OXFORD ECONOMICS

Cyber-attacks: Effects on UK Companies

July 2014

A report for CPNI

CPNI
Centre for the Protection of National Infrastructure

OXFORD ECONOMICS

Contents

Executive Summary

Gary Becker's seminal 1968 paper on the economics of crime shaped the way economists think about crime policy and is still applied in many contexts today. Becker explored the decision making function of rational criminal actors, suggesting that criminals choose to engage in illicit activity based on their own assessment of the costs and benefits. Rational criminal actors weigh up the potential yield from a criminal act, the risk of being caught and the severity of the punishment.

The decision making process of state-sponsored cyber-attacks differs from that of ordinary criminals in important ways, which may potentially limit the direct applicability of the traditional economic models of crime such as Becker's. State-sponsored attackers are characterised by the very fact that a "non-profit" state entity is involved (as opposed to Becker's individual "for profit" criminals), potential information asymmetry, a perception of immunity from prosecution and the intangible value attributed to acts of patriotism (which does not figure in traditional economic approaches to crime, such as Becker's).

At the same time, there is value in understanding the economic theory of crime, as advanced by Becker. States are unlikely to change their activities in the short term, particularly because of non-pecuniary/distorted concepts of returns. However they may do so in the long term, especially if deterred by adequate security measures and changes in operational procedures, (i.e. if the costs of cyber-attacks rise) and as they realise that the returns to cyber-attacks may be mixed at best . This again points to a need for firms to understand the nature of - and threat posed by - current attacks, so as to raise the costs of cyber-attacks for nation-state perpetrators in order to help deter future attacks.

Apart from the implications for individual firms, cyber-attacks impact on the UK economy as a whole in two major ways:

- Increasing the cost of doing business
- Distorting the pattern of long run investment ("dynamic effects")

Survey work on the nature of cyber-attacks in the UK undertaken by Oxford Economics and the Ponemon Institute found the following:

- **Cyber-attacks are a common problem.** 60% of respondents had experienced a cyber-attack within the last 12 months.
- **Loss estimates were highest for damage to reputation/branding.** All other costs were reported with raw averages around the £2 million mark, with adjusted means slightly under half that and medians of £175,000. **However, the raw average reputation/branding loss estimate was £2.9 million.**
- **Intellectual property and commercially sensitive data is stolen in all sectors, but by no means happens to everyone.** With this in mind it is interesting to note that 80% of respondents reported that they had not experienced any IP or commercially sensitive information loss in the last 24 months.

- **The majority of firms who did suffer a loss of IP or commercially sensitive information felt they were damaged by it.** 61% said that they had experienced a loss of competitive advantage due to the loss of IP. 59% said that they had experienced a loss of competitive advantage due to the loss of commercially sensitive information.
- **The most common loss of competitive advantage came in the shape of "compromised negotiations or business ventures"** (31%), followed by the "appearance of copied products or practises" (20%) and the "emergence of new competition" (19%).
- **While only a minority of companies suffer IP/commercially sensitive information losses, the cost of such losses is considerably higher than is the case for "day to day" losses.** The adjusted mean loss of IP was valued at £13.2 million and the adjusted mean loss of commercially sensitive business information was valued at £12.8 million.

In addition to the survey of UK firms, which identifies the direct costs incurred as a result of cyber-attacks, Oxford Economics has undertaken an event study to analyse the potential reputational loss firms may suffer. As a proxy for reputational damage we use negative stock market returns that may be experienced immediately around the public disclosure of a cyber-attack.

Although further confirmatory analysis would be useful, our results suggest that publicised cyber-attacks do generally have impacts on stock market valuations and, by extension, upon corporate reputations. If this is the case, it means that the investment companies make in IT security to prevent these attacks may maintain shareholder value for these companies.

1 Introduction

The Centre for the Protection of National Infrastructure (CPNI) has requested that Oxford Economics carry out a study of the impact of state-sponsored cyber-attacks on UK firms.

The project consists of four 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

Cyber-attacks are a complex topic. They are both difficult to detect and difficult to measure the impacts of. For that reason, a variety of theoretical, empirical, and qualitative research frameworks were applied to get to the heart of the impact of these attacks on UK firms and what this means for UK plc.

Numerous studies have attempted to place a value on the cost of cyber-attacks to the national or global economy but, due to the lack of transparency as well as other statistical problems, estimates are sketchy and spread over a very wide range. This report focuses on UK companies' experience of cyber-attacks and on the broader "cyber-attack landscape" rather than on attempting to derive a specific cost impact for the effects of cyber-attacks on the UK economy.

2 Economic framework – Impact of state-sponsored cyber-attacks on UK firms

2.1 Counting the cost of cyber-attack: previous studies and pitfalls

The costs associated with cyber-attacks are not transparent. Companies are often guarded about the extent of their losses from cyber-attacks for fear of reputational damage or litigation. In the case of state-sponsored attacks, the companies will be wary of the impact any revelations could have on their strategic relationship with that originating state.

Numerous studies have attempted to place a value on the cost of cyber-attacks to the national or global economy but, due to the lack of transparency as well as other statistical problems, estimates are sketchy and spread over a very wide range. A study carried out by Detica for the Cabinet Office in 2011[1] came under criticism for its estimate that cyber-attacks cost the UK economy £27bn per year, with industry experts and academics claiming many of the assumptions were overblown. A McAfee report from 2013[2] estimated a £100bn annual cost to the US economy using proxy valuations from other sectors. However, Florencio and Herley (2013)[3] in a study for Microsoft Research argue that all aggregate cost estimates for cyber-attacks suffer from an upward bias, partly as a result of extrapolating small survey samples to the entire economy, partly because cost estimates by their very nature only allow for positive errors (zero provides a hard floor to estimates, but there is no ceiling).

Surveys of this nature could also be vulnerable to other statistical discrepancies, such as non-response bias (if for example those who suffered an attack were more likely to respond to the survey than those who didn't) or non-representative sample bias (meaning the estimates cannot be accurately scaled up to represent the entire population).

In response to Florencio and Herley's conclusions, one might argue that the apparent exaggeration of costs by survey respondents is not so clear cut. Some of the very large outliers may indeed be a reflection of true outliers in the general population. Alternatively, sample outliers could understate "true" population outliers. The key issue is that the limited number of observations could induce bias in either direction. Further, many respondents may well be underplaying the cost of cyber-attacks, rather than exaggerating it. Such behaviour would follow the historical pattern of many firms that are a victim of fraud (and which historically has made the estimation of fraud so difficult).

---

[1] Detica, Office of Cyber Security and Information Assurance in the Cabinet Office "The Cost of Cyber Crime" (2011).

[2] McAfee, Centre for Strategic and International Studies "The Economic Impact of Cybercrime and Cyber Espionage." (2013)

[3] D. Florencio, C. Herley "Sex, Lies and Cyber-crime surveys". Microsoft Research. (2013)

Other studies have used a survey methodology to develop a richer understanding of the experiences of individual firms, avoiding the pitfalls of extrapolating the estimates to the entire economy. The UK Government Department for Business, Innovation and Skills (BIS) together with PWC and Infosecurity Europe[4] performs an annual survey of businesses, which found in 2013 that the average cost of information breaches among its sample (over 1,400 respondents) were rising, with several breaches costing upwards of £1 million. A survey by the Ponemon Institute in late 2013[5] found that among its 36 (UK) company sample, companies were being successfully attacked more than once per week and the most costly attacks were those caused by malicious insiders, denial of service and web-based attacks.

This report focuses on UK companies' experience of cyber-attacks and on the broader "cyber -attack landscape" rather than on attempting to derive a specific cost impact for the effects of cyber-attacks on the UK economy.

That said, understanding the broader economic impact is important because it helps to illustrate how and why cyber-attacks represent a problem not just for individual UK companies but for the country as a whole. This issue is discussed below.

In considering economic issues, we have also assumed that the study is effectively "ringfenced" so that it is concerned only with economic effects on the UK. (We do however, relax this assumption at specified points in the discussion below to illustrate how, even on a global level, cyber-attacks can be detrimental to growth.)

2.2 A framework for understanding the impact of cyber-attacks

2.2.1 Why do nations engage in cyber-attacks?

Gary Becker's seminal 1968[6] paper on the economics of crime shaped the way economists think about crime policy and is still applied in many contexts today. Becker explored the decision making function of rational criminal actors, suggesting that criminals choose to engage in illicit activity based on their own assessment of the costs and benefits. Rational criminal actors weigh up the potential yield from a criminal act, the risk of being caught and the severity of the punishment.

It is worth considering whether Becker's ideas on returns and risk influence whether or not government sponsored cyber-attacks are launched at UK firms.

[4] BIS, PWC, Infosecurity Europe. "2013 Information Security Breaches Survey. A Technical Report" (2013)

[5] Ponemon Institute "2013 Cost of Cyber Crime Study: United Kingdom" (2013)

[6] G. S. Becker (1968) Crime and Punishment: An Economic Approach, Journal of Political Economy 76:169-217

2.2.2 The returns to illegal activity

The yield associated with an attack on a UK firm will depend on the type of attack and the timing. Stealing secret commercial information can potentially be extremely lucrative, but only if the attacker can use the information while it is still of use. Some have argued that intellectual property and commercially sensitive business information often has a very short shelf-life before it falls out of date or is overtaken by new developments. Alternatively, it may be difficult to apply such technology given its complexity, especially given the interlocking nature of modern technology.

Unlike the targets of the attacks themselves, the individuals carrying out cyber-attacks may not be in a position to know this, so a form of "information asymmetry" may occur. Arguably then it may be more difficult to make a return on cyber-attacks than is the case with traditional crimes such as burglary, to which Becker's model has been applied in the past.

Moreover, other forms of cyber-attacks, such as a Distributed Denial of Service (DDOS) attacks, are aimed at causing harm to the victim rather than being commercially lucrative for the attacker.

Unlike individual criminals, it may be difficult for the attackers themselves to make direct "revenues" from their activities. Rather their efforts may be passed on to other elements of government or the business community – e.g. the military, commercial negotiators. At the same time, organisations engaged in cyber-attacks incur costs. Staff must be trained and paid and systems maintained[7].

By their very nature, the organisations engaged in cyber-attacks would therefore not be expected to make a "profit" in the sense of Becker's individual criminals. Nor, given the long term and amorphous issues involved, is it even clear that the states involved would even make a positive return (in either an economic or a financial sense) from such activities.

Becker's model might therefore appear to be of limited applicability to state sponsored cyber-attacks in this sense. However, the same considerations which apply to individuals in the short term may apply to states in the long run. Cyber-attacks are relatively new. As states learn more about its potential costs and benefits it is likely that they will refine their activities and become more targeted in their approach. Some anecdotal evidence, as well as evidence from the survey conducted for this report, suggests this may already be occurring (see for example the responses to Questions 9b and 9c).

Furthermore, there can be very significant non-monetary motivations behind state-sponsored cyber-attacks. These have been studied on the individual level

[7] While these are *not* costs borne by the UK, they do represent opportunity costs for the economies of the originating nations – and by extension global costs of crime. Those staff could be used elsewhere in the economy rather than merely seeking to transfer knowledge which has already been generated, for example. Likewise, Becker also pointed to such opportunity costs as a part of the costs of crime – e.g. many burglars could be employed elsewhere, creating wealth rather than seeking merely to "transfer" it.

in the past. Khetri (2009)[8] identifies many examples of patriotic and nationalistic motivations in malicious cyber activities, pointing to "cyber-wars" taking place between China and competitors including Taiwanese, Japanese and US hackers. Thus, some cyber-attackers justify their actions under the banner of patriotism rather than acknowledging any "criminal" behaviour on their own part.

While states do not tend to publicise or brag about their cyber activities, such motivations may well form a part of an unofficial narrative, particularly in the case of states who feel they have been denied rightful access to ideas or technologies.

2.2.3 The direct costs: risk of detection and severity of punishment.

Certain types of cyber-attack are easier to conceal than others. For example, a hacker attempting to remotely exfiltrate data from a target is potentially more exposed precisely because the stolen data is sent somewhere, though some perpetrators do not really worry about being detected, so long as they are able to get the information they require. Acts of sabotage are easier to cover up (if desired).

However, the international nature of cyber-attacks complicates the victim's understanding of the origin of any attack and the risk of punishment for state-sanctioned or state-sponsored cyber-attacks is low in any event. There is no established, universal legal framework to depend on, and efforts to build international mechanisms for internet -governance and cyber-crime cooperation are still at an early stage. Bilateral action when cyber-attacks do occur is heavily constrained by legal and diplomatic boundaries.

Unlike Becker's individual criminals then, countries cannot easily be sent to jail and there are constraints on any form of punitive measure. At the same time Becker's framework is still of use in understanding the pervasive nature of cyber-attacks. A criminal who faces no sanctions is more likely to continue with their activities and lacking an effective punishment, states might likewise be encouraged.

Difficulties arise even when activities occur in the "grey" world of "state encouraged" (as opposed to state sponsored or organised) cyber-attacks. Khetri (2009) suggests the propensity of the criminal justice system to prosecute cyber criminals in Russia and China is generally low, unless the act jeopardises national interests or national security. His work found that much of Russian society sees cyber-attacks directed at the West as a form of "gentleman's misdemeanour" or even a "heroic" act, and the courts and security services echo this opinion. Individuals indicted for cyber-attacks have had charges dropped and have later appeared as advisers to the Russian government[9].

[8] N. Khetri (2009) "Positive externality, increasing returns and the rise in cybercrimes", Communications of the ACM, 52(12), 141-144.

[9] A. Klimburg (2011) "Mobilising Cyber Power" Survival vol 53.no. 1 (February-March 2011) pp 41-60

Klimberg (2011)[10] argues that the state has an interest in maintaining or tolerating cyber-criminal organisations because they can be used as deniable proxies for future offensive efforts and thus contribute to the state's cyber security posture. He suggests the more easily traceable attacks, such as DDOS and web-defacement attacks, are likely to operate with at least tacit approval from the state and many observers believe that the more resource-intensive, sophisticated attacks must have state backing.

2.3 Implications for UK plc?

2.3.1 Capacity for response

The decision making process of state-sponsored cyber-attacks differs from that of ordinary criminals in important ways, which may potentially limit the direct applicability of the traditional economic models of crime such as Becker's. State-sponsored attackers are characterised by the very fact that a "non-profit" state entity is involved (as opposed to Becker's individual "for profit" criminals), potential information asymmetry, a perception of immunity from prosecution and the intangible value attributed to acts of patriotism (which does not figure in traditional economic approaches to crime, such as Becker's).

The assessment of both returns and risks of state sponsored cyber-attacks may therefore differ markedly from those suggested by traditional economic approaches, at least in the short run.

This implies that the scope for UK enforcement agencies to change the behaviour of state-sponsored cyber-attackers by influencing their cost benefit evaluations is limited. Likewise, UK businesses are not able to change the environment they operate in. Rather, they must invest their resources in understanding the risks they face and take operational decisions based on those risks.

At the same time, there is value in understanding the economic theory of crime, as advanced by Becker. States are unlikely to change their activities in the short term, particularly because of non-pecuniary/distorted concepts of returns. However they may do so in the long term, especially if deterred by adequate security measures and changes in operational procedures, (i.e. if the costs of cyber-attacks rise) and as they realise that the returns to cyber-attacks may be mixed at best[11]. This again points to a need for firms to understand the nature of - and threat posed by - current attacks, so as to raise the costs of cyber-attacks for nation state perpetrators in order to help deter future attacks.

[10] A. Klimburg (2011) "Mobilising Cyber Power" Survival vol 53.no. 1 (February-March 2011) pp 41-60

[11] To provide a similar example, the falling rate of bank robberies in the UK appears to be the result of long term changes in security measures and operational procedures – see http://www.bbc.co.uk/news/technology-25526671

2.3.2 Economic implications

Apart from the implications for individual firms, cyber-attacks impact on the UK economy as a whole in two major ways:

- Increasing the cost of doing business
- Distorting the pattern of long run investment ("dynamic effects")

A number of costs at the firm level were highlighted in the survey work undertaken for this study (see Appendix 2). However, these effectively amount to the fact that the presence of cyber-attacks pushes up the cost of doing business in the UK. New security systems must be developed, downtime is increased, productivity is adversely affected, IP is lost and investment may be deterred (or wastefully repeated).

In standard microeconomic terms this has the effect of pushing firm supply curves upwards and to the left as the supply of each unit of a product becomes more expensive to produce, thus reducing overall economic welfare by making each good less "affordable" for end consumers[12]. In parallel, as each unit of output becomes more expensive to produce because of the added burden of cyber-attacks, the long term productivity of the UK economy is reduced, inhibiting long run economic growth[13].

Apart from raising production costs, cyber-attacks may also have (negative) "dynamic effects", by distorting long term investment patterns. A 2013 study by the Brookings Institute[14] observed the varied impact that cyber-attacks have on different sectors of an economy. They suggest that highly competitive and innovative sectors such as consumer electronics are particularly vulnerable to the theft of commercially sensitive data, for example regarding a strategic product launch, whilst knowledge driven sectors like chemicals are vulnerable to the theft of IP that might undermine large R&D investments. The conclusion is

---

[12] Assuming that higher fixed costs are passed through to product prices. Note that while some "secondary" industries (e.g. those focussed on developing cyber-attack security systems) may prosper as a result, the net effect on the economy is still negative and is represented through the impacts on the "primary" demand and supply curves of the organisations directly impacted by cyber-attacks. A good discussion of these issues is provided in Boardman, A., Greenberg D., Vining, A., Weimer D., (2005) *Cost-Benefit Analysis* (3rd Edition).

[13] Of course, some of the IP and commercially valuable information stolen by cyber criminals could in theory boost growth in other economies. As this study is ringfenced to the UK, that would not seem directly relevant, though to continue the argument, some might maintain that "sharing" information with foreigners would produce global spillover effects which would be positive for the UK and other countries in the long run. However even using this global perspective "forced" spillovers are unlikely to be economically efficient, as returns are not properly allocated and incentives to invest are reduced in the long term. Apart from this, as noted, there is the complication that cyber-attacks may not actually yield benefits. Moreover, even where there are some gains, some have suggested that a free ride via cyber-attacks might deter long run innovation in the originating states (McAfee 2013).

[14] A. Friedman, A. Mack-Crane, R. Hammond, Brookings Institute Center for Technology Innovation "Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences" (2013)

that cyber-insecurity distorts the distribution of long term capital investment and hence productive economic activity across sectors of the economy. In this way, cyber-attacks, by taking the economy on an alternate growth path, could negatively affect long term economic performance.

So, taking together the points made above, from a global perspective the net total costs of cyber-attacks could include the increased costs of doing business and distorted investment patterns in the "victim" country (even after allowing for "forced" spillover growth), the opportunity costs of carrying out the crime by the attacker, and any negative effects on innovation in the originating states.

2.4 Cyber-attacks cost typology

Economic frameworks in respect of cyber-attacks have been discussed above. As indicated these essentially boil down to the fact that cyber-attacks increase the costs faced by UK firms (though there may be other dynamic effects in the long run such as changes to overall investment patterns).

One well known typology used for assessing the costs of crime, consistent with the microeconomic framework above is that of Brand and Price from their 2000 Home Office Research Study[15]. Brand and Price identify three categories of crime costs:

- Costs incurred in anticipation of crime, such as security expenditure and insurance administration costs. These costs fall mostly on potential victims of crime.
- Costs incurred as a consequence of criminal events, such as property stolen and damaged, emotional and physical impacts and health services. These costs fall mainly on victims, but also on services dealing with the consequences, such as health services.
- Costs deriving from the response to crime, such as costs to the criminal justice system. These fall mainly on the tax payer.

In order to assist in understanding how cyber-attack acts themselves are impacting on firms, this study is mainly concerned with the second of these costs – the costs incurred as a consequence of cyber-attacks. Nonetheless, the applicability of this typology to cyber-attacks in respect of all three of these costs is considered below.

2.4.1 Costs in anticipation of crime

These costs include expenditure on cyber security including software, staff costs and training.

[15] S. Brand, R. Price (2000) "The Economic and Social Cost of Crime" Home Office Research Study 217

While the focus of this study is on actual costs incurred as a result of actual cyber-attacks, we also asked survey respondents about their security posture (see the discussion of survey results below).

Estimates of the amount spent on cyber-security are notoriously difficult to come by as accounting procedures differ across firms. The 2013 BIS information security survey[16] found that around 10% of the IT budget was being spent on security among its sample, an increase from 8% a year earlier. The portion was larger for small and medium sized companies. A large UK technology firm, interviewed as a part of a case study for the current research, suggested large organisations were not taking cyber-crime seriously unless they were spending $6 million per annum. Also within that range, another multi-national organisation estimated they spend in the region of 1-2% of a $50 million IT budget on security, but could not provide exact figures.

Other costs may also exist for the firm in anticipation of crime. For example, the reduction in productivity (loss of time) due to extra security measures, "clunky" software etc. as well as other related incidental costs, such as insurance administration costs.

As indicated, since the focus of this study is on costs incurred as a result of actual cyber-attacks we have not attempted to directly quantify the anticipation costs faced by UK firms in the course of this study.

Nonetheless, work by the Ponemon Institute in the United States, using categories similar to those used in the survey work undertaken for the current study did examine the issue of preventative spending. Based on 503 respondents, they summed cyber clean-up and remediation costs and prevention costs, finding that they accounted for 37% and 63% of the resulting total respectively. The "raw" mean for cyber clean up and remediation costs in the current study was found to be £2.3 million over 24 months (or £0.8 million if adjusted for outliers). If carried through to the UK this would imply a "raw" average cost of £3.9 million for prevention costs over 24 months, or an (outlier) adjusted average of £1.4 million. (However note that prevention costs include amortised capital investments, which could have a substantial influence on the figures.)

2.4.2 Costs as a consequence of criminal acts

These costs are potentially the largest but also the most unclear. Understanding the nature of such costs is one of the motivations behind the current study. The typology used in the survey conducted for this study identifies the following costs:

- clean-up or remediation costs in the wake of any given cyber-attack;
- lost user productivity;
- disruption to normal operations;

[16] BIS, PWC, Infosecurity Europe. "2013 Information Security Breaches Survey. A Technical Report" (2013)

- damage to or theft of IT assets or infrastructure;
- the damage to a firm's reputation or brand value;
- the damage to competitiveness due to stolen intellectual property; and
- damage to competitiveness due to loss of commercially sensitive information.

Cyber insecurity might also produce some indirect spill-over costs for UK firms, due to the interconnectedness of supply chains and business networks in the UK and internationally. For example firms might suffer indirect costs if one link in their supply chain is damaged by cyber-attack.

We explore the direct costs, although not indirect costs, of cyber-attack through an industry survey and event analysis, in the following chapters.

2.4.3 Costs of enforcement

This strand of costs is minimal for state-sponsored cyber-attacks. International law on cybercrime is weak and asymmetric and international cyber-attacks are virtually impossible to prove. They are also potentially costly to make public if they risk damaging a broader diplomatic and economic relationship.

Nonetheless the UK's costs in this area are not £0. Efforts are being made at establishing international accords and principles to govern cyber space and the UK government also works bilaterally with other countries to try and resolve problems of infringements in cyber space and intellectual property theft. This represents an opportunity cost. The diplomatic resource could be more productively spent on more profitable endeavours for UK plc, through the extent of this cost cannot easily be separated out and assessed. Also note that while such costs form a part of the total economic costs of cyber-attacks in the UK they would accrue to the UK government rather than directly to UK firms (though they also impose an implied cost at the margin, as governments are, in part, financed via company taxation).

3 Survey results

3.1 Background

In order to better understand the nature of cyber-attacks in the UK and how it affects UK businesses Oxford Economics sub-contracted the Ponemon Institute to undertake survey work on the nature of cyber-attacks in the UK.

The Ponemon Institute has a background in survey work on cyber-attacks both within the UK and internationally. It has produced a variety of international publications on the issue, including the *Cost of Cyber Crime Study: United Kingdom.*

An email/internet-based survey process was used to undertake the work. The Ponemon Institute has built up a propriety database of IT professionals, IT security practitioners and other IT related roles as a result of its past survey work. A total of 9,973 surveys were sent out to UK firms on this database during January 2014, with a number of filters in place to help ensure survey reliability.

A sample of 427 responses was obtained (after screening for 68 rejected surveys), an effective response rate of 4.3%.[17] According to the Ponemon Institute, the response rate for a learned panel of IT and IT security practitioners is normally between 2.75 to 5.0 percent. Hence, the 4.3% response rate obtained is above the mean. 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.

The survey targeted those with responsibility for IT-related functions, including budgets, performance, strategy and security.

This chapter presents a summary of responses along with a related discussion of key issues. Appendix 1 provides a copy of the survey questionnaire. Detailed survey responses are presented in Appendix 2, along with some graphical presentation of responses not presented in this chapter, with the exception of Question 17 (Q17). Appendix 3 includes the responses to Q17.

[17] The Ponemon Institute examined late response differences to determine the possibility of non-response bias (a common method for checking for such bias). Ninety-one responses captured on or after day seven of the 14-day survey were determined to be late. A total of eight (8) survey questions were randomly selected to determine the potential impact of time on responses. The Ponemon Institute was unable to find significant differences between early and late responders, suggesting no evidence of non-response bias.

3.2 Survey demographics

Information on respondents:

- Position
- Industry classifications (broken up into 18 industry groups)
- Global organisation headcount
- UK headcount
- Global organisational revenue
- UK revenue

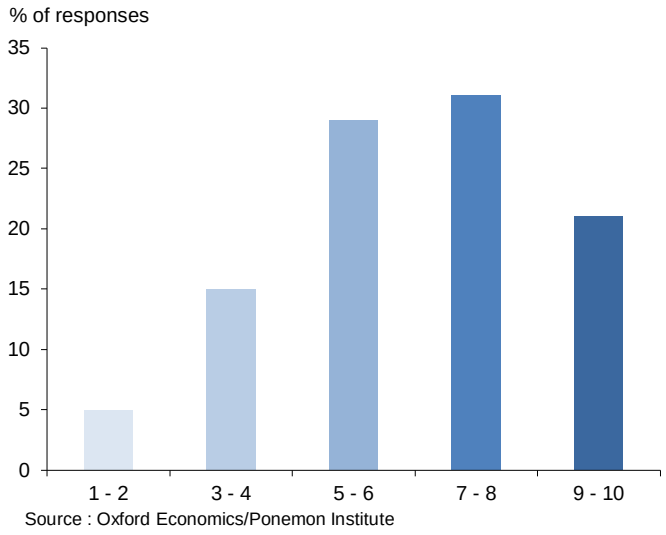
Full respondent demographic data is presented in Appendix 2.

3.3 Security Posture

Questions 1 – 2, 10 and 11 and 12 related to respondents' security posture with respect to cyber-attacks.

Results show that companies sampled have a moderately confident view of their cyber security preparedness. 21% of respondents graded their cyber security postures as 9 or 10 out of 10, with a further 31% choosing 7 or 8/10. Only one fifth marked their own posture below 4/10 (Q1).

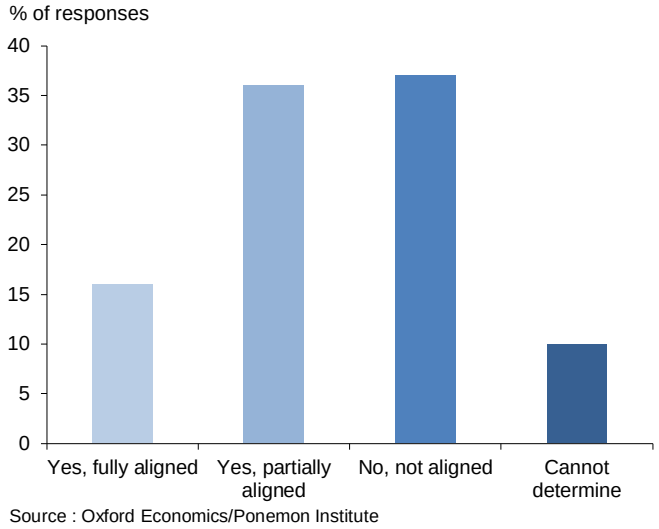
Chart 3.1: Q1 "How would you rate your organisations' cyber security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)?" (1=Not Effective, 10=Very Effective)



Source : Oxford Economics/Ponemon Institute

Half of respondents considered their cyber-security strategy to be partly or fully aligned with their business objectives and mission (Q10).

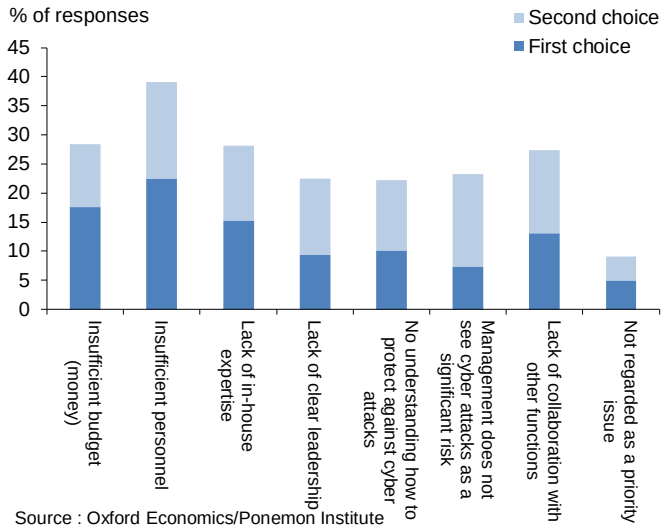
Chart 3.2: Q10 "Is your organisation's cyber security strategy aligned with its business objectives and mission?"



Source : Oxford Economics/Ponemon Institute

The lack of dedicated resources to sufficiently deal with the threat was a common theme. The leading cause for cyber insecurity cited by the sample was insufficient personnel (cited by 39%), followed by insufficient budget (cited by 28%) then a lack of in-house expertise (also 28%). Roughly one fifth of respondents pointed to management issues such as a lack of clear leadership and not assessing cyber-attacks as a significant risk as a key challenge (Q11).

Chart 3.3: Q11 "What challenges keep your organisation's cyber security posture from being fully effective? Please select the top two choices only."



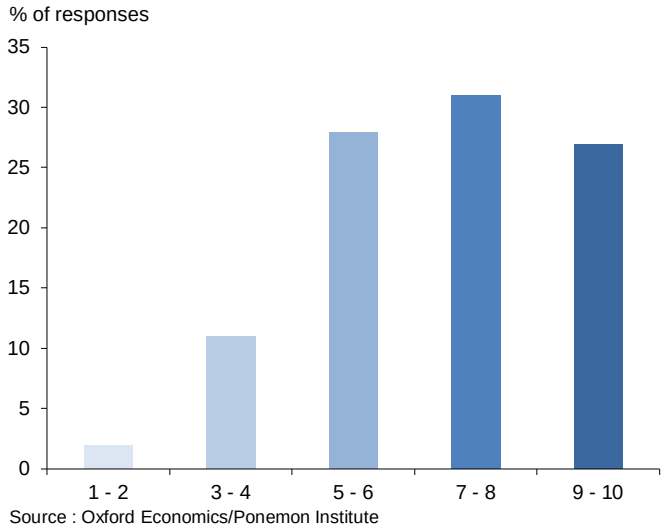
Source : Oxford Economics/Ponemon Institute

The survey designers, Ponemon Institute, commented that past studies have revealed a perennial problem with IT security departments securing approval for funding bids due to the unpredictability of the projected costs and benefits, and

the difficulties this causes them in justifying value for money to the Executive Board.

Achieving a fully effective cyber security posture is not easy. 27% of respondents rated the difficulty as 9 or 10/10, (where 10 = very difficult) with a further 31% choosing 7 or 8/10 (Q12).

Chart 3.4: Q12 "Using the following scale, how difficult is it for your organization to achieve a fully effective cyber security posture? 1 =not difficult and 10 = very difficult."



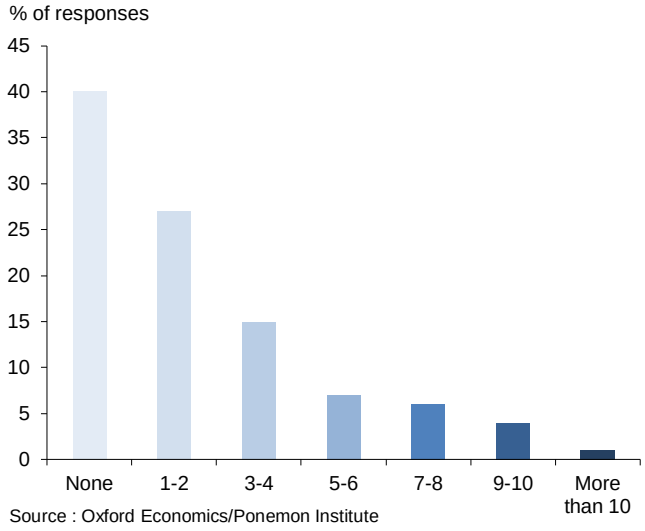
Source : Oxford Economics/Ponemon Institute

3.4 Cyber-attack experience

Questions 3 – 9 and 13 related to respondents' experience of cyber-attacks. The results are reported in Appendix 2, however a number of key findings are summarised below.

Cyber-attacks are a common problem. 60% of respondents had experienced a cyber-attack within the last 12 months (Q3).

Chart 3.5: Q3 "How many cyber-attacks has your organization experienced over the past 12 months?"

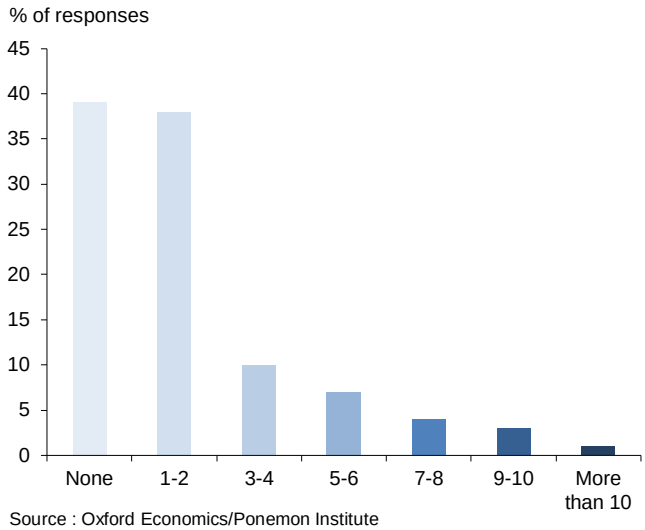


Source : Oxford Economics/Ponemon Institute

Of those that experienced an attack in this period:

- 31% lost sensitive information (Q4)
- 78% experienced an attack that had evaded intrusion detection systems (Q5a)
- 76% of respondents had experienced a cyber-attack that evaded their anti-virus software (Q5b)
- 61% of exploits were considered to be Advanced Persistent Threats (APTs) (5c)

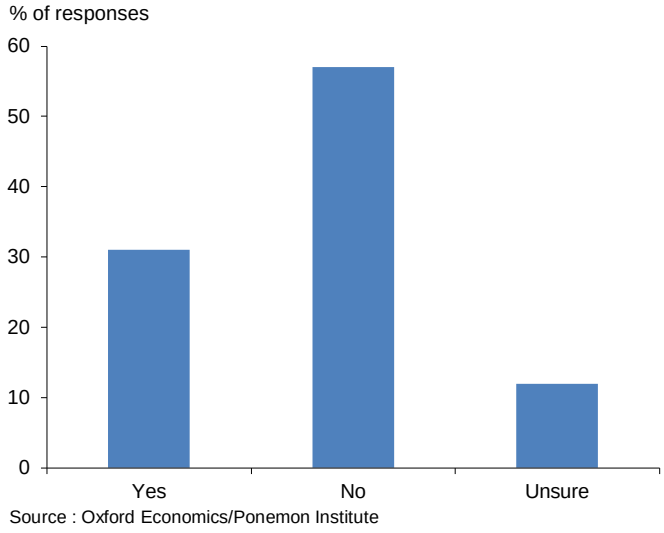
Chart 3.6: Q6 "How many separate APT-related incidents did your organisation experience over the past 12 months?"



Source : Oxford Economics/Ponemon Institute

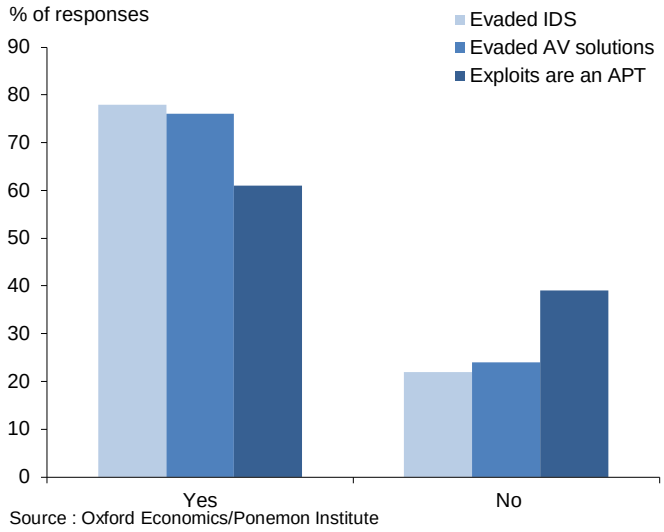
APTs can be seen as a likely proxy for government-sponsored cyber-attacks, although in recent years, a few criminal syndicates (not affiliated with a nation state) have been detected launching APT-type attacks against companies. Nonetheless, these attacks are quite sophisticated and it is likely that most are still perpetrated by nation states. Conversely, it should be noted that even attacks not identified as APTs, could still be the result of state sponsored activity, as respondents may not have realised they were being targeted by a state-sponsored entity.

Chart 3.7: Q4 "Has your organisation experienced an incident involving the loss or exposure of sensitive information in the past 12 months?"



Source : Oxford Economics/Ponemon Institute

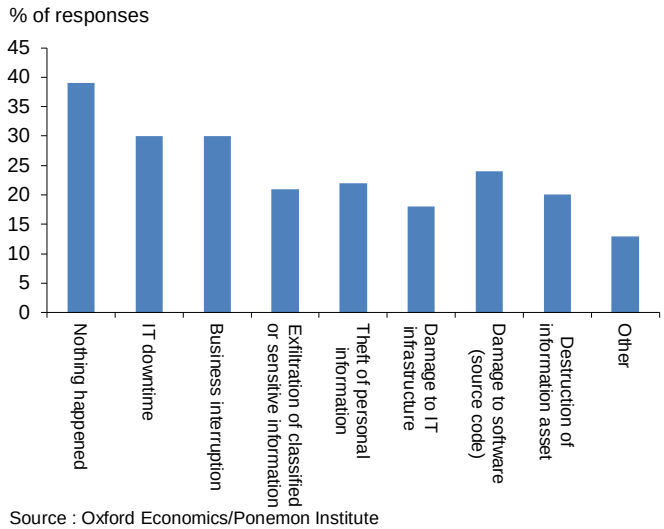
Chart 3.8: Q5a "Has your organisation ever experienced situations when cyber-attacks have evaded your intrusion detection systems (IDS)?"
Q5b "Has your organisation ever experienced situations when cyber-attacks have evaded your anti-virus (AV) solutions?"
Q5c "Do you consider any of these exploits an APT?"



Source : Oxford Economics/Ponemon Institute

Although nothing happened in 39% of cases of APTs, IT downtime and business interruption were common consequences (each reported by 30% of respondents). 24% reported software damage, while 22% reported theft of personal information and 21% of classified or sensitive information (Q7).

Chart 3.9: Q7 "What happened to your organisation as a result of the APTs it experienced? Please select all that apply."



Source : Oxford Economics/Ponemon Institute

Companies perceive "criminal syndicates" to be the number one perpetrators, followed closely by "nation-state attackers". In the experience of CPNI, however, attacks from criminal syndicates are far easier to detect. Many victims of state sponsored cyber-attacks are unaware they have been compromised. Other types of attackers were seen as considerably less likely to launch attacks, with "Other corporations" considered least likely to launch an attack (Q8).

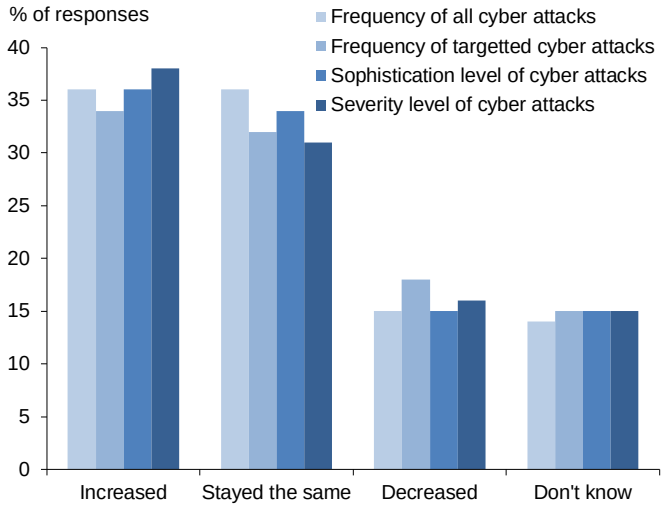
Table 3.1: Q8 "Please rank order the following types of attackers from 1 = most likely to launch to 6 = least likely to launch an attack against your company."

	Average rank	Rank order
Criminal syndicates	**2.29**	**1**
Nation-state attackers	**2.4**	**2**
Cyber-terrorists	**3.6**	**3**
Lone wolf hackers	**3.93**	**4**
Hacktivists	**4.04**	**5**
Other corporations	**4.93**	**6**
Average	**3.53**	

Source: Oxford Economics/Ponemon Institute

Between 34%-38% of respondents considered the frequency, sophistication and severity of cyber-attacks to have risen over the past 24 months and only 15%-18% to have fallen (Q9a,b,c,d).

Chart 3.10: Q9a "Within your organisation how has the frequency of all cyber-attacks changed?"
Q9b "Within your organisation how has the frequency of targeted cyber-attacks changed?"
Q9c "Within your organisation how has the sophistication level of cyber-attacks changed?"
Q9d "Within your organisation how has the severity level of cyber-attacks changed?"

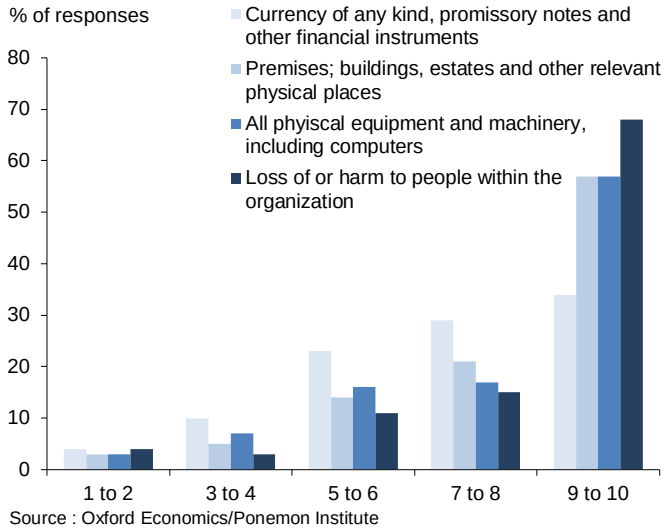


Source : Oxford Economics/Ponemon Institute

Examination of cross-tabs, matching industry classification to Q9c found particularly high levels of agreement with the proposition that the sophistication of attacks had increased amongst those in construction (66.7%, n=12), automotive (60%, n =10), mining (44.4%, n=9), financial services (43.3%, n=60), manufacturing (43.2%, n=44) academia and aerospace and defence (both 42.9%, n=7 and n =14 respectively) in our sample. However caution must be expressed about these results given the small sample sizes for individual industries and that this represents a sample of firms that may not be representative of the landscape of firms in the UK economy.

Respondents identified the organisation's "people" as the asset a cyber-attack would harm the most with an extrapolated average rating of 8.47/10 out of a variety of tangible assets including people, buildings, plant and equipment money and materials (Q13a1-5).

Chart 3.11: Q13a "The following table provides five tangible assets that may be put at risk as a result of cyber-attacks against your company. Please rate each asset type using the following scale to denote the potential impact of asset compromise to your organisation: 1 = no impact to 10 = maximum impact."

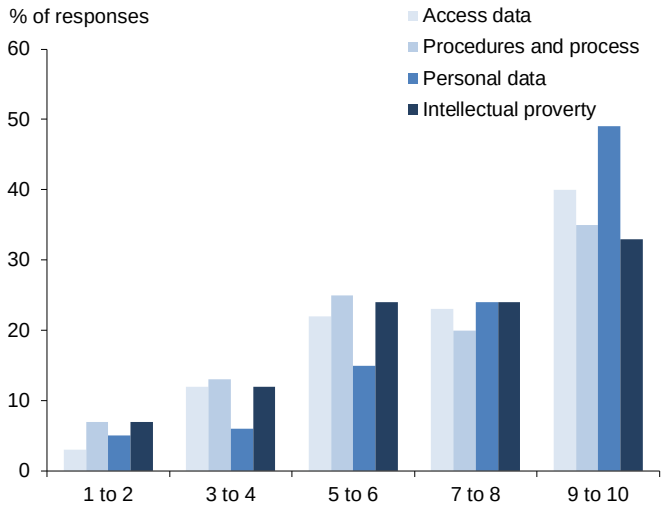


Source : Oxford Economics/Ponemon Institute

Respondents were also asked about information assets at risk from cyber-attacks, with the most impactful information asset breach identified as relating to "personal data" (7.66/10). Other types of information assets included access data (which allowed access previously prevented by security measures), procedures and process (how things work within organisations), intellectual property and commercially sensitive information (Q13b1-5)[18].

[18] Interestingly enough, compromise of "intellectual property" and "commercially sensitive information" were regarded by the respondents as the relatively least impactful of information breaches. However, this may reflect the fact, noted below, that 80% of survey responses did not believe they had experienced such compromises. As discussed below, losses amongst the sub-group who *did* experience such breaches appear to be much more serious than that for other forms of cyber-attacks. Furthermore, losses of intellectual property and commercially sensitive information are the hardest to value.

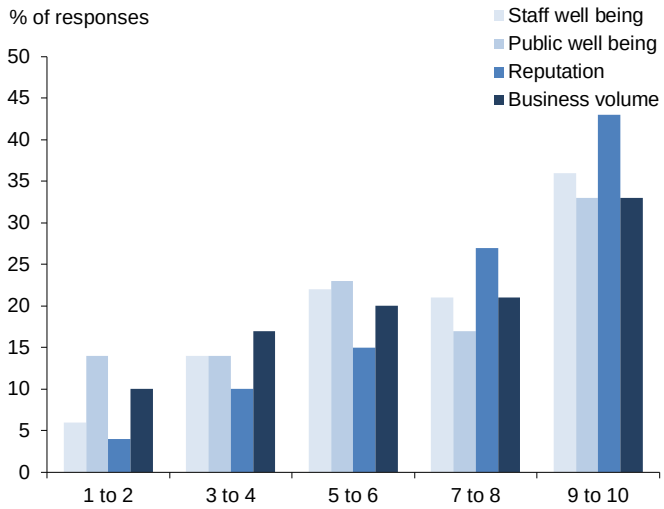
Chart 3.12: Q13b "The following table provides five information assets that may be put at risk as a result of cyber-attacks against your company. Please rate each asset type using the following scale to denote the potential impact of asset compromise to your organisation: 1 = no impact to 10 = maximum impact."



Source : Oxford Economics/Ponemon Institute

Respondents considered the organisation's reputation as the intangible asset that would be impacted most by cyber-attack (Q13c1-4) with a rating of 7.39/10 for the scale of impact. Other intangibles included staff well-being, public well-being and business volume.

Chart 3.13: Q13c "The following table provides four intangible assets that may be put at risk as a result of cyber-attacks against your company. Please rate each asset type using the following scale to denote the potential impact of asset compromise to your organisation: 1 = no impact to 10 = maximum impact."



Source : Oxford Economics/Ponemon Institute

3.5 Loss estimates

As indicated above, a central part of the costs of crime are the costs as a direct consequence of the crime itself. Accordingly, 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 in the following areas:

- 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)

Results of the responses to these questions, disaggregated into cost band, are presented in Appendix 2. Summary results of this analysis have also been presented in the tables below.

Some critics have questioned the reliability of the means in such surveys in the presence of large outliers and relatively small sample sizes[19]. This critique is mainly directed at extrapolations seeking to assess the total national cost of cyber-attacks, rather than studies such as the current one which focus on the "landscape" of cyber-attacks in the sample taken. Nonetheless, allowance has been made for such objections in the results presented below.

Accordingly, results are presented in terms of the "raw" survey mean, an adjusted mean (adjusting for outliers by excluding observations more than 2.5 standard deviations from the mean) and the median[20].

[19] Florencio and. Herley (2013). While these authors make important points, many of these relate to the need to examine medians as well as means, given the potential distortions of outliers, an issue long acknowledged by researchers. Accordingly medians are presented below. Further, the authors suggest that all such studies are upwardly biased; however it is not immediately apparent that this is so. In principle, sample outliers based on small sub-populations might just as likely understate outliers in the overall population as much as overstate them. Moreover, considering the historical reticence to report cyber-attacks – or fraud in general - respondents may have more of an incentive to understate losses rather than exaggerate them (as suggested by the authors). The removal of/ignoring outliers has itself been the subject of criticism by some analysts as they may yield important information about the underlying population.
The three measures presented in the tables below allow the reader to make an informed judgement about outcomes using the measure of their choice. Note that only "raw" means are presented in Appendix 2.

[20] The raw means were derived with reference to the (proportionally weighted) mid-point of each of the response categories for the individual questions. Open ended categories (e.g. "more than £100,000,000) were assigned a value 10% above the specified category figure (I.e. effectively £110,000,000). The adjusted means excluded observations beyond 2.5 standard deviations from the "raw" mean. The cut-off point of 2.5 standard deviations was based on Van Selst and Jolicoer

Table 3.2: Surveyed UK firm cyber-attack costs over last 24 months (£ million) [21]

Item	Clean up/ remediation (n=375)	Lost productivity (n=375)	Disrupted operations (n=375)	Damage/theft of IT (n=371)	Reputation/ Branding (n=272)
Mean	**2.3**	**1.9**	**2.3**	**1.9**	**2.9**
Adjusted Mean	**0.8**	**0.9**	**0.8**	**0.8**	**0.9**
Median	**0.18**	**0.18**	**0.18**	**0.18**	**0.38**

Loss estimates were highest for damage to reputation/branding. All other costs were reported with raw averages around the £2 million mark, with adjusted means slightly under half that and medians of £175,000.

However, the raw average reputation/branding loss estimate was £2.9 million. Some of this gap may be explained by a smaller sample size (155 respondents said they could not answer this question as opposed to between 52-56 for the other responses to this question (Q14)).Outliers may also play a role, adjusted average losses were closer to the other cost categories (£0.9m). However the median of approximately £380,000 is also higher than for other cost categories. It may be the case that while many firms felt they couldn't assess this question, those who could felt these costs were relatively high.

Even taking the most conservative measure (the median) these costs represent a substantial burden on British victims of cyber-attacks, given that the loss of employee time, impaired productivity and financial costs incurred represent money which could be used elsewhere (e.g. product development, R&D, marketing). Likewise, loss of brand value is wasteful in that previous attempts to build such value would be undermined meaning more must be spent to derive a given level of branding and consequent financial return.

Not only do these costs represent a financial burden for the firms involved, they impair economic growth in the long term. In effect, they represent an increase in input costs firms face in order to undertake a given amount of activity. This reduces productivity – and with it GDP growth – relative to a world without cyber-attacks.

However, the relative burden would vary depending on the size of the firm – e.g. a small firm facing a £1 million cost would be harder hit in relative terms than a much larger one. Analysis of cross-tabs (UK firm revenue vs cost categories Q

(1994) as reported in Cousineau D and Chartier S, (2010) "Outliers detection and treatment: a review" *International Journal of Psychological Research* 3 (1).

[21] The costs reported in this section are also referred to as "day to day" cyber-attack costs below, to distinguish them from the more far reaching and in some cases longer term costs of intellectual property loss and loss of sensitive business information, described below.

14a-e, excluding outliers) indicates that, in our sample, firms with larger UK revenues tend to experience larger costs[22].

Cross-tab comparisons were also made comparing industry classifications with firm costs (Q14a-e). Considerable caution must be expressed about the results given the small sample numbers in any given industry and that the sample is not representative of the landscape of UK firms. However analysis, based on examining the top two cost categories (in practice, costs over £5 million) with industry type suggests that, for this sample:

- Clean-up/remediation costs are relatively high[23] for firms in the automotive (n =10), media (n=13), telecoms (n=28) and transportation (n=27) industries.
- User productivity costs are relatively high in academia (n=7), aerospace and defence (n=10), conglomerates (n=34), financial services (n=53) and professional services (n=27).
- Disruption to normal operations was relatively high for mining (n=8), transportation (n =29) and aerospace and defence (n=10).
- Damage/theft of IT assets and infrastructure was relatively high for manufacturing (n =38), media (n =13) and transportation (n=27).
- Damage to reputation and marketplace image (brand value) was relatively high for transportation (n=17), aerospace and defence (n =9), automotive (n=7) and oil and gas (n=11) firms.

3.6 Intellectual property, commercially sensitive information and R&D

3.6.1 Intellectual property and commercially sensitive information

A key issue underlying concerns about cyber-attacks is that of intellectual property (IP) and commercially sensitive business information.

The two may be distinguished, in that IP typically relates to information which is of use in the long term and could potentially be the subject of patents, copyright, design rights, trademarks etc.– e.g. fighter jet designs. Commercially sensitive

[22] This analysis was carried out by comparing firm revenue with the percentage of firms reporting costs in the top two cost categories (in practice costs of £5 million or above). The percentage of firms reporting costs in these categories tended to rise with firm revenues, with no firms earning under £20 million reporting costs above £5 million and 13%-38% of firms earning £1 billion to £2.99 billion reporting such costs, depending on the sub-question of Q14. (Firms with revenues above this were discounted due to the small numbers involved.) While the purpose of the current paper is simply to illustrate this trend a future statistical analysis might examine this issue in more detail.

[23] "Relatively high" was determined by examining the percentage of firms reporting costs above £5 million. The three or four industries with the highest such percentages are described as having relatively high costs.

business information relates more to issues of short term business strategy – e.g. meeting notes, contractual agreements, negotiating strategies; "red line" issues etc.

A common concern is that the theft of IP, in particular, may result in other governments/companies either gaining confidential information and/or stealing a march on British companies thereby putting them at a long term disadvantage.

However, against this, some have argued that the loss of IP *per se* is of less consequence given that it is difficult to apply the "bits and pieces" of stolen IP in practice and that, given the nature of advanced economies and modern technology, stolen IP soon becomes obsolete.

Indeed this debate echoes older and broader ones about the value of IP and the balance between protecting IP vs encouraging innovation. In recent years this has most commonly been found in debates about audio-visual piracy and other forms of counterfeiting (e.g. brand imitation). There have been arguments that copyright holders are overly sensitive towards the issue and that sharing of IP could spur economic growth via enhanced innovation, as well as potentially benefiting the rights holders by enhancing overall product sales in a variety of areas. In the UK the recent Gowers Review and the Hargreaves Review have both sought to balance competing claims in these areas[24].

The case for protection of commercially sensitive information would appear clearer although even here there have been challenges to the idea that secrecy needs to be preserved – e.g. arguments questioning whether insider trading should be legal[25].

For both intellectual property and commercially sensitive information, a state sponsored cyber-attack represents a transfer of economic power from the UK to another country. Therefore, even if a free transfer of ideas was accepted by the originating party, it would still be a disadvantage for the UK as a whole, though globally, consumers may benefit.

Intellectual property and commercially sensitive data is stolen in all sectors, but by no means happens to everyone.

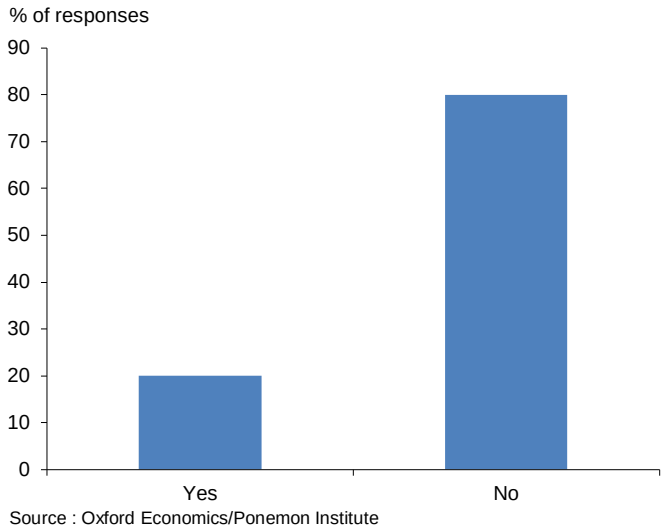
---

[24] HM Treasury (2006), *Gowers Review of Intellectual Property* ; Intellectual Property Office (2011) *Digital Opportunity: A Review of Intellectual property and Growth*

[25] Of course, to the extent IP and sensitive business data are lost by UK firms they will be obtained by foreign ones and in theory could potentially spur growth there. Given that the current study focusses on the UK, it is effectively ring-fenced so that such potential foreign gains do not count as growth – hence such simplistic "transfer" arguments do not hold. However even if this were not the case, and a global growth perspective adopted, points raised elsewhere in this paper should be recalled. Foreigners will have spent time and money to effect what is merely a transfer of already existing knowledge – hence there are global opportunity costs. Further, as indicated it may be difficult to apply the knowledge obtained either due to the complexity of modern systems, obsolescence or strategic mishandling of the information gained (in the case of business intelligence in particular). Finally some have made the point that relying on foreigners to develop IP/undertake R&D may inhibit national innovation in the long run, thereby reducing overall global innovation and growth (McAfee 2013). The fact that all of these elements add to other costs faced by UK firms is a good illustration of the negative effects cyber-attacks have on global as well as UK growth.

With this in mind it is interesting to note that 80% of respondents (340 out of 427) reported that they had *not* experienced any IP or commercially sensitive information loss in the last 24 months (Q15a).

Chart 3.14: Q15a "Has your firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber-attacks within the past 24 months?"



Source : Oxford Economics/Ponemon Institute

Therefore the great majority of respondents did not experience such losses (or were not aware they had)[26].

Examination of cross-tab data indicates that company size (whether measured by UK revenue or headcount) did not make a major difference to whether or not companies reported that they had experienced IP or commercially sensitive losses in our sample. For example, excluding the very highest revenue bracket which accounted for only one firm, the lowest response (in terms of percentage saying "yes" to Q15a) came from firms in the £20-49.9 million UK revenue bracket, where 14% of firms responded with "yes" whereas the highest was 30% (from firms in the £1 billion to £2.99 billion bracket)[27].

[26] It should be noted that this also has the effect of reducing the sample sizes for Q15b-19c inclusive.Q15b and 16a had 87 respondents while the others had 74..

[27] By way of interest, in the very lowest revenue bracket (under £20 million) 15%of firms in our sample reported they had experienced IP and commercial losses while in the second highest (£3 billion – £6.99 billion) 19% of firms reported they had. While the results have not be subject to formal statistical testing, this suggests that firms of all sizes had roughly similar experiences with IP/commercial theft – the problem was not demonstrably greater with larger firms for example. The results were similar if measured using UK headcount as an indicator, with "yes" percentages ranging from 14%-26% (the lower figure being in the less than 1,000 headcount category, the higher in the md-range 5001-26,000 category. Indeed, a higher proportion of firms (26%) in the "mid-range" headcount bracket of 5,001-25,000 employees said "yes" than those in highest two headcount brackets (25% and 20% respectively).

It is worth asking what types of firms did experience such losses. When broken down to an industry level, analysis of cross-tabs (industry classification vs loss of IP and commercially sensitive information) indicates that the highest proportions of respondents in our sample experiencing a loss could be found in aerospace and defence (42.9% of such firms), chemicals (36.4%) and mining (33.3%) and creative and media (31.3%)[28]. The fact that we are not analysing a representative sample, however, may mean that these sectors who suffer the highest proportions of incidents are not representative for the UK as a whole. In general, however, we may compare this to the Brookings study discussed earlier, which found that knowledge driven sectors are more vulnerable to IP theft while highly competitive and innovative sectors are more vulnerable to the theft of commercially sensitive data[29].

Of the 20% who said they had experienced such a loss:

- 61% said that they had experienced a loss of competitive advantage due to the loss of IP (with 39% saying they hadn't - Q15b).
- 59% said that they had experienced a loss of competitive advantage due to the loss of commercially sensitive information (with 41% saying they hadn't -Q16a).

In other words the majority of firms who suffered a loss of IP or commercially sensitive information felt they were damaged by it.

Inspection of the relevant cross-tabs comparing Q15a with Q16b appears to suggest that respondents appear to differentiate between IP and commercial losses rather than simply seeing them as one and the same. For example 23 respondents indicated that lost IP had cost them a competitive advantage but that lost commercially sensitive business information had not[30]. Only 13 respondents out of 87 (15%) did *not* experience a loss of commercial advantage through *either* means.

[28] These results are interesting for indicative purposes but note that small sample sizes given the level of industry disaggregation and an unrepresentative sample may limit their applicability. In terms of the above cited industries, sample sizes were as follows: 14 firms in aerospace and defence, 22 in chemicals, 9 in mining and 16 in creative and media.

[29] A. Friedman, A. Mack-Crane, R. Hammond, Brookings Institute Center for Technology Innovation "Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences" (2013)

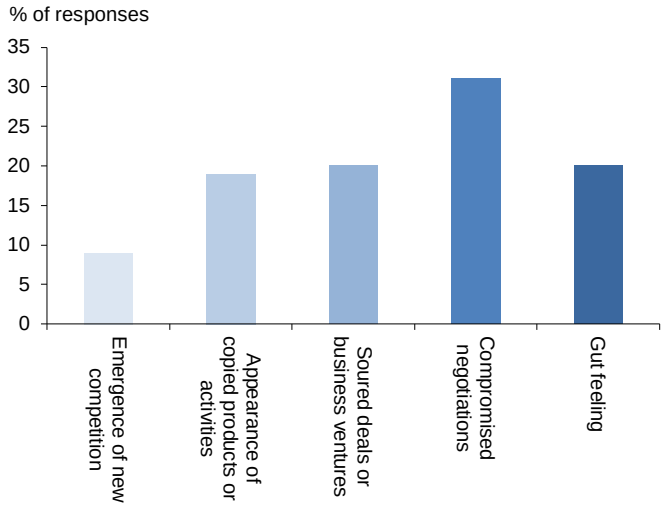
[30] Of course this could simply be because their losses were only in IP or because they did experience such a loss of commercially sensitive information but it didn't impact their business. However the point remains that respondents appear to be differentiating between the two categories.

Table 3.3: Cross tabs – Q15b vs Q16a

Item	Loss of commercially sensitive info – has caused loss of competitive advantage	Loss of commercially sensitive info – has not caused loss of competitive advantage
Loss of IP - Has caused loss of competitive advantage	30	23
Loss of IP - Has not caused loss of competitive advantage	21	13

The most common loss of competitive advantage through either form (Q16b) came in the shape of "compromised negotiations or business ventures" (31%), followed by "soured deals" (20%) and the "appearance of copied products or practises" (19%).

Chart 3.15: Q16b "If yes [to Q16a], how did your firm determine the loss of competitive advantage as a result of the cyber-attack?"

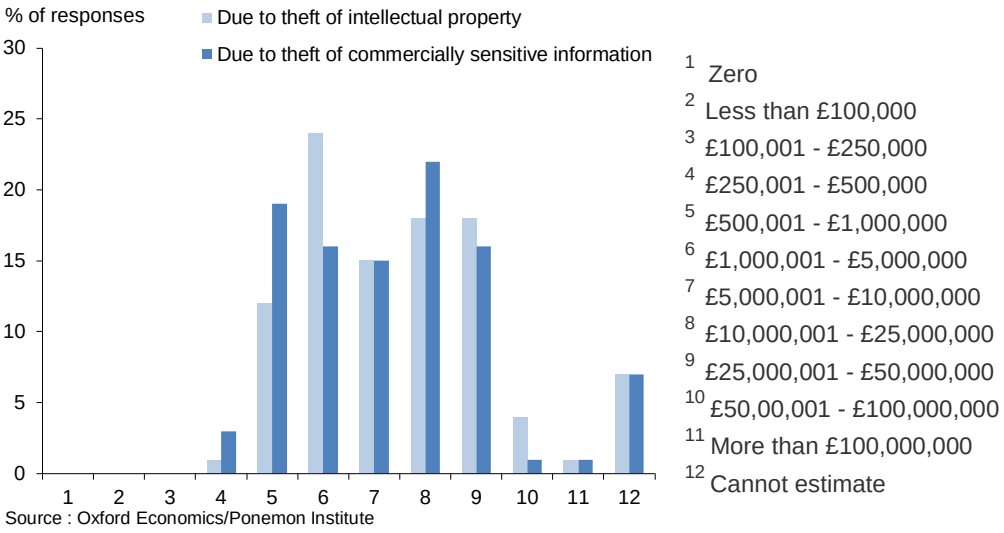


Source : Oxford Economics/Ponemon Institute

Respondents were also asked to quantify their estimated losses due to IP theft and the loss of commercially sensitive data.

Chart 3.16: Q19a "Approximately, how much did losses due to the theft of intellectual property cost your organisation over the past 24 months?

Q19b "Approximately, how much did losses due to theft of commercially sensitive information cost your organisation over the past 24 months?"



Source : Oxford Economics/Ponemon Institute

The table below indicates the mean, outlier adjusted mean and median losses arising from intellectual property losses over the last 24 months (Q19a) and the loss of commercially sensitive business information over the same period (Q19b).

Table 3.4: Surveyed UK firms – Losses of IP and commercially sensitive business costs due to cyber-attacks over past 24 months (£ million)

Item	IP costs (n =69)	Commercially sensitive business costs (n =69)
Mean	**17.3**	**15.1**
Adjusted Mean	**13.2**	**12.8**
Median	**7.5**	**7.5**

While we cannot generalise to the overall population of UK firms, the mean, adjusted mean and median of the IP and commercially sensitive business losses are all well above the equivalent "day to day" losses reported in Qs 14a-14e for our sample.

A priori this might suggest that while only a minority of companies suffer IP/commercially sensitive information losses, the cost of such losses is considerably higher than is the case for "day to day" losses. A focussed approach to cyber-attacks might therefore concentrate on the types of companies which experienced or were likely to experience IP and commercially sensitive business losses.

As was the case with "day to day" costs above, analysis of cross-tabs for both IP and commercially sensitive information losses, suggests the highest losses are incurred by firms with larger revenues, For example, in the case of IP losses,

excluding outliers, while no respondent firms in the lowest UK revenue category (under £20 million) experienced cybercrime losses above £10 million, 100% of firms in the £1 billion to £2.99 billion category did so. Analysis of the "intermediate" responses between these two revenue categories seems suggestive of a trend within our sample.[31]

Also worthy of note is that 78% of these estimates were arrived at through some form of formal assessment (Q19c).

3.6.2 Research and Development spend

Another area of concern to policymakers has been the impact of cyber-attacks on R&D. One argument is that cyber-attacks deter R&D. As firms invest in R&D but simply see the fruits of their investments stolen, they may be tempted to reduce such investment. Apart from denying firms potential financial returns from R&D, this would have the long run effect of reducing the amount of innovation and growth within the economy. This is because the pattern of investment would be distorted away from its "first best uses" and/or because overall R&D within the economy is reduced (particularly as more and more firms fall victim to cyber-attacks).

To measure the impacts of the loss of R&D, the survey sought written "freeform" responses on the impact which cyber-attacks had on R&D (Q17), and an indication of whether R&D investment increased or decreased as a result of cyber-attacks (Q18a). As the loss of IP/commercially sensitive data are likely to be closely linked to subsequent R&D decisions, responses to these questions were sought from those (74) respondents who had indicated that they had suffered a loss of competitive advantage due to the theft of IP/commercially sensitive data.

The majority of respondents (62%) indicated that cyber-attacks would not result in a change in their R&D investment, while 16% indicated it would decrease and 22% indicated it would *increase*.

The latter figure is particularly surprising; however the responses to Q17 help shed some light on it. Responses included comments such as:

[31] For example, there were only 5 responses in the former of these categories and 9 in the later, though sample size numbers were higher in the intermediate revenue categories between these two (ranging from 11-14). Note while only 50% of firms in the highest revenue category with respondents reporting IP/commercial losses (£3- £6.99 billion) experienced losses above £10 million, the sample size (n = 2) and the unrepresentative sample does not permit any meaningful interpretation.
A generic issue here is that as only 87 respondents in total indicated that they had experienced IP/commercial losses any more detailed analysis is restricted by the small nature of the sub-sample(s).
Nonetheless a similar trend was observed in the case of commercially sensitive losses (excluding outliers) where no firms in the lowest revenue category (n =5) experienced losses of £10 million or greater while 90% of firms in the £1 billion to £2.99 billion category (n =10) did so.

- *[My company] had to increase R&D budget to make up lost ground.*
- *Investments in R&D security will substantially increase.*
- *While management is more cautious, we had to investment more [sic] to maintain competitive ground.*
- *My company had to increase this year's research budget because of competitor gains.*
- *Our board is concerned that the theft of IP demands renewed commitment in IP investment.*
- *I think investment had to increase in the short run only.*
- *In the short run, no impact whatsoever. In the longer term, I don't know.*
- *My organisation has stepped up spending on security controls over IP and business confidential information.*
- *The research and development activities [sic] had to step up because of economic espionage by the Chinese.*
- *My belief is that we had to increase investment to keep pace with our competitors.*
- *I can't comment on the particulars, but we did not change our investment level just our strategies.*

In other words, reasons for respondents indicating they would increase their spending on R&D included:

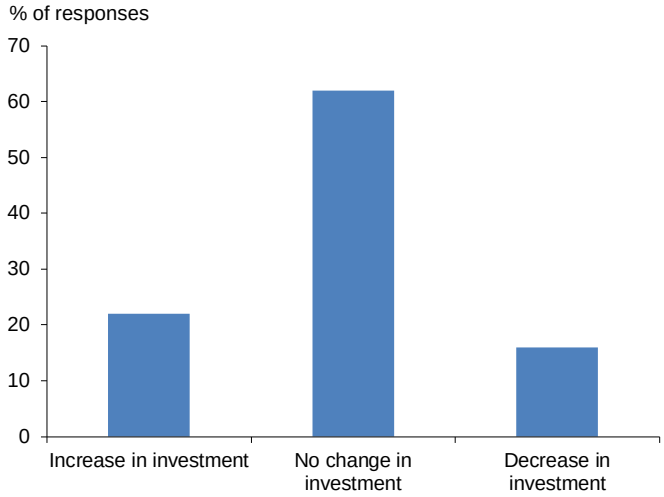
- They had to increase spending to make up for lost ground either to deal with their existing competitors or perhaps those launching the attacks; and/or
- It was interpreted as a “spend on cyber-attacks prevention issue” and accordingly they indicated they would increase spending.

It should be noted that, in economic terms, either a decrease or an increase in R&D investment in response to cyber-attacks could be seen as inefficient and as affecting long term productivity. The negative effects of a decrease were cited above. However, increasing investment to make up for lost ground would not be necessary if there were no cyber-attacks. Effectively, the R&D spend must be repeated, meaning a larger investment for the same fixed return.

In terms of spending on R&D specifically to bolster cyber defences the arguments are similar to those described above – absent cyber-attacks, investment is likely to be better allocated elsewhere.

In this context, it is instructive to note that the combined “increasing” and “decreasing” respondents account for some 38% of the total. In other words, 38% of respondents in our sample altered their R&D investment plans as a result of the “disturbance” created by cyber-attacks in the short term.

Chart 3.17: Q18a "How did your organisation's investments in research and development change as a result of the cyber-attacks it experienced?"



Source : Oxford Economics/Ponemon Institute

To follow on from this point, in the cases of both those firms who indicated they would increase investment and the majority who indicated there would be no change, a key question relates to the long run as opposed to the short run. It is likely that many of the responses gathered related to the immediate future of perhaps a year or two.

However, beyond this timeframe things may be different. In the event that successful cyber-attacks continue there may be a rethink – as hinted by some of the freeform responses.

An analogy might be responding to the loss of a home burglary by purchasing new items. If a home is repeatedly burgled it is unlikely purchases will be repeatedly made. Rather the owners are likely not to make such purchases again and/or consider moving out of their current area to a new one.

Likewise, given the above responses, it is likely that given the timeframe over which R&D takes place, reduced investment in response to cyber-attacks only develops over the longer term. It may therefore not be immediately perceived as a direct response to cyber-attacks, particularly given the timeframes involved and staff turnover/loss of institutional memory. Further econometric analysis using time series data may be possible in the future and allow for an assessment of the magnitude of this effect.

4 Event Studies of Cyber-Attacks

In addition to the survey of UK firms, which identifies the direct costs incurred as a result of cyber-attacks, Oxford Economics has undertaken an event study to analyse the potential reputational loss firms may suffer. As a proxy for reputational damage we use negative stock market returns that may be experienced immediately around the public disclosure of a cyber-attack.

4.1 Background

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. Event studies are particularly relevant to cyber-attacks because firms are often loathe to publicly disclose the occurrence of such incidents, fearing the market reaction to such disclosures. In the United States, the Securities and Exchange Commission has recently published guidelines recommending that firms disclose cybersecurity risks and incidents, but does not require firms to disclose these details in annual reports[32]. Often, the public disclosures that do occur are leaked by unofficial sources to newspapers. Hence, event studies around the disclosure of cyber-attacks may shed light on whether markets think that cyber-attacks are a significant risk to a firm, via the signalling effect of investor sell-offs after a disclosure.

There are several existing studies of cybersecurity incidents on stock prices for affected firms. Campbell et al (2003) find some evidence of a negative stock market reaction for cybersecurity incidents, with highly significant negative impacts observed on breaches involving unauthorised access to confidential data.

Cavusoglu et al (2004) find that security breaches are negatively associated with the market value of the announcing company. In their sample, victim companies lost, on average, 2.1% of their market value within two days of the announcement, amounting to an average market capitalisation loss of US$1.65 billion per breach, suggesting that the cost of inadequate cybersecurity is high for investors. In addition, they found that breach costs increased during their study period, over the years 1996-2001, and that these breaches were more costly for small firms than for large ones. Firm size is an important variable. Large firms have greater access to capital markets, lower costs of capital, diversified income sources and market products. These firms can more easily absorb the costs of cyber-attacks and can spend more on the prevention of cyber-attacks than small firms.

Ernst & Young also published an event study on the financial impacts of information breaches in 2003, estimating the impacts by type of cyber-attack. For the 22 events studied over the 1996-2002 period, the average fall in share price attributable to a cyber-attack was estimated at 2.7 per cent over one day, increasing to 4.5% over a three-day period. These losses represented a

[32] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

combined loss of US$20.2 billion, or US$918 million per event. The authors also classified the attacks into certain types of events: Web site defacements, Denial of Service (DoS), theft of credit card information, and theft of other customer information; finding that markets react more negatively when there is the possibility of third-party legal liability in cases of credit card theft. Also, DoS events garner a more negative market reaction.

4.2 The Sample

Oxford Economics undertook an event study for the purposes of this report in order to evaluate whether analysis of stock market returns suggested that companies experienced reputational loss in the event of a cyber-attack. The period 2005-2013 was chosen for this purpose.

Initially, 71 events were logged in our database from a Factiva search and general search engine query of news articles. 21 cyber-attacks in our database occurred in firms that were not publically traded, and these events were therefore removed from the dataset. Five further events were discarded because the securities were not yet publically listed at the time of the cyber-attack. In the final dataset, 45 distinct events were captured in this event study, from 2005 to 2013. Appendix 4 includes the final list of events, with the company name, event data and industry of the company.

4.3 The Methodology

To find if the announcement of the cyber-attack affected a firm's stock price, we estimate first what the return of each individual stock would have been if the event had not occurred. This is termed the "normal return." Like many previous event studies, and as recommended by MacKinlay (1997), 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 gives us a better ability to detect the effects of the cyber-attack on the return of the stock (if any).

Market indices were chosen depending on which geographical market the stock traded in. Table 4.1 below shows which market index was used for which geographical markets:

Table 4.1: Market indices utilised per geographical market

Market	Market Price Index
United States	S&P 500 Composite Index
Japan	TOPIX Index
United Kingdom	FTSE All Share Index
Australia	ASX All Ordinaries Index
Europe	FTSEUR1ST 300 E Index

Source: Oxford Economics

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[33]. The 120-day estimation window encompassed stock return data for the 120 days immediately preceding the 3-day event window[34].

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[35] if the abnormal return is statistically different from zero. Arguably, one could say that the more useful test is whether the average of the sum of all abnormal returns over the 3-day event window for all firms is equal to zero or not[36]. 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.

Some of the assumptions for the OLS regression are violated in our event study sample. There are some firms that are attacked at the same time within one industry[37]. In addition, we have no reason to believe that cyber-attacks would

[33] The preceding and following days are included to cater for cases where the news is published on one side of the globe, but the stock trades on another side, or for cases where the news is published after markets close on the event day.

[34] Of course, days where the market does not trade are not counted in these windows.

[35] Using a student t-test.

[36] This is a test of "joint significance."

[37] Known as contemporaneous correlation.

affect all firms in the sample in the same way[38]. In order to control for this, a more robust regression specification, a seemingly unrelated regression (SUR), was run. Two separate Wald tests were then conducted: if returns to all shares in the sample over the three-day event window were statistically different from zero and if the average return to all shares in the sample was statistically different from zero. If statistically different from zero (and negative), this would demonstrate that perhaps there is a reputational effect on companies affected by cyber-attacks, using the share price as a proxy.

4.4 Results of the event study

Table 4.2 shows the results of the OLS estimation. Examining the average abnormal return over the event windows, we found that average abnormal returns for more than half of the events were negative, suggesting a negative impact on stock market valuation from cyber-attacks. Under a truly random distribution, we would expect only half to be negative.

Upon further analysis, however, only three events had an average abnormal return that was statistically significant (using OLS estimation), and hence likely to be the result of news announcements of cyber-attacks. All three events, for BHP Billiton, Adobe, and Baker Hughes showed negative returns. Therefore, for these firms, it may be the case that they suffered a reputational loss, in addition to any other costs incurred as a result of the cyber-attack. Of these three firms:

- The BHP Billiton cyber-attack was publicly reported as being launched by the Chinese State. A couple of other large mining companies, Rio Tinto and Fortescue Metals, were publically reported as being attacked by the Chinese State at the same time. This was likely due to the desire by China to gain an advantage in its procurement of iron ore. However, our study does not find an effect for Rio Tinto and Fortescue Metals.
- The Adobe cyber-attack was identified as an APT, with hackers gaining access to Adobe's digital certificate code signing infrastructure. As a result, hackers were able to create malware that would pass for legitimate Adobe software. It is clear that this attack was an intermediate attack, to gain access to tools that would facilitate other attacks.
- Finally, Baker Hughes, a Texas-based provider of advanced drilling technology for the oil and gas industry was attacked by the Chinese State, as part of a wider attack on a number of oil and gas firms. These firms included Exxon Mobil, Royal Dutch Shell, BP, and Marathon Oil. As a result of these attacks, the firms lost project-financing information for oil and gas field bids and operations. However, our study does not find an effect for the shares of Exxon Mobil, Royal Dutch Shell, BP, and Marathon Oil.

[38] Standard errors are not homoskedastic across events.

In addition, a test was conducted to see if the average abnormal return across the entire sample was statistically different from zero as a result of cyber-attack news disclosures. The average loss across the sample of 45 firms was 1.70% over the three-day event window. In terms of forgone market capitalisation this represents a nominal loss of £30 billion across all 45 events, or an average of £666 million per event[39]. However, this loss is not found to be statistically different from zero using the OLS methodology and thus we cannot attribute the lost market value to the cyber-attacks in this instance.

Next, we employed the SUR methodology, as a robustness check, to take into account the assumptions violated in our sample for OLS estimation. We generated 45 equations (from the 45 different events) and used this system to test for joint significance of negative returns over the 3-day event period. The first Wald test, conducted to see if all the returns across the 45 companies over the 3-day event window were statistically different from zero, showed that indeed they are, albeit at a 10% significance level (a 5% significance level is normally the usual standard). The second Wald test, to see if the average returns across the 45 companies over the 3-day event window were statistically different from zero, also showed a similar result, but at a much higher significance level (1%).

This result shows that the average shareholder return around the time that cyber-attacks were announced publically was significantly different from zero and negative (-0.62%), representing an overall market capitalisation loss of £10.9 billion across all 45 events and an average loss of £243 million per cyber-attack[40]. While these results are much higher than those identified in our survey sample in Chapter 3, they offer some consistency of perspective in pointing to the large potential damages associated with reputational damage. It is also worth noting some caveats in comparing these results with those of Chapter 3:

- The sources and contexts of the two estimates differ. In particular, stock market valuations reflect investor perceptions (potentially of a broader range of issues) over a given timeframe (in this case 3 days). In one sense, the Chapter 3 estimates provide a practice based (or "bottom up") assessment while this Chapter provides a potential "top down" approach based on investor perceptions. An issue for future "top down" analysis, in particular, may be how or whether these effects persist in the longer term.
- Following on from the first point, the sample set of companies covered in Chapter 3 was not restricted to listed (and therefore generally larger) companies where knowledge of cyber-attacks was made more widely known. One might therefore expect a differing scale of results.

It is also worth noting that earlier event studies cited above (e.g. Cavusoglu et al (2004), Ernst & Young (2003)) have found higher market capitalisation losses per cyber-attack. This may be due to methodological differences, but it also may

[39] Using Datastream market valuations for the date of the event, and the exchange rate on the day. These estimates are not adjusted for inflation.

[40] *Ibid.*

be because this sample is much newer and one would expect investors' understanding and response to cyber-attacks to have significantly evolved over the period as the market came to better understand this new phenomenon.

4.5 Implications

Taken by themselves these results suggest that publicised cyber-attacks generally have some impact on stock market valuations and by extension company reputations. If this is the case, it means that the investment companies make in IT security to prevent these attacks may maintain shareholder value for these companies.

However, given the opaque characteristics of cyber-attacks, it may also be the case that sometimes false information published about the nature and extent of an attack impacts on the stock price for a company. For example, one of the firms we interviewed revealed that false information regarding a cyber-attack had been released via a prominent news source.

We examined our sample of news stories on cyber-attacks to separate out the ones with enough detail to give readers of such stories a sense of the potential impact. Out of the 45 news events, only 6 had enough detail to give the reader a sense of the potential impact on a company:

- Sony Playstation
- EMC's RSA's SecurID
- Citibank
- Coca Cola
- AMSC
- QinetiQ

Although only these six events were determined to have enough detail to have a sense of potential impact from the news story, we found that across the 45 event sample, the news of cyber-attacks generally affected the share price. This means that investors are reacting to news stories, even if there is too little detail to determine whether this attack has a significant impact for the company. A further extension of this event study could involve separating out different types of cyber-attacks to test which types of attacks have a negative effect on shareholder returns.

Lastly, while appropriate caveats have been noted above, the findings here that reputational costs (as proxied by the share price return during the event window) are significant are broadly in line with our survey results. Both sets of results suggest that reputational costs from cyber-attacks may be relatively large. For the reasons discussed above, the share price may offer a proxy for a firm's reputational loss from the announcement of cyber-attacks, however further supporting analysis would be useful in helping to confirm these results and their duration.

Table 4.2: Event study findings (OLS specification)

Company	Average Abnormal Return	Significance Level	Cumulative Abnormal Return
Sony (Playstation Network)	-1.3%	-	-4.0%
Trend Micro	1.0%	-	3.0%
Mitsubishi Heavy Industries	-0.1%	-	-0.3%
Nissan	0.2%	-	0.5%
Reed Elsevier's LexisNexis Inc.	0.1%	-	0.2%
United Business Media (UBM)	0.5%	-	1.4%
Shell	0.2%	-	0.5%
BP	0.3%	-	0.8%
BHP Billiton	-0.9%	5.0%	-2.8%
Rio Tinto	-1.0%	-	-2.9%
QinetiQ	-0.8%	-	-2.5%
Dun & Bradstreet Corp	-0.1%	-	-0.3%
VeriSign (Symantec Corp)	0.0%	-	-0.1%
Intel	0.8%	-	2.4%
JP Morgan Chase	0.1%	-	0.2%
Citigroup	1.0%	-	2.9%
Adobe	-0.4%	10.0%	-1.2%
New York Times	-0.9%	-	-2.6%
Lockheed Martin	-0.3%	-	-0.9%
EMC	0.5%	-	1.4%
Korn Ferry International (KFY)	-0.2%	-	-0.5%
Google	-1.0%	-	-3.0%
Adobe	-0.4%	-	-1.1%
Exxon	0.1%	-	0.4%
Marathon Oil Corp	-1.4%	-	-4.3%
Conocophillips	-0.1%	-	-0.2%
Baker Hughes	-0.6%	10.0%	-1.7%
Symantec	1.0%	-	3.0%
Citigroup	-1.9%	-	-5.7%
Intercontinental Exchange	-7.5%	-	-22.6%
Nasdaq OMX	-0.3%	-	-0.9%
Monster.com	-1.7%	-	-5.2%
AT&T	0.2%	-	0.7%
TJX (T K Maxx/T J Maxx)	-0.4%	-	-1.3%
Disney	0.1%	-	0.2%
New York Times	-0.7%	-	-2.1%
News Corp	-0.1%	-	-0.4%
Coca Cola	0.1%	-	0.4%
Wells Fargo & Co	-0.3%	-	-0.9%
American Express	0.1%	-	0.4%
JP Morgan Chase	-0.7%	-	-2.0%
AMSC	-8.1%	-	-24.3%
Under Armor	-0.2%	-	-0.6%
Delhaize Group	0.3%	-	0.8%
Fortescue Metals	-0.5%	-	-1.5%

Note: Significance level based on t-test of average abnormal returns.

Source: Oxford Economics

5 Case Studies

In order to complement the preceding analysis Oxford Economics conducted a series of interviews with a number of UK firms aimed at getting a direct understanding of how cyber-attacks had affected their operations. While firms are traditionally reluctant to discuss such issues, with the assistance of CPNI and under conditions of anonymity, Oxford Economics was able to contact a number of firms and discuss their respective experiences of cyber-attacks. These interviews formed the basis of Case Studies 1-5 detailed below.

In addition a secondary literature survey of "open source" information uncovered enough detail to develop an additional Case Study (Case Study 6), Note that the firm in question is identified in this case, as this information was already in the public domain.

Key findings from these cases include:

- Approaches to cyber defence should encompass several lines of defence. Simply using firewalls alone can lead to a sense of complacency.
- Restricting the number of potential entry points is clearly important.
- Staff awareness sessions are one of the more beneficial first line measures.
- Security needs may differ across different areas of the organisation, so a tailored approach may be most efficient in some circumstances.
- "Most at risk" information should be identified and protected accordingly.
- "Waterhole" attacks, made via suppliers of companies who are the ultimate targets, are an emerging threat which requires more attention.

Case Study 1: A best practice example of cyber security

This multinational company had global reach, significant dealings with China and experience of significant cyber security breaches. They provided their account of how they have bolstered their defences to establish a much more robust cyber security posture.

Restricting entry points and target hardening are important

The firm had redesigned and significantly bolstered its cyber defences in the last 2 years, which started with a rationalisation of its entire network. Previously, there were over 100 entry points, which were too many to monitor. These were reduced to under 10 over a 6-month period and systems have been embedded that enable the IT security team to look inside the data flowing through those gateways, and to spot patterns of behaviour that indicate a potential breach.

The firm implements what it describes as “a simple strategy, but ruthlessly implemented”. Basic security was improved by hardening all devices to make them less easily compromised. More privileged users on the network have to pass through a second layer of authentication, which makes it very difficult for attacks to gain main administrative privileges.

There is no magic bullet for security. The security team analyses the cyber “kill chain” and persistently strengthens it at every stage; educating users not to click on emailed links, hardening operating systems in case they do click on links, managing lateral movement across the network and controlling elevated privileges, monitoring Domain Name Servers to see if there is any manipulation, monitoring flows across the firewall for irregular commands from outside to inside devices.

Most at risk information should be identified

The theft of sensitive data or intellectual property occurs at the end of that kill-chain and was a real concern for the firm. Their approach was to try to identify what information was most at risk, and most valuable to lose, and put layers of security around it accordingly. “It’s an onion, rather than an egg model of protection” so that the most valuable information has the most protection around it. So far there is no indication of a significant IP loss having been suffered.

The company has observed an increase in cyber-attacks, but is not sure if this is down to an increase in volume or improved detection. The head of IT security said the company had suffered thousands of cyber-attacks over a 24 month period and millions of “security events”. In contrast to another company who discussed their experience with us personally, his gut feeling was that a minority of the attacks were directly state-sponsored, perhaps 10%, but those attacks tend to be the more high-end sophisticated attacks. Despite increased attacks, they had not suffered any material losses in the past 2 years.

In terms of cost, as a ballpark estimate, the company probably spent 1-2% of the overall US$50m IT budget on information security. In rationalising their systems down to under 10 gateways, they have actually reduced staff costs on IT security in the past two years whilst simultaneously becoming more effective.

Ultimately, their message is that if a company wants to strengthen its IT security it requires a holistic approach. It is not enough just to focus on fending off the sophisticated APT threats. The biggest challenge is obtaining management support, through for example a cyber-security steering committee on the executive board. Once you have high level buy in, everything else flows from there.

Case Study 2: A hard-hitting approach to cyber security

A large multinational spoke to us on an anonymous basis to discuss their personal experience with nation-sponsored cyber-attacks.

The majority of cyber-attacks are state-sponsored.

Almost all cyber-attacks experienced by this firm were nation-sponsored. The vast majority were thought to be propagated by China (95%), with the rest split between Russia and Hezbollah. In 2012, this company detected 339 cyber-attacks. In 2013, this number decreased to 150, but this firm believes it is a temporary lull as hackers go after easier targets perhaps to impress the new Chinese party leadership.

Expenditure on IT security is only a small portion of the total value of information at risk.

The UK business of this company spends between £22 -£32 million per annum on cyber-security, yet the value of information at risk from cyber-attacks is estimated at £3.5 billion. Therefore, the annual expenditure on cyber security represents less than 1% of the value of information at risk. This expenditure is viewed as a necessary cost of doing business, though it does mean that perhaps prices or overhead costs are higher as a result. This company believes that if other companies are not spending more than $6 million per annum on cyber-security, they are not taking the threat seriously.

Weak IT security stances from suppliers is a major risk.

There is a drift towards what is known as waterhole attacks, where hackers target websites visited by employees of companies. In this case, hackers are targeting the websites of supply chain firms that their employees visit. This is partly because large firms have got better at bolstering IT security and hackers are going after the weak links in their supply chains. This company made the observation that there is little awareness in industry of the threat of cyber-attacks. They find that this is especially true for smaller companies, who think they are safe because they have firewalls. Managing the risk of cyber-attacks from the weak security stance of suppliers is especially tricky when a firm has a very large supply chain.

Expenditures on R&D have increased as a result of the threat of cyber-attacks.

After detecting a cyber-attack, allegedly from China, that succeeded in extracting some documentation of R&D, this company increased expenditure on R&D around cyber-security in order to protect their valuable intellectual property assets. The successful attack, however, did not cause this firm to lose competitive advantage because the information stolen was out of date. Furthermore, they have not lost any intellectual property due to cyber-attacks over the past two years.

Discussing your IT security stance and identified risks within industry forums is an important tool that can help companies to jointly increase their IT security strategies.

This company, after discovering an ongoing state-sponsored cyber-attack and installing systems and strategies to wipe the threat and bolster their IT security stance to prevent future attacks, began to discuss their experience within two industry forums in the US and the UK. Their presentation instigated the threat and intelligence sharing that now goes on regularly in the UK forum.

Case Study 3: On the fringe rather than the front line

This large UK based multinational sees itself as on the fringe of cyber-security risk, rather than front line. The company operates on an international scale in a traditional industry that had not previously considered itself at risk from cyber-attacks. The head of information security admits to the company having been "behind the curve" on cyber security compared to other sectors and considering its size and global reach. The company employs only eight full time information security staff across its global operations and had been relying on a fairly traditional security framework, with anti-virus software on the end-points etc.

Action by government bodies can be critical to alerting business

The company was alerted to three significant state-sponsored attacks on its systems by CPNI. Fortunately none of those attacks resulted in significant losses, apart from hefty consultancy fees for external experts to diagnose points of entry and assess the damage. The company believes the attacker may have been interested in strategic intelligence regarding a particular sector the company was operating in, or information on the consortium framework it belonged to for a specific project bid.

The company considers the breaches 'near misses' as they could potentially have caused more damage. It has undertaken significant improvements to its cyber-resilience following the attacks. A CPNI briefing to the board highlighting last year's three attacks helped in winning their support, and the company recognises that the attacks likely catalysed its cyber-security upgrade programme. But the company continues to take a pragmatic approach. It will upgrade its systems on a 'step-by-step' basis, with a longer term programme contingent on the outcome of an initial assessment in 2014. It will likely continue to use external consultants for the more technical aspects, rather than building in-house expertise.

Risks may change as companies evolve

Whilst alert to the risks, the company calculates a relatively low return to investment in security measures compared to other companies we spoke to. This is partly because an overhaul of the IT infrastructure would be highly complex and costly - the company has grown more than fivefold in the past decade, mostly through major acquisitions, and the resulting organisational infrastructure is not completely integrated. It is also partly because the company is realistic about the scale of the risk that it faces from cyber-attack. It regards its commercial information as not particularly secret, and its secrets as not particularly commercially valuable.

Nevertheless, the information security team is aware of the risks the company does face. Commercially sensitive information, if lost, could jeopardise a valuable project bid if it fell into the wrong hands. The company's private trade practices, which it considers its core intellectual property, could lead to more long term losses if stolen and copied, eroding the company's competitive advantage. One element that may become more valuable in the future is the company's very large meta dataset, and associated modelling software, which is vulnerable to watering hole attack and attractive to state intelligence agencies. The company is also very conscious of the potential damage a large-scale virus, like the Shamoon virus that hit Saudi Aramco last year, could do to its business because the core business is heavily time-bound and delays could lead to substantial fines.

Case Study 4: Safeguards and the Onion Model of Protection

Important safeguards include staff briefings

Another company we spoke to revealed that staff briefing and awareness is one of the more beneficial safeguards against cyber-attacks (in addition to hardening & segregating their network). Part of the reason lies in the difficulty of pre-emptively identifying weaknesses in IT security, as the devil is in the details, effectively requiring a considerable amount of diagnostics work. As a result, many firms (especially SMEs), will find themselves spending the majority of IT security resource on responding to infringements rather than preventing them. If an infringement can be identified and diagnosed quickly, however, the risk from cyber-attack can be minimised before the attack progresses to the end of the kill chain, where information is exfiltrated from the company's servers.

This company first began briefing employees on a rolling basis after their first APT attack, approximately 5 years ago. The briefing generally covers how cyber-attacks have occurred and what systems the company has put in place to prevent them. This allows them to get buy-in from their staff on the prevention of cyber-attacks, an important step as some safeguards might otherwise prove to be ineffective as staff find ways around them. In addition, as staff awareness increases, they report suspect attachments or links the moment they receive them, allowing the firm to pre-emptively block hackers from entering the system in the first place.

They undertake briefings for groups of 12-24 employees at a time and feel that groups this size provide the best opportunity to customise the briefing for staff and to have personal engagement at a meaningful level. In order to maximise the level of engagement, they begin sessions by showing a scene of the Bond film, *Skyfall*, showing the potentially dangerous consequences of cyber-attacks as an initial hook, with discussion of actual attacks and how they are carried out afterwards. With technical staff, they go into the technical details of attacks.

Bigger isn't always better

This company is also an interesting case study of how IT security is done in an independently operated company that is part of a much larger group. While one large firm we interviewed implemented a global system of prevention for cyber-attacks, this company coordinated and shared information with other companies in the same parent umbrella, but did not have integrated IT systems in place across the companies in the parent umbrella. This can be an advantage when different companies within the umbrella have vastly different security needs.

An expensive, globally implemented security system can be highly valuable for IT protection in one part of the business, but may not be appropriate for another which works in a different business environment. This is potentially important for businesses operating on tighter profit margins and another example of the onion model of security employed by the firm in Case Study 1. Furthermore, firms are at an indirect risk of cyber-attacks via linkages with partners and supply chain firms. In this context, small, smart and bespoke IT security systems are used to minimise the risks specific to the company and its business.

Case Study 5: Service providers are rich targets for cyber-attackers

As a service provider this company is not an obvious target for state sponsored cyber-attacks. As an outsourcing company, it does not have valuable intellectual property and holds only a limited amount of commercially sensitive business information. However it does manage large amounts of client data, which may be coveted by cyber-attackers. The same is true for many types of service providers, such as law firms and accounting firms (some incidents with service providers were also covered in Chapter 4). This raises the question of whether firms which are service providers might be targeted as a back door to client information and whether awareness-raising also needs to be enhanced at such organisations.

High volume operations by service providers pose a potential risk

This particular firm holds more than 500 different contracts across the globe. In the UK alone, this firm employs tens of thousands of employees. The firm is involved in a wide range of projects, with a diverse client list, which includes a number of national governments. The sheer volume of its operations makes it an attractive target for cyber-attacks.

This company experienced one known state-sponsored cyber-attack, which CPNI alerted it to. For this cyber-attack, the company spent £250,000 in incident management alone, a figure that is 10 times larger than what spend would be to remedy a typical (non-state sponsored) cyber-attack. Although no data loss was found, the clean-up effort, outsourced to a British firm, took six months of work. An aggregate estimate of all costs of the incident, including indirect costs such as man-hours of employees assigned to the project, lost productivity, etc. brings the total cost closer to an estimated £350,000 for one APT. As this is the only state-sponsored attack detected by

this organisation within the last 24 months, it is interesting to compare this figure to some of the survey results reported in Chapter3.

Reputational costs are of particular concern to firms

In addition to the monetary cost of any given breach, there is also a potentially substantial reputational cost. Companies are bound by the UK's data protection act to disclose losses associated with a security breach, although the reputational damage could sometimes outweigh any fines under this legislation. An EU-wide data directive is due to come out this year, which might make disclosure of data breaches mandatory or introduce heftier fines. That could change the game with regards to IT investment for many firms in the service sector.

This company is spending approximately £500,000 per year to bolster its IT capabilities as part of a three-year cyber programme to fix gaps in its cyber-armour. Recognising that there is not one perfect tool to prevent or protect against cyber-attacks, the IT security team are taking a balanced approach, making sure not to overinvest in any one area while leaving gaps in others.

Case Study 6: A Cyber Attack Resulting in a Crippling Loss of Business

Although many cyber-attacks never result in a loss of business confidential information, intellectual property, or other valuable information, some do, with potentially devastating consequences. In addition, some of the more sophisticated state-sponsored cyber-attacks are never detected, rendering the likelihood of identifying negative impacts from such attacks much lower. This case provides an example of a company that experienced a devastating loss of intellectual property in 2011 and was able to detect this loss due to the sloppy way in which the cyber-attackers covered their tracks.

The Business of AMSC

AMSC is a global solutions provider serving wind and power grid businesses, founded in 1987. The CEO, Daniel McGahn, had honed the company's research capabilities on wind-turbine control systems to market to Chinese companies. The main customer of AMSC's wind turbine software, Sinovel, represented more than two-thirds of AMSC's $315 million annual revenue in 2010. This customer, in turn, stole the source code of AMSC software (via an insider), effectively shutting AMSC out of the market in China and even began to export to international markets, providing direct competition to AMSC with their stolen software in those markets.

Detection of Loss

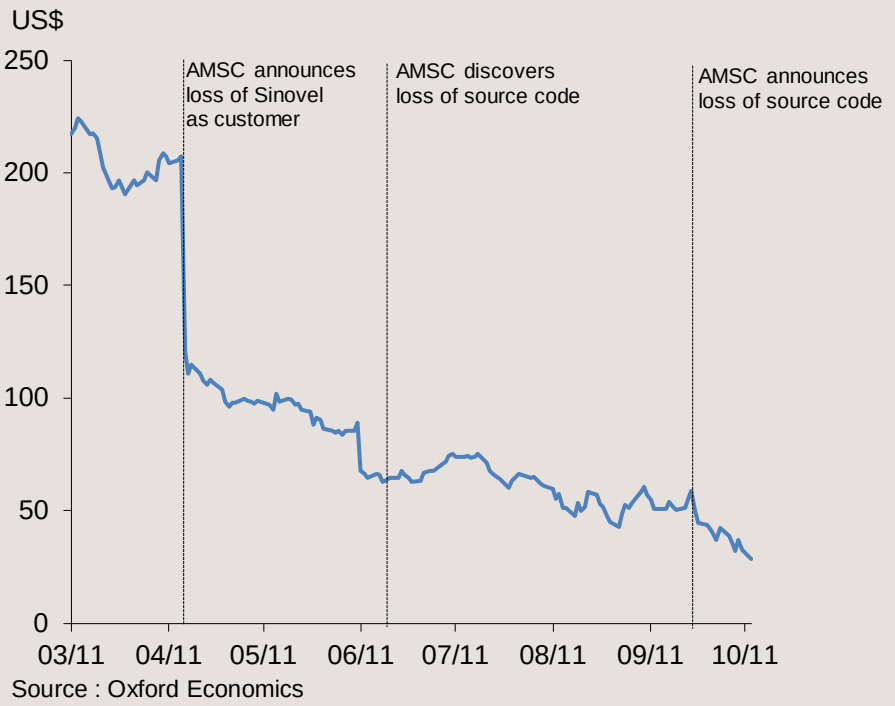
The first clue that something was amiss came when Sinovel, in March 2011, began turning away AMSC shipments. By April 2011, Sinovel had stopped making purchases altogether. Two months later, tests of new software on wind turbines in China failed, necessitating a visit to the turbine to examine the cause of the failure. At this point, AMSC discovered that the turbines were running a pirated version of AMSC software. Upon further investigation, AMSC uncovered that Sinovel had paid an AMSC software engineer working at their Austrian research facility, Dejan Karabasevic, $1.7 million over a six-year contract period to steal AMSC's source code and write software for Sinovel's existing wind turbines.

This is an example of a more uncommon type of cyber-attack, as the source code was taken via an insider. The likely reason an insider theft occurred, rather than an outright cyber-attack, is that the Austrian research facility housed the source code on a server that was not accessible from the Internet. This was done to prevent the more typical remotely instigated cyber-attack. Still, Sinovel found a way around this by paying one of AMSC's engineers to steal the code instead. It goes to show that even a rigorous cyber-security strategy still does not guarantee protection from cyber-attacks.

Impacts of Loss

The shipment of supplies that Sinovel turned away on March 31, 2011 was worth $70 million, and AMSC claimed it was owed another $70 million for components already shipped. Furthermore, AMSC lost the entire value of several supply contracts with Sinovel, set to run through to 2013 and worth more than $700 million. With regard to shareholder valuations, when AMSC announced in April 2011 that it lost its biggest customer, investors fled, scrubbing 40% of the valuation of AMSC in a single day. By September 2011, AMSC had lost 80% of its value. From August 2011 to September 2011, the company had made redundant 30% of its staff. The chart below shows the trend in AMSC share prices.

AMSC NASDAQ Share Prices: March 2011- October 2011



Source : Oxford Economics

Legal Action against Sinovel

In order to recoup some of these losses, AMSC filed several cases with different authorities. AMSC filed an arbitration case relating to unpaid shipments in Beijing. In addition, in September 2011, AMSC filed four civil complaints in Chinese courts claiming $1.2 billion in damages. Also, the company requested that the Chinese police bring criminal action against Sinovel and some Sinovel employees. China's Supreme Court rejected Sinovel's request that the two copyright-infringement cases be moved to arbitration in February 2014, and ruled that the cases will be heard in court.

After publically announcing the theft of the software, Sinovel lost its first major international client (to whom it was going to export turbines with the stolen software). AMSC can file lawsuits in any market in which Sinovel exports turbines with the stolen code. When stolen software was discovered in Sinovel turbines in the United States, AMSC filed a suit and the U.S. Department of Justice charged Sinovel and two Sinovel employees for the theft of AMSC source code and the use of that code in four Sinovel turbines installed in the state of Massachusetts.

6 Bibliography

BIS, PWC, Infosecurity Europe. “2013 Information Security Breaches Survey. A Technical Report” (2013)

BIS, PWC, Infosecurity Europe. “2013 Information Security Breaches Survey. A Technical Report” (2013).

Boardman, A., Greenberg D., Vining, A. & Weimer D., (2005) Cost-Benefit Analysis (3rd Edition).

Brand S., Price R. (2000) “The Economic and Social Cost of Crime” Home Office Research Study 217

Campbell, K., Gordon, L., Loeb M. and Zhou, L. (2003), “The economic cost of publicly announced information security breaches: empirical evidence from the stock market,” Journal of Computer Security 11, pp. 431-448.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004), “The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers,” International Journal of Electronic Commerce, Fall 2004, Vol.9, No. 1, pp. 69-104.

Cousineau D. & Chartier S., (2010) “Outliers detection and treatment: a review” International Journal of Psychological Research 3 (1).

D. Florencio, C. Herley. “Sex, Lies and Cyber-crime surveys”. Microsoft Research. (2013)

Detica, Office of Cyber Security and Information Assurance in the Cabinet Office. “The Cost of Cyber Crime” (2011).

Florencio & Herley (2013), “Sex, lie and cyber-crime surveys,” Microsoft Research.

Friedman, A., Mack-Crane, A. & Hammond, R., Brookings Institute Center for Technology Innovation. “Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences” (2013)

G. S. Becker (1968) Crime and Punishment: An Economic Approach, Journal of Political Economy 76:169-217

Garg, A., Curtis, J., Halper, H. (2003), “Quantifying the financial impact of IT security breaches,” Information Management & Computer Security, 11/2, pp. 74-83.

Gordon, L. and Silvester, K. (1999), “Stock market reactions to activity-based costing adoptions,” Journal of Accounting and Public Policy, Vol. 18, pp. 229-251.

HM Treasury (2006), Gowers Review of Intellectual Property; Intellectual Property Office. “Digital Opportunity: A Review of Intellectual property and Growth” (2011)

Khetri N., (2009) “Positive externality, increasing returns and the rise in cybercrimes”, Communications of the ACM, 52(12), 141-144.

Khotari, S.P., and Warner, J.B. (2006), "Econometrics of event studies", *Handbook of Corporate Finance: Empirical Corporate Finance,* Vol. A, Chapter 1

Klimburg, A. (2011) "Mobilising Cyber Power" Survival vol 53.no. 1 (February-March 2011) pp 41-60

MacKinlay, C. (1997), "Event studies in economics and finance," Journal of Economic Literature, Vol. 35, No. 1, pp. 13-39.

McAfee, Centre for Strategic and International Studies. "The Economic Impact of Cybercrime and Cyber Espionage." (2013)

Ponemon Institute. "2013 Cost of Cyber Crime Study: United Kingdom" (2013)

7 Appendix 1 - Survey Questionnaire

Business Impact of Cyber Insecurity on UK Companies

Final. Prepared by Ponemon Institute, 6 January 2014

Dear Respondent:

The purpose of our study, conducted on behalf of the Government, is to better understand the cyber-security threats and challenges facing UK companies and their impact on firms. Your participation in this survey is completely confidential. No personally identifiable or company identifiable information is requested. All responses will be compiled, analysed, and distributed at an aggregate level.

If you have specific questions or issues regarding this survey, please contact Ponemon Institute at research@ponemon.org.

Respectfully,

L.A. Ponemon

Chairman & Founder
Ponemon Institute LLC

Definitions

Organisation refers to the working unit where you exercise your role or function. For instance, you may define your organisation as the IT department, corporate compliance, risk management, finance and accounting and so forth.

Cyber attack refers to all computer-based assaults on an organisation's IT infrastructure, applications, databases and source data. Cyber attacks typically involve malicious software or code that seeks to infiltrate networks or infect endpoint devices. While the attacker is often an external agent such as a lone hacker, criminal syndicate or nation-sponsored agents, attack methods may also involve malicious or criminal insiders.

S1. Which of the following best describes your role in managing the IT function within your organisation? Check all that apply.

— Setting IT priorities
— Managing IT budgets
— Selecting vendors and contractors
— Determining IT strategy
— Evaluating programme performance
— Bolstering IT security
— None of the above [STOP]

Part 1: Your organisation's security posture

Q1. How would you rate your organisation's cyber security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)?

Not effective	1	2	3	4	5	6	7	8	9	10	Very effective

Q2a. How does your organisation determine the qualifications or expertise of personnel who manage cyber security risk? Please select all that apply.

— Professional certification
— Work histories (on the job experience)
— Specialised training
— Advanced degrees
— Other (please specify)

Q2b. Does your organisation have a sufficient number of in-house personnel who possess these qualifications?

— Yes
— No

Part 2: Cyber attack experience

Q3. How many cyber attacks has your organization experienced over the past 12 months?

— None (Go to Q13)
— 1 to 2
— 3 to 4
— 5 to 6
— 7 to 8
— 9 to 10
— More than 10

Q4. Has your organisation experienced an incident involving the loss or exposure of sensitive information in the past 12 months?

— Yes
— No
— Unsure

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.

Q5a. Has your organisation ever experienced situations when cyber attacks have evaded your intrusion detection systems (IDS)?	Q5b. Has your organisation ever experienced situations when cyber attacks have evaded your anti-virus (AV) solutions?
— Yes — No	— Yes — No

Q5c. Do you consider these any of these exploits an APT?

— Yes
— No

Q6. How many separate APT-related incidents did your organisation experience over the past 12 months?

— None (Go to Q8)
— 1 to 2
— 3 to 4
— 5 to 6
— 7 to 8
— 9 to 10
— More than 10

Q7. What happened to your organisation as a result of the APTs it experienced? Please select all that apply.

— Nothing happened
— IT downtime
— Business interruption
— Exfiltration of classified or sensitive information
— Theft of personal information
— Damage to IT infrastructure
— Damage to software (source code)
— Destruction of information asset
— Other (please specify)

Q8. Please rank order the following types of attackers from 1 = most likely to launch to 6 = least likely to launch an attack against your company.

— Nation-state attackers
— Criminal syndicates
— Lone wolf hacker
— Hacktivists
— Cyber-terrorists
— Other corporations

Please rate the following statements using one of the three choices provided below each item. Note that the time period for estimating the net change is the previous **24 months** (relative to the prior years).

Q9a. Within your organisation, how has the **frequency of all** cyber attacks changed?

Increased	Stayed the same	Decreased	Don't Know

Q9b. Within your organisation, how has the **frequency of targeted** cyber attacks changed?

Increased	Stayed the same	Decreased	Don't Know

Q9c. Within your organisation, how has the **sophistication level** of cyber attacks changed?

Increased	Stayed the same	Decreased	Don't Know

Q9d. Within your organisation, how has the **severity level** of cyber attacks changed?

Increased	Stayed the same	Decreased	Don't Know

Q10. Is your organisation's cyber security strategy **aligned** with its business objectives and mission?

— Yes, fully aligned
— Yes, partially aligned
— No, not aligned
— Cannot determine

Q11. What challenges keep your organisation's cyber security posture from being fully effective? Please rank the following choices from 1 = most challenging to 8 = least challenging.

— Insufficient budget (money)
— Insufficient personnel
— Lack of in-house expertise
— Lack of clear leadership
— No understanding how to protect against cyber attacks
— Management does not see cyber attacks as a significant risk
— Lack of collaboration with other functions
— Not regarded as a priority issue

Q12. Using the following scale, how difficult is it for your organization to achieve a fully effective cyber security posture?

Not difficult	1	2	3	4	5	6	7	8	9	10	Very difficult

Part 3. Organisational assets at risk

Q13a. The following table provides five **tangible assets** that may be put at risk as a result of cyber attacks against your company. Please rate each asset type using the following scale to denote the **potential impact** of asset compromise to your organisation:

No impact	1	2	3	4	5	6	7	8	9	10	Catastrophic impact

Asset Types	Definitions	Rating
People	Loss of or harm to people within the organisation	
Premises and locations	Buildings, estates and other relevant physical places	
Plant and equipment	All physical equipment and machinery including computers	
Money	Currency of any kind, promissory notes and other financial instruments	
Materials	Physical commodities, resources or purchased products	

Q13b. The following table provides five **information assets** that may be put at risk as a result of cyber attacks against your company. Please rate each asset type using the following scale to denote the **potential impact** of asset compromise to your organisation:

No impact	1	2	3	4	5	6	7	8	9	10	Catastrophic impact

Asset Types	Definitions	Rating
Access data	Data that enables access previously prevented by security measures	
Procedures and process	Description of how things work within an organisation	
Personal data	Personal data of all sorts that identifies the natural person	
Intellectual property	Key knowledge information held by an organisation	
Commercially sensitive	Business information that can give competitors or external agents commercial advantages	

Q13c. The following table provides four **intangible assets** that may be put at risk as a result of cyber attacks against your company. Please rate each asset type using the following scale to denote the **potential impact** of asset compromise to your organisation:

No impact	1	2	3	4	5	6	7	8	9	10	Catastrophic impact

Asset Types	Definitions	Rating
Staff well being	Feeling of satisfaction and contentment associated with health, welfare and quality of life for those internal to the organisation	
Public well being	Feeling of satisfaction and contentment associated with health, welfare and quality of life for those external to the organisation	
Reputation	Public perception of the organisation, including perceived ethics and trustworthiness	
Business volume	Potential loss of business prospects, including client relationships, customer support and the organisation's ability to continue as a going concern	

Part 4. Cost estimation

What range best describes the total cost incurred by your organisation in the **past 24 months** due to cyber attacks? For purposes of estimating total costs, please refer to the following five categories.

- Remediation and technical support activities including forensic investigations, incident response activities, help desk and customer service operations
- Users' idle time and lost productivity because of downtime or system performance delays
- Disruption to normal operations because of system availability problems
- Damage or theft of IT assets and infrastructure
- Reputation loss and brand damages

Please note that the cost estimate should include all direct cash outlays, direct labour expenditures, indirect labour costs, overhead costs and lost business opportunities.

Q14a. Approximately, how much did cyber security compromises cost your organisation in terms of clean-up or remediation (including technical support costs)?

— Zero	— £5,000,001 to £10,000,000
— Less than £100,000	— £10,000,001 to £25,000,000
— £100,001 to £250,000	— £25,000,001 to £50,000,000
— £250,001 to £500,000	— £50,00,001 to £100,000,000
— £500,001 to £1,000,000	— More than £100,000,000
— £1,000,001 to £5,000,000	— Cannot estimate

Q14b. Approximately, how much did cyber security compromises cost your organisation in terms of lost user productivity?

— Zero	— £5,000,001 to £10,000,000
— Less than £100,000	— £10,000,001 to £25,000,000
— £100,001 to £250,000	— £25,000,001 to £50,000,000
— £250,001 to £500,000	— £50,00,001 to £100,000,000
— £500,001 to £1,000,000	— More than £100,000,000
— £1,000,001 to £5,000,000	— Cannot estimate

Q14c. Approximately, how much did cyber security compromises cost your organisation in terms of disruption to normal operations?

— Zero	— £5,000,001 to £10,000,000
— Less than £100,000	— £10,000,001 to £25,000,000
— £100,001 to £250,000	— £25,000,001 to £50,000,000
— £250,001 to £500,000	— £50,00,001 to £100,000,000
— £500,001 to £1,000,000	— More than £100,000,000
— £1,000,001 to £5,000,000	— Cannot estimate

Q14d. Approximately, how much did cyber security compromises cost your organisation in terms of damage or theft of IT assets and infrastructure?

— Zero — Less than £100,000 — £100,001 to £250,000 — £250,001 to £500,000 — £500,001 to £1,000,000 — £1,000,001 to £5,000,000	— £5,000,001 to £10,000,000 — £10,000,001 to £25,000,000 — £25,000,001 to £50,000,000 — £50,00,001 to £100,000,000 — More than £100,000,000 — Cannot estimate

Q14e. Approximately, how much did cyber security compromises cost your organisation in terms of damage to reputation and marketplace image (brand value)?

— Zero — Less than £100,000 — £100,001 to £250,000 — £250,001 to £500,000 — £500,001 to £1,000,000 — £1,000,001 to £5,000,000	— £5,000,001 to £10,000,000 — £10,000,001 to £25,000,000 — £25,000,001 to £50,000,000 — £50,00,001 to £100,000,000 — More than £100,000,000 — Cannot estimate

Firms may also experience a loss of intellectual property due to cyber attacks as research, techniques and "know-how" are acquired virtually "free of charge".

In addition, firms may lose commercially sensitive business information (e.g. negotiation strategies, stock information, business plans and strategies), which may confer more immediate benefits.

In the context of the following questions, please assume intellectual property refers to a product of the intellect that has **commercial value**, including copyrighted or patented property such as literary or artistic works, appellation of origins, business methods, and industrial processes. Please note the greatest risk to organisations is the theft of intellectual property not protected by copyrights, patents or other legal systems.

Q15a. Has your firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 24 months?

— Yes
— No (Go to Q20)

Q15b. If yes, do you think the loss of **intellectual property**, in particular, has caused your firm to lose a competitive advantage? Or do you think that this isn't really the case (e.g. perhaps rivals can't use information in an effective manner or perhaps information will soon be out of date)?

— Yes, I believe it has caused a loss of competitive advantage
— No, it hasn't caused a loss of competitive advantage

Q16a. Do you think the loss of **commercially sensitive business information**, in particular, has caused your firm to lose its competitive advantage? Or do you think that this isn't really the case?

— Yes, I believe it has caused a loss of competitive advantage
— No, it hasn't caused a loss of competitive advantage

Q16b. If yes, how did your firm determine the loss of competitive advantage as a result of the cyber attack?

— Emergence of new competition
— Appearance of copied products or activities
— Soured deals or business ventures
— Compromised negotiations
— Gut feeling
— Other (please specify)

Q17. How has the loss of intellectual property or other commercially sensitive business information affected your firm's propensity to make investments in research and development?

[Contextual response]

Q18a. How did your organisation's investments in research and development change as a result of the cyber attacks it experienced?

— Increase in investment
— No change in investment
— Decrease in investment

Q18b. [If you selected decrease or increase] How much did investments in research and development change as a result of the cyber attacks your organisation experienced?

— Less than 5%
— 5 to 10%
— 11 to 15%
— 16 to 25%
— 26 to 50%
— More than 50%

Please choose the cost range that denotes potential losses due to the theft of your company's intellectual property and other commercially sensitive information.

Q19a. Approximately, how much did losses due to the theft of intellectual property cost your organisation over the past 24 months?

— Zero	— £5,000,001 to £10,000,000
— Less than £100,000	— £10,000,001 to £25,000,000
— £100,001 to £250,000	— £25,000,001 to £50,000,000
— £250,001 to £500,000	— £50,00,001 to £100,000,000
— £500,001 to £1,000,000	— More than £100,000,000
— £1,000,001 to £5,000,000	— Cannot determine

Q19b. Approximately, how much did losses due to theft of commercially sensitive information cost your organisation over the past 24 months?

— Zero — Less than £100,000 — £100,001 to £250,000 — £250,001 to £500,000 — £500,001 to £1,000,000 — £1,000,001 to £5,000,000	— £5,000,001 to £10,000,000 — £10,000,001 to £25,000,000 — £25,000,001 to £50,000,000 — £50,00,001 to £100,000,000 — More than £100,000,000 — Cannot determine

Q19c. Please explain how you arrived at the estimated cost ranges provided in Q19a and Q19b.

— Prior internal assessment has been conducted
— Prior assessment has been conducted by external consultants
— Rough estimation
— Gut feel
— Other [Contextual response]

Q20. One of the aims of this survey is to increase understanding of the nature of cyber attacks and the damage they could do to firms operating in the UK. Do you have an experience with a cyber attack which you believe provides a good illustration of the damage it can do?

— Yes
— No

If yes, please feel free to share some of the details about this cyber attack in the space provided below or contact research@ponemon.org to schedule a confidential interview. As is the case with the rest of this survey all responses will be treated as **anonymous** unless you indicate otherwise.

[Contextual response]

Part 5. Role & Organisational Characteristics

D1. What best describes your position or organisational level?

— Department head
— Executive/Director
— Manager
— Supervisor
— Technician
— Associate/staff
— Consultant/contractor
— Other (please specify)

D2. What best describes your company's primary industry classification?

— Academia
— Aerospace & Defence
— Automotive
— Chemicals
— Conglomerates
— Construction
— Creative & Media
— Energy – Oil & Gas
— Energy – Power Generation
— Financial Services
— Legal Services
— Life Sciences (Biotech & Pharmaceuticals)
— Manufacturing
— Mining
— Professional Services
— Telecom
— Transportation
— Other

D3. What is the worldwide headcount of your organisation?

— < 1,000
— 1,000 to 5,000
— 5,001 to 25,000
— 25,001 to 75,000
— > 75,000

D4. What is the UK headcount of your organisation?

— < 1,000
— 1,000 to 5,000
— 5,001 to 25,000
— 25,001 to 75,000
— > 75,000

D5. What is the worldwide revenue of your organisation for the last fiscal year? If you're unsure, please provide a rough estimate.

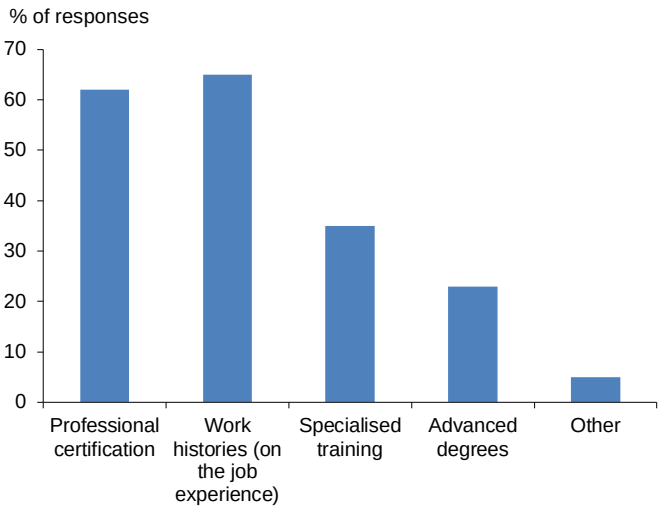
— Under £20 million
— £20 million to £49.9 million
— £50 million to £299.9 million
— £300 million to £999.9 million
— £1 billion to £2.99 billion
— £3 billion to £6.99 billion
— £7 billion and above

D6. What is the UK revenue of your organization for the last fiscal year? If you're unsure, please provide a rough estimate.

— Under £20 million
— £20 million to £49.9 million
— £50 million to £299.9 million
— £300 million to £999.9 million
— £1 billion to £2.99 billion
— £3 billion to £6.99 billion
— £7 billion and above

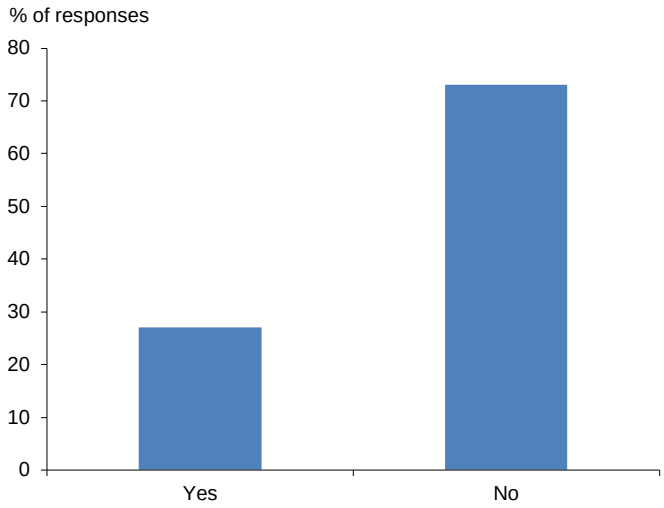
8 Appendix 2 – Survey results

Chart A2.1: Q2a "How does your organisation determine the qualifications or expertise of personnel who manage cyber security risk? Please select all that apply."



Source : Oxford Economics/Ponemon Institute

Chart A2.2: Q2b "Does your organisation have a sufficient number of in-house personnel who possess these qualifications?"



Source : Oxford Economics/Ponemon Institute

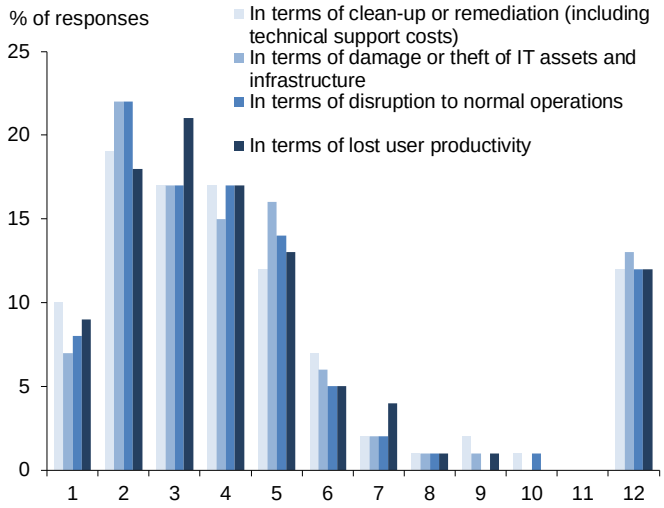
Chart A2.3: Q14a "Approximately, how much did cyber security compromises cost your organisation in terms of clean-up or remediation (including technical support costs)?"

Q14b "Approximately, how much did cyber security compromises cost your organisation in terms of lost user productivity?"

Q14c "Approximately, how much did cyber security compromises cost your organisation in terms of disruption to normal operations?"

Q14d "Approximately, how much did cyber security compromises cost your organisation in terms of damage or theft of IT assets and infrastructure?!"

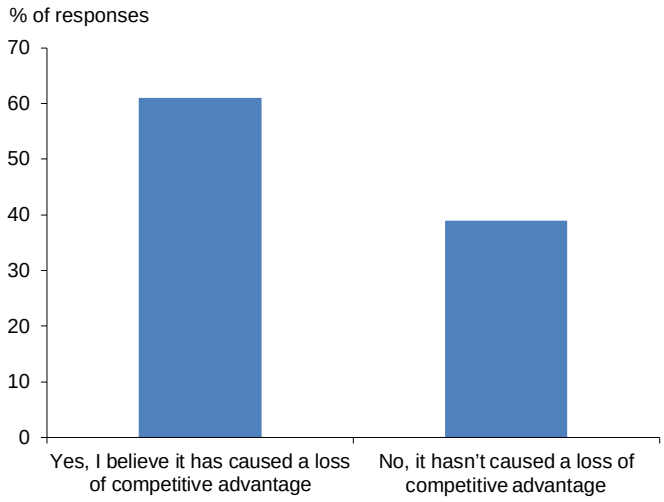
Q14e "Approximately, how much did cyber security compromises cost your organisation in terms of damage to reputation and marketplace image (brand value)?"



1 Zero
2 Less than £100,000
3 £100,001 - £250,000
4 £250,001 - £500,000
5 £500,001 - £1,000,000
6 £1,000,001 - £5,000,000
7 £5,000,001 - £10,000,000
8 £10,000,001 - £25,000,000
9 £25,000,001 - £50,000,000
10 £50,00,001 - £100,000,000
11 More than £100,000,000
12 Cannot estimate

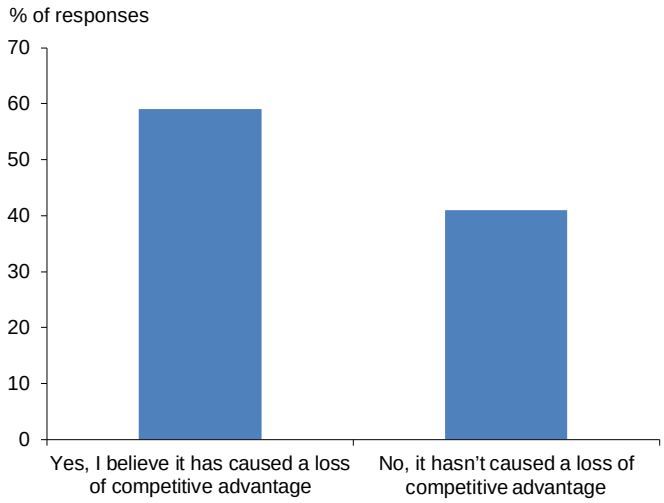
Source : Oxford Economics/Ponemon Institute

Chart A2.4: Q15b "If yes [to Q15a], do you think the loss of intellectual property, in particular, has caused your firm to lose a competitive advantage? Or do you think that this isn't really the case (e.g. perhaps rivals can't use information in an effective manner or perhaps information will soon be out of date)?"



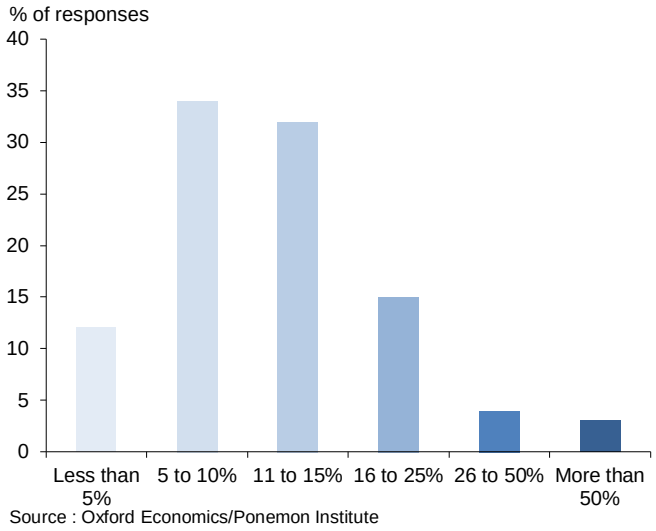
Source : Oxford Economics/Ponemon Institute

Chart A2.5: Q16a "Do you think the loss of commercially sensitive business information, in particular, has caused your firm to lose its competitive advantage? Or do you think that this isn't really the case?"



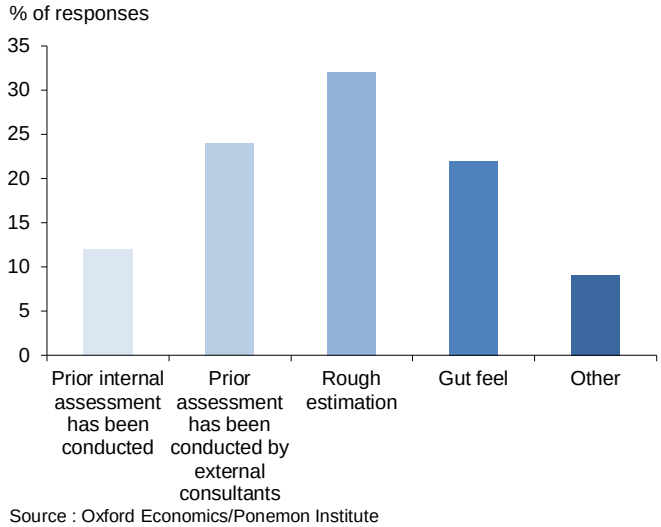
Source : Oxford Economics/Ponemon Institute

Chart A2.6: Q18b "(If you selected decrease or increase [In Q18a]) How much did investments in research and development change as a result of the cyber-attacks your organisation experienced?"



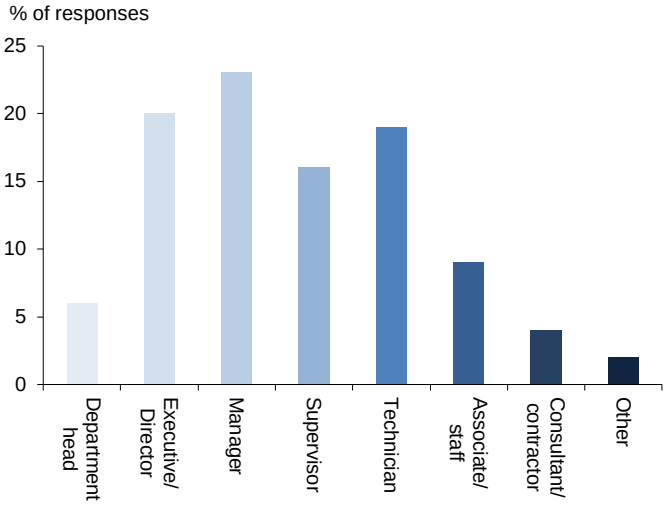
Source : Oxford Economics/Ponemon Institute

Chart A2.7: Q19c "Please explain how you arrived at the estimated cost ranges provided in Q19a and Q19b."



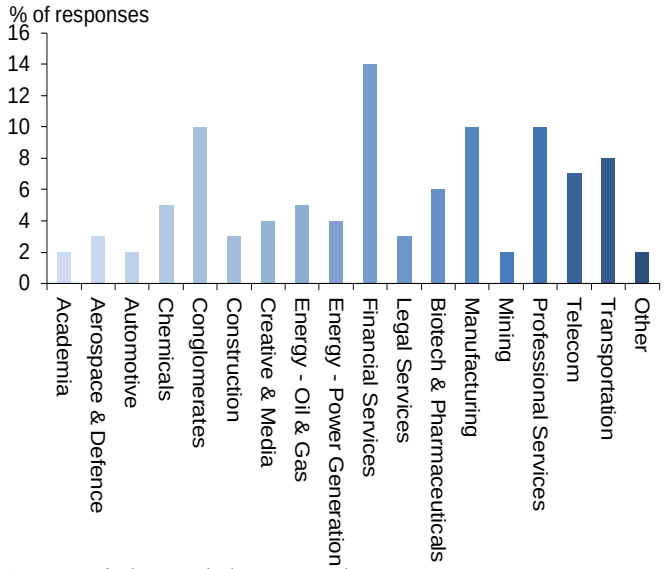
Source : Oxford Economics/Ponemon Institute

Chart A2.8: D1 "What best describes your position or organisational level?"



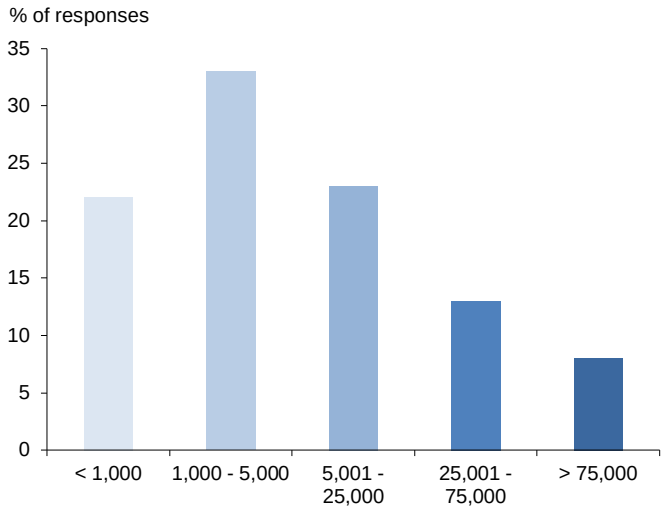
Source : Oxford Economics/Ponemon Institute

Chart A2.9: D2 "What best describes your company's primary industry classification?"



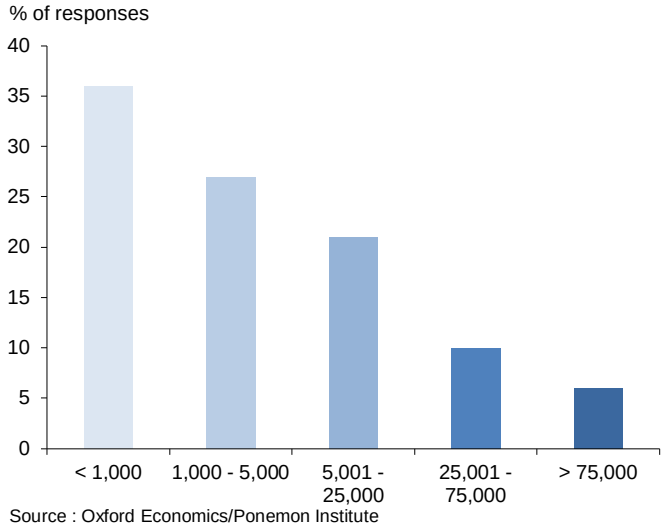
Source : Oxford Economics/Ponemon Institute

Chart A2.10: D3 "What is the worldwide headcount of your organisation?"



Source : Oxