** cyber criminals steal sensitive customer data from a company (such as customer financial, medical or criminal record details) with the purpose of selling the data on to other criminal networks or using it themselves for blackmail attempts. For our study, we have not included accidental data loss but only losses from deliberate and technological means. **Industrial espionage:** this takes many forms, such as a rival organisation (or associated third party) illegally accessing confidential information to gain competitive or strategic advantage (for example, by finding out a rival's bid price) or to gain insider knowledge for financial gain (for example, by becoming aware at an early stage of a possible merger or acquisition deal). Cyber criminals could use the insider information they glean to acquire or sell shares, or, in rare cases, by betting on currency fluctuations. **IP theft:** cyber criminals, often sponsored by rival organisations or nation states, steal ideas, designs, product specifications, trade secrets, process information or methodologies, which can greatly erode competitive advantage or even the operational or technological advantage prized. **Money laundering:** cyber criminals use online means to launder the proceeds of criminal acts (for example, through complex, internet-enabled transfers between global or offshore bank accounts). This type of activity is usually associated with organised criminal networks that have a wide or international reach.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	To address the complexity of less understood cybercrime the report uses a **causal model**, relating different cybercrime types to their impact on the UK economy. The model provides a simple framework to assess each type of cybercrime for its various impacts on citizens, businesses and the government. Various types of cybercrime are mapped to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macroeconomic models of the UK. The magnitude of the costs of cybercrime are calculated using three-point estimates (worst-case, most-likely case and best-case scenarios), focusing on **IP theft** and **industrial espionage** and its effect on the different industry sectors.

	Assessments are based on estimates and assumptions rather than specific examples of cybercrime, or from data of a classified or commercially sensitive origin. The assessment uses information in the public domain, supplemented by the knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private sector organisations. The results, therefore, should be used as a credible, illustrative guide to the nature of the impacts of cybercrime rather than as accurate and robust estimates of the impacts of cybercrime. The methodology is adapted by the methodology used by the Home Office in their 2001 report on the economic impact of crime in the UK to define the following types of cost associated with cybercrime: ▪ **Costs in anticipation of cybercrime** – which include individual and organisational security measures (such as installing physical and virtual protection such as antiviral software), insurance costs and costs associated with gaining compliance to required IT standards (for example the Payment Card Industry Data Security Standard, PCI DSS) ▪ **Costs as a consequence of cybercrime** – which take into account direct losses to individuals and companies (including business continuity and disaster recovery response costs), and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness ▪ **Costs in response to cybercrime –** such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues ▪ **Indirect costs associated with cybercrime –** which include such factors as reputational damage to organisations, loss of confidence in cyber transactions by individuals and businesses, reduced public sector revenues and the expansion of the underground economy The study has focused on the costs as a **consequence of cybercrime** and has included some additional costs in **response to cybercrime** where these can be realistically estimated. However, because the situation is inherently complex, there are a number of methodological issues. These are as follows: ▪ The impact has been measured as a “snapshot”, using the economic situation of 2010 as a baseline. It has not attempted to predict economic impacts for 2011 or beyond, because, as of this study, market conditions still remained fluid and a very large number of variables would affect the estimates. ▪ Because economic data for UK industry sectors and citizens varies considerably depending on its source and context, estimates are based, wherever possible, on economic data provided by official government bodies, such as the Department for Business, Innovation and Skills and the Blue Book 2010. It was not always possible to obtain 2010 data; estimates are based on the most contemporary data available and applied as if they were 2010 data. ▪ Although certain indirect economic impacts can be attributed to cyber-criminal activity, those which exhibit a high degree of situational complexity are excluded. For example, short-term fluctuations in a

company's share price caused by theft of customer data are excluded. Measuring this sort of impact is challenging because such fluctuations depend on the prevailing market conditions at the time of the theft and the number of other factors specific to the individual company affected.
- It excluded costs in anticipation of cybercrime, such as insurance costs and the costs of purchasing anti-virus software, because these are likely to be factored into normal day-to-day expenditure for the government, businesses and individuals.

Overall the approach to estimating economic impacts is conservative where there is a high degree of uncertainty caused by a lack of data, particular sensitivities or when cybercrime is going underreported.

For most of these areas, 3-point estimates are presented – worst-case, best-case and most-likely case – to allow for sensitivity and scenario analysis.

The methodology does not provide definitive estimates of economic impacts for cybercrime in every case and for every industry. Rather, one of the primary aims was to provide a **framework for future estimates**, which can be updated as more accurate information is obtained through further study and analysis.

Methodology for assessing the impact of IP theft

The study identifies two methods for calculating the costs to the UK economy of IP theft through cybercrime.

- The first method uses the total R&D expenditure for each UK industry sector as a starting point. The expected return on investment as a percentage for this R&D spend was estimated, which created an overall market value for the IP. This value recognises that IP theft does not just lead to short-term losses from R&D spend, but also to future losses from the value that industry sectors would wish to recoup from their initial expenditure.
- The second method started with the total cash flow for each UK industry sector, and then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value.

Once the economic value of the IP had been derived from both methods, estimates were made of the probability of cyber theft for each industry sector using three-point estimates, with the subsequent IP exploitability and revenue impact also calculated as a percentage. This enabled the assessment of the economic impact of IP theft on both the basis of R&D spending and the overall economic value of IP.

In developing the methodology for measuring the impact of IP theft, assumptions are made regarding:

- The total amount of R&D spending in each UK business sector (using up-to-date and credible data where it is available)
- The average estimated return on investment that each UK business sector would expect from its R&D spend (to estimate the true value of the IP and not just the current market worth)
- The average estimated level of IP 'exploitability' for cyber criminals (recognising that not all IP can be easily exploited)

- The level of economic impact that IP exploitation would have on the UK economy (recognising that, even though it may be exploited, stolen IP does not necessarily lose all its residual value)

In the absence of robust estimates for actual levels of IP theft, the methodology assumes that the 'business model' cyber criminals adhere to for IP theft follows the same principles of any other type of business: the desire to maximise financial gain and minimise business risk.

For IP theft by cyber criminals, the methodology attempts to determine the means, motive and opportunities presented to potential attackers. It recognises that the nature of IP generated in different business sectors is different and has different levels of exploitability and economic impact if it is stolen.

Therefore, the method used by the study to calculate the costs to the UK economy of IP theft through cybercrime started with the value added to the UK economy by each industry sector as given in the Blue Book. It then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value.

Once the economic value of the IP had been derived, estimates were made of the probability of cyber theft for each industry sector using three-point estimates, with the subsequent IP exploitability and revenue impact also estimated as a percentage.

The results give an estimate of the value lost to the economy due to IP theft across the different industry sectors.

Given the number of variables and lack of 'official' data, the methodology uses a **scenario-based approach**, which establishes three-point estimates to determine the range of uncertainty. Using this approach, we have identified:

- **The best-case scenario:** IP thefts by cyber attack are not widely reported because, although they may be technically possible, they are not widespread. Therefore, a very small amount of IP is actually stolen.
- **The worst-case scenario:** The sophistication of and resources available to cyber criminals, coupled with the vulnerability many businesses have towards cyber attacks, means that most IP worth stealing is stolen. The logic of this position is that if cyber criminals have the means, motive and opportunity they will use it for financial gain. In this scenario, the economic impact is limited by the ability of the cybercriminal to exploit the IP effectively rather than to acquire it.
- **The most likely scenario:** Theft of IP by cyber criminals can occur but it needs to guarantee a big return. The level of IP theft within a business sector is therefore determined by the level of motivation of the criminal to attack specific targets, which means that some business sectors are significantly more attractive than others.

This report assumes that there are two possible models of IP theft used by cyber criminals. The first model would see cyber criminals targeting selected companies to acquire specific information that they know can be exploited effectively. In this model, the IP is targeted explicitly, possibly 'to-order' if the attacker is working on behalf of an otherwise legitimate business. The second

model would see cyber criminals attempting to obtain IP in bulk from as many companies as possible and then assessing it to determine whether to exploit it, if at all.

However, the proportion of IP stolen cannot at present be measured with any degree of confidence. The methodology makes the assumption that the level of IP theft is proportional to the level of motivation that cyber criminals have in acquiring it. It is assumed that their level of motivation is affected by the following factors:

- Their ability to obtain the IP using alternative means, for example by reverse-engineering a legitimately acquired sample, which would reduce or indeed remove their motivation for a cyber attack
- The importance they place on time–to-market in the sector, which increases the motivation for a cyber attack if time is more of the essence
- The level of innovation typically presents in the IP within the sector – a high level of innovation would make the IP intrinsically more value to cybercriminals, hence a higher degree of motivation
- The size of the market that exploitation of the IP will allow them to address
- The level of security awareness within the sector and the deployment of security countermeasures by targeted companies. Although this may be a factor in reducing the success rate of IP thefts, we do not think that increased levels of security will necessarily reduce the level of motivation for an attack where the returns are sizeable. Instead, it may motivate the cybercriminal to use even more sophisticated means

Methodology for assessing the impact of industrial espionage

In developing the methodology for estimating the impact of industrial espionage, the following assumptions are made about:

- The value added to the UK economy by each UK business sector using up-to-date and credible data, where available
- The average proportion of open tender contracts placed in each UK business sector, the likelihood of UK organisations winning at least one of these contracts, and the level of exploitability for rival organisations should they gain access to sensitive contract documents
- The total value of merger and acquisition activity for each UK business sector using up-to-date and credible data, where available
- The expected rate of return on investment in shares for targets of merger and acquisition activity, short selling and currency-price fluctuations, and the level of exploitability of commercially-sensitive information (to assess impacts from illegal investment in shares for target organisations, the impact from illegal investment in short selling and the impact of market fluctuations respectively)

In line with IP theft by cyber criminals, the methodology has attempted to determine the means, motive and opportunities presented to potential attackers. It recognises that the nature of industrial espionage in different

	business sectors is different and has different levels of exploitability and economic impact if it is stolen. It is more likely that cyber criminals will target organisations for espionage based on size and perceived revenue rather than the business sector that they operate in. 3-point estimates of the costs to the UK are made of: ▪ **The loss of competition-sensitive information –** estimated as the proportion of a sector's annual value-added to the UK economy that is dependent on large-scale tendering competitions, multiplied by estimates for the probability that any of these would be subject to cyber attacks and the resultant exploitability of the stolen information ▪ **Information on mergers and acquisitions –** estimated by taking the total value of mergers and acquisitions for each business sector in the last year and multiplying these by estimates for the probability that any of these would have been subject to cyber attack, the exploitability of the information and the maximum illegal return that could be generated without the exploitation being detected. Separate calculations were made for cybercriminals being able to manipulate the share price of the organisation through "short selling" or, in the case of exceptionally large mergers, benefiting Online theft from businesses As there are no reliable published estimates for direct online theft from business, the study attempts to estimate the likely impact by looking at the cash-flow per year across the different business sectors and making some assumptions about the level of cybercrime. The approach estimates a maximum percentage of annual cash-flow that a business sector could potentially tolerate being lost. This was multiplied by an estimate of the probability that businesses in this sector were subject to successful cyber attacks. Due to the sensitivity of the results to this estimate, three-point estimates of the worst case, best case and most likely costs were calculated. Extortion The approach considers the combined turnover of business of small, medium and large size, and multiplied these by an estimate made of the proportion of companies that would be vulnerable to extortion, the probability of an extortion attempt being made and the probability that it would be successful.
Sample size	Based on a modelling approach
Respondents characteristics (size and sector)	N/A
Costs identified (with definitions)	Direct costs ▪ Cost of online theft

	▪ Cost of extortion These costs could potentially impact any of the six functions in the business value chain: ▪ R&D, because companies are less likely to invest ▪ Design of products, services, or processes, because companies are less willing to turn new ideas into products ▪ Production, because companies want to reduce costs ▪ Marketing and sales, because companies want to cut expenditure to reduce their attractiveness to the underground economy ▪ Distribution, because companies are affected by reduced demand for exports ▪ Customer service, because companies have less money to spend on their customers Costs associated with cybercrime for organisations include implementing their business continuity and disaster **recovery plans:** ▪ Diverting personnel and resources away from business-as-usual activities ▪ Good will and compensation payments to customers affected by online scams and identity theft ▪ Regulatory penalties for customer data breaches ▪ "Clean-up" consultancy costs associated with legal and forensic issues **Indirect costs** could arise from share-price manipulation, enabled by sophisticated industrial espionage, as well as the attrition of UK industry influence overseas as a result of IP theft. The knock-on effects of IP theft or industrial espionage on UK companies include: ▪ Reduced turnover through direct loss of business ▪ Reduced profitability by losing first-to-market advantage and increasing price competition ▪ Reputational damage caused by disclosure of the theft and arrival on the market of counterfeit goods ▪ Reduction in share price, which may be particularly acute if the company also happens to be an acquisition target ▪ Loss of competitive advantage, which may be more apparent in overseas markets ▪ Additional costs incurred through attempts to protect future IP ▪ Opportunity costs, as the company becomes less willing to invest; ▪ Redundancies as R&D facilities and product lines decrease in capacity or are closed ▪ Company failures, particularly if the theft has occurred from small and medium enterprise (SME) reliant upon IP-enabled trade sales ▪ Reduction in investment from overseas
Comment on applicability of costs and ability to replicate	Methodology is not relevant for estimating costs at firm level.

Cyber attacks: Effects on the UK, Oxford Economics, 2014	
Description of report contents and objectives	The Centre for the Protection of National Infrastructure (CPNI) requested that Oxford Economics carry out a study of the impact of state-sponsored cyber attacks on UK firms. The project consists of 4 parts: ▪ An economic framework to understand the impact of state sponsored cyber attacks on UK firms ▪ A survey of UK firms to provide a cost estimate of the impact of cyber attacks (including references to case studies of UK firms where relevant) ▪ An event study around the impact of cyber attacks on market valuations ▪ A series of case studies illustrative of the experience of UK firms with cyber attacks
Countries	UK
Type of cyber-breach (with definition)	▪ Loss of sensitive information ▪ Advanced Persistent Threat (APT) refers to a type of cyber attack designed to evade an organisation's present technical and process countermeasures. APTs are specifically designed to bypass firewalls, intrusion detection systems, and anti-malware programs. Many APTs are designed with a specific purpose. For example, some may be designed to gather information, including confidential information. Others may take the form of a continuous barrage of targeted and sophisticated attacks aimed at governments, companies and individuals in order to compromise individual systems and whole organisations
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Survey methodology An email/internet-based survey process was used to undertake the work. This used the existing database of IT professionals, IT security practitioners and other IT related roles developed by the Ponemon Institute. A total of 9,973 surveys were sent out to UK firms on this database and a sample of 427 responses was obtained, an effective response rate of 4.3%. Note that this sample is not representative of the population of UK firms. It represents a convenience sample, illustrating the results of this particular sample. While results cannot be extrapolated to make inferences about all UK firms, it provides an instructive view of the experiences of these firms with cyber attacks. as a part of the survey, respondents were asked to quantify the estimated losses they had experienced as a result of cyber attacks. The cost estimates related to costs incurred over the past 24 months Event study methodology Oxford Economics undertook an event study to analyse the potential reputational loss firms may suffer. As a proxy for reputational damage they

	used negative stock market returns that may be experienced immediately around the public disclosure of a cyber attack. Event studies seek to determine the effect of an event on the stock prices of publicly traded companies and are typically used in the fields of financial economics, accounting, and law and economics. To find if the announcement of the cyber attack affected a firm's stock price, they estimate first what the return of each individual stock would have been if the event had not occurred. This is termed the "normal return." The market model is used to calculate the normal return. This model relates the return of a stock to the return of the relevant market index, thus separating out the portion of the return that is correlated with broader market movements and the portion that is specific to that individual share price behaviour. By removing the portion of the return related to the broader market movements and focusing instead on the portion of the return specific to the individual stock, it provides a better ability to detect the effects of the cyber attack on the return of the stock (if any). Data on daily returns to the select stocks for which we found public announcements of cyber attacks were partitioned into two sections – a 3-day event window and a 120-day estimation window. The 3-day event window encompassed the day of the public announcement of the cyber attack (day 2), as well as the preceding and the following day. The 120-day estimation window encompassed stock return data for the 120 days immediately preceding the 3-day event window. An ordinary least squares (OLS) regression was run to find the relationship between the stock return and the market index using the 120-day estimation window for each stock. Subsequently, the parameters of that estimation were used to calculate the expected return of each stock over the 3-day event window, where the cyber attack was made public. This is the return we would have expected if there had not been an announcement of a cyber attack. The difference between the actual return observed over the three days on stock exchanges and the expected return we calculated is termed the "abnormal return." This is the portion of the volatility of the stock that is not explained by the market and may be the result of the announcement of a cyber attack. Subsequently, the average of the abnormal return over the 3-day event window was calculated for each stock and divided by its standard deviation (a measure of volatility) to determine if the abnormal return is statistically different from zero. If returns are statistically different from zero (and negative), then it would suggest that perhaps cyber attack announcements, in general, do have a reputational effect on companies. Case studies methodology In order to complement the preceding analysis a series of interviews were conducted with a number of UK firms aimed at getting a direct understanding of how cyber attacks had affected their operations.
Sample size	Survey: 427 Events study: 45 events

Respondents characteristics (size and sector)	The survey targeted those with responsibility for IT-related functions, including budgets, performance, strategy and security.
Costs identified (with definitions)	▪ Clean-up/remediation costs ▪ User productivity costs ▪ Disruption to normal operations ▪ Damage/theft of IT assets and infrastructure ▪ Damage to reputation and marketplace image (brand value) Respondents were also asked to quantify their estimated losses due to IP theft and whether the cyber attack impacted their spending on R&D and the loss of commercially sensitive data.
Comment on applicability of costs and ability to replicate	Survey approach to businesses is highly relevant for this study.
The cost of malicious cyber activity to the US economy, US Council of Economic Advisors, 2018	
Description of report contents and objectives	This report examines the economic costs that malicious cyber activity imposes on the US. economy.
Countries	US
Type of cyber-breach (with definition)	A malicious cyber activity is defined as an activity, other than one authorized by or in accordance with US. law, that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident thereon.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Cost for firms The least subjective method for estimating the impact of a cyber security events on a publicly traded firm is to quantify its stock price reaction to the news of such events. For a publicly traded firm, its market value reflects the sum of (1) the value of its current assets and (2) the present discounted value of all future free cash flows that the firm is expected to earn over its life span. In efficient capital markets, the market value will adjust quickly to reflect a new valuation following any news that affects the firm value. An **event study methodology** is used to calculate how market prices react to news of cyber attack or a data breach to quantify the impact on the firm's value. This the market's view of how the sum of these costs lowers the firm's value.

	In this analysis, the report uses the newsfeed from Thomson Reuters for public news of cyber attacks and data breaches at specific firms. They identify news of such events by searching news headlines for key words such as "cyber attacks", "hacking" and "data breach". To isolate the impact of the events on stock prices announcements of cyber attacks and data breaches that fall within seven days of a quarterly earnings announcement are removed. Analysis is from January 2000 to January 2017. To estimate the impact of an adverse cyber event on a firm's value, the reaction of its stock price over the event window that begins on the day that the adverse cyber event was publicly disclosed in the news and ends seven days after. The methodology used in prior event studies (e.g. Neuhierl, Scherbina, and Schlusche, 2013[1]) was used. Two widely used models were considered; the market model and the Capital Asset Pricing Model, to estimate baseline returns. Both models produce similar results. Only results based on the market model are reported. In the market model, the market return is subtracted from the stock return in order to calculate the abnormal stock return on each event day. These values are then summed over the event window to calculate a Cumulative Abnormal Return (CAR). Moreover, because Thomson Reuters frequently issues closely spaced updates on prior adverse cyber events, it is required that each subsequent news articles be at least seven days removed from the previous news—which effectively removes updates on a previously reported news item. The study improves on earlier studies with respect to the costs of adverse cyber events because it uses a longer and more complete dataset of such events and estimates the costs from stock price reactions. Additionally, the report details various case studies. These case studies, as well as other descriptions of cyber attacks and data breaches provided in the text, are based entirely on media reports and the authors' own calculations using public sources. Case studies investigate the spill over effects to economically linked firms.
Sample size	290 events experienced by 186 firms
Respondents characteristics (size and sector)	Because institutional customers of newsfeeds typically trade large and liquid stocks, newsfeeds disproportionately cover large firms.
Costs identified (with definitions)	▪ **Effect of firm's value** – the CAR effect on a firm's stock value ▪ **Costs associated with prevention** – acquiring security products (spam filters, anti-virus protection), training, fraud detection and tracking efforts ▪ **Wider economic costs** – stealing IP slows down the rate of development and adoption of new information and communication

[1] Neuhierl, Scherbina and Schlusche (2013) "Market Reaction to Corporate Press Releases," Journal of Financial and Quantitative Analysis, Vol. 48 (4), pp.1,207-1,240.

	technologies and thereby lowers the efficiency gains that can be achieved through these new technologies.
Comment on applicability of costs and ability to replicate	Includes costs for the government and wider economy which would not be relevant for businesses. The methodology used to calculate the effect of a cyber-breach on a firm's value would not be replicable by firms as it uses an event study methodology.
How data breaches affect stock market price, Comparitech, 2018	
Description of report contents and objectives	The report attempts to assess the extent to which investors react to data breaches and whether Wall Street punishes companies that leak customer data. Specifically looks at: ▪ The effect of a data breach on closing share price at various time intervals ▪ The percent difference in closing share price performance versus the NASDAQ over the same period of time from the day prior to a breach ▪ How long it takes for a share price to "bottom out" after a breach
Countries	US
Type of cyber-breach (with definition)	Looks at data breaches of over 1 million data records, broken down into: ▪ **Leaks of highly sensitive info** (credit card numbers, social security numbers) ▪ **Leaks of unencrypted passwords, secret questions and other log-in info** ▪ **Breaches of information that can't be directly used to access someone's account** but can be used to target account holders with advertisements, scams etc.
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Analysed the closing share prices of 28 companies, all of them listed on the New York Stock Exchange, starting the day prior to the public disclosure of their respective data breaches. Included are many of the largest data breaches in history; all of them resulted in at least 1 million records leaked, and some surpassed 100 million. Some companies were breached more than once, for a total of 33 breaches analysed. Compared the performance of each stock with the NASDAQ for the same time period and calculated the difference in performance between them. The NASDAQ is a common standard for overall market performance, and most of these stocks are listed on it. We used a NASDAQ composite index as a benchmark for the wider market. One of the biggest limitations to this study is sample size; there are not many companies that fit the criteria. As with any financial market study, there is a huge slew of factors that could affect stock price which cannot be accounted for.

Sample size	28
Respondents characteristics (size and sector)	Companies listed on the New York Stock Exchange, that had experienced a breach of 1 million or more records, where the breach had been publicly disclosed: Apple, Adobe, Anthem, Community Health Systems, Capital One, Dun & Bradstreet, Facebook, First American Financial, eBay, Equifax, Global Payments, Home Depot, Health Net, Heartland Payment Systems, JP Morgan Chase, LinkedIn, Marriott International, Monster, T-Mobile, Sony, Staples, Target, TJ Maxx, Under Armour, Vodafone, and Yahoo.
Costs identified (with definitions)	▪ Fall in a firm's **stock price** – looks at immediate and long-term impact on a firm's stock price. ▪ **Pay outs** – if a data breach leaks particularly damaging information that ultimately incurs financial damages to a company's customers, and the company was shown not to have adequately protected the information leaked in that breach, then customers often sue in class-action lawsuits. These usually result in settlements. ▪ **Other costs** disclosed in financial reports – while a company might divulge what information was leaked and how many records were affected in that initial disclosure, other consequences might not be revealed until the company releases its requisite quarterly shareholder report. This could include loss of sales or users, diverting funds to invest in data security, or other important information related to the breach that could cause investors to jump ship.
Comment on applicability of costs and ability to replicate	Limited applicability due to the methodological challenges of accurately measuring the effect of a cyber-breach on stock price and difficulty of firms being able to self-report this. Based on a small number of large firms that have experienced a significant breach.
Measuring the financial impact of IT security on businesses, Kaspersky, 2016	
Description of report contents and objectives	The report attempts to assess the economics of budgets used to safeguard businesses against potential financial losses caused by a security incident. To do this they look at IT security budgets, the complexity of their infrastructure, attitudes toward security threats and solutions and the real cost of data breaches and security incidence experienced.
Countries	25 countries, not specified
Type of cyber-breach (with definition)	▪ Viruses and malware causing a loss of productivity ▪ Inappropriate IT resource use by employees ▪ Physical loss of devices or media containing data ▪ Inappropriate sharing of data via mobile devices ▪ Loss of access to internal services ▪ Loess of access to customer-facing services ▪ Data loss/exposure due to targeted attacks

	▪ Incidences involving non-computing, connected devices ▪ Electric leakage of data from internal systems ▪ Incidents affecting suppliers that we share data with ▪ Incidents affecting third party cloud services we use ▪ Incidents affecting IT infrastructure hosted by a third a party ▪ Data loss/exposure due to attacks on point-of-sale (POS) systems (bank/retail only)
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	Global survey with more than 4,000 business representatives from 25 countries looking at their IT security budgets, the complexity of their infrastructure, attitudes towards security threats and solutions, and the real cost of data breaches and security incidents experienced.
Sample size	Over 4,000
Respondents characteristics (size and sector)	Business representatives
Costs identified (with definitions)	▪ Additional internal staff wages ▪ Lost business ▪ Employing external professionals ▪ Damage to credit rating/insurance premiums ▪ Extra PR (to repair brand damage) ▪ Compensation ▪ Improving software and infrastructure ▪ Training ▪ New staff
Comment on applicability of costs and ability to replicate	Costs are derived from a largescale survey of business representatives. However, the lack of definitions for identified costs limits the ability to replicate costs.
Enhancing the role of insurance in cyber risk management, OECD, 2017	
Description of report contents and objectives	This report provides an overview of the financial impact of cyber incidents, the coverage of cyber risk available in the market, challenges to market development and initiatives aimed at addressing those challenges. The report provides a series of policy recommendations aimed at enhancing the contribution of the cyber insurance market to managing this increasingly prevalent risk.
Countries	OECD countries

Type of cyber-breach (with definition)	The categorisation developed by the Chief Risk Officer (CRO) Forum (2016) is used which includes 4 broad categories: **Data confidentiality breach** The CRO Forum (2016) classification sub-divides data confidentiality incidents into 2 types: ▪ Incidents involving own confidential data (e.g. financial data, trade secrets, IP) ▪ Incidents involving third party confidential data (e.g. customers' personal information). Usefully, the classification of an incident in this category is based on the detection by a company of the confidential data "outside of its data perimeter" rather than the specific incident that led to the unauthorised release of data. This means that the scope of this category includes the many different underlying causes of the release of confidential data, ranging from improper disposal of company records to unauthorised access to a company's internal networks (often referred to as a "network security breach") **System malfunction/issue** The CRO Forum classification includes five sub-categories of system malfunction/issue: ▪ Own system malfunction ▪ Own system affected by malware ▪ Network communication malfunction ▪ Inadvertent disruption of third-party system ▪ Disruption of external digital infrastructure **Data integrity/availability** The CRO Forum classifies incidents involving the deletion, corruption or encryption of either own or third party data into a category on data integrity/availability. Similar to the data confidentiality category, the classification of an incident in this category is based on the detection of deleted, corrupted or encrypted data, rather than the underlying cause. The CRO Forum classification also establishes separate sub-categories for own and third party data. For the purposes of this report, 2 illustrative examples will be examined: ▪ The deletion or corruption of own or third party data due to a software error ▪ The encryption of own or third party data as a result of an intrusion by ransomware – there may be some differences in terms of consequences between incidents where the underlying data is own data or third party data, although this is most likely valid only in a minority of cases (e.g. where the impacted company has some kind of obligation to maintain a complete and accurate catalogue of third party data)

	Malicious activity The CRO Forum incident classification includes 3 sub-categories of malicious activity: ▪ Misuse of system (i.e. misuse of a digital system to distribute defamatory or embarrassing messages) ▪ Targeted malicious communication (e.g. phishing attempts aimed at securing confidential information) ▪ Cyber fraud, cyber theft (e.g. an unauthorised financial transfer) – for the purposes of this report, 2 illustrative examples will be examined: − The misuse of a system for defamatory statements − Cyber fraud/theft based on unauthorised network access and/or unauthorised use of financial credentials – one of the most common forms of targeted malicious communications ("CEO-phishing") is usually aimed at cyber fraud/theft
Methodology (including methodological challenges, strengths/weaknesses and overall assessment of its robustness)	The report is based on questionnaire responses received from the re/insurance companies and brokers active in this market globally and the ministries of finance and insurance regulators responsible for overseeing that market. Descriptions of the main categories of incidents and losses, based on definitions and a taxonomy developed by the insurance sector (specially by the Chief Risk Officers (CRO) Forum). In addition, evidence from the wider literature is used to evidence and support the reports' conclusions and recommendations.
Sample size	Not stated
Respondents characteristics (size and sector)	Responses to the questionnaire were received from the governments of Austria, Chile, Colombia, Costa Rica, Estonia, Finland, France, Germany, Hungary, Iceland, Israel, Italy, Japan, Latvia, Luxembourg, Mexico, Poland, Portugal, Russia, Slovak Republic, Sweden, Chinese Taipei, Turkey and the United States. In terms of insurance brokers, managing general agents and their associations, responses were received from the following organisations: A&I Member Services (Australia), Arthur J. Gallagher (Australia), BFL Canada Risk & Insurance, Burns & Wilcox (United States), Collegiate Management Services (United Kingdom), CGSC (United Kingdom), Managing General Agents' Association (United Kingdom), Marsh (Europe), Miller Insurance Services (United Kingdom), Price, Forbes & Partners (United Kingdom), SEIB Insurance Brokers (United Kingdom), The Council of Insurance Agents & Brokers (United States) and Willis Towers Watson (United Kingdom). In terms of insurance companies and their associations, responses were received from the following organisations: AIG (United States), Allianz Global Corporate & Specialty (Germany), Aviva (Canada), AXA (France), AXA (Italy), BTA Baltic Insurance Company (Latvia), CFC Underwriting (United Kingdom), Delta

	Insurance (New Zealand), ERGO Insurance (Latvia), Global Federation of Insurance Associations, Hollard Specialist Liabilities (South Africa), International Underwriting Association, Lloyd's (United Kingdom), QBE Europe (United Kingdom), SHA (South Africa), Telesure (South Africa), Zurich (Switzerland), an anonymous insurance company from Belgium and three anonymous insurance companies from Ireland. Responses were received from five reinsurance companies: General Re (United States), JLT Re (United Kingdom), Munich Re (Germany), Partner Re (Switzerland), and Scor (France).
Costs identified (with definitions)	▪ **Data and software loss** – costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted ▪ **Product liability or professional services errors and omission (E&O) liability/professional indemnity** – depending on the nature of the companies' business, a system or software malfunction leading to a defect in the company's product or a failure to provide adequate professional services could lead to a liability claim or class action by its customers ▪ **Physical asset damage** – if the system that malfunctions is involved in controlling the functioning of machinery or equipment (i.e. operational technology), damage to physical assets is possible. Damages to system hardware (whether or not as part of an operational technology failure) would also normally be considered physical asset damage ▪ **Technology errors and omissions (E&O) liability** – if the system or software that malfunctions was acquired from a third party technical services provider, the provider may face a liability claim related to the malfunction ▪ **Cyber ransom and extortion losses** – including the cost of experts to manage the incident and the amount of any ransom payment made ▪ **Cyber theft:** use of financial credentials to make an unauthorised transfer of funds or through deception (for example, by impersonating a company officer in an email seeking to initiate a transfer of funds). In these cases, the cyber fraud or theft would lead to pure financial losses (categorised as financial theft and/or fraud under the CRO Forum loss classification) ▪ **IP theft** – loss of value of an IP asset, resulting in pure financial loss ▪ **Incident response costs** – compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defence costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs; (ii) public relations and communications costs; (iii) remediation costs (e.g. costs to delete or cost to activate a "flooding" of the harmful contents published against an insured); (iv) notification costs ▪ **Network security/security failure [liability]** – compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incident response costs. The policyholder/observed company may not

	have any damage but has been used as a vector or channel to reach a third party ▪ **Regulatory & legal defence costs (excluding fines and penalties):** − Regulatory costs – compensation for costs incurred to the observed company or related third parties when responding to governmental or regulatory inquiries related to a cyber attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties) − Legal defence costs – coverage for own defence costs incurred to the observed company or related third parties facing legal action in courts following a cyber attack ▪ **Communication and media (liability)** – compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web page defacement as well as patent/copyright infringement and trade secret misappropriation ▪ **Legal protection** – costs of legal action brought by or against the policyholder including lawyer fees and costs in case of trial (e.g. identity theft, lawyer costs to prove the misuse of victim's identity) ▪ **Assistance coverage/psychological support** – assistance and psychological support to the victim after a cyber event leading to the circulation of prejudicial information on the policyholder without his/her consent ▪ **Products (liability)** – compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber event, excluding technical products or operations (technology E&O) and excluding professional services errors and omissions) ▪ **Directors and officers (D&O) (liability)** – compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event ▪ **Professional services E&O/Professional indemnity (liability)** – compensation costs related to the failure in providing adequate professional services or products resulting from a cyber event, excluding technical services and products (technology E&O) ▪ **Environmental damage** – compensation costs after leakage of toxic and/or polluting products consecutive to a cyber event
Comment on applicability of costs and ability to replicate	Provides detailed descriptions of types of cyber-breaches and potential losses that can be incurred as a result. However, it does not attempt to use these categories to estimate costs at a firm level. Examples of costs to firm are provided only at case study level using secondary data sources.

Ipsos MORI's standards and accreditations

Ipsos MORI's standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a 'right first time' approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

ISO 27001

This is the international standard for information security designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation.

Data Protection Act 2018

Ipsos MORI is required to comply with the Data Protection Act 2018. It covers the processing of personal data and the protection of privacy.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

Ipsos MORI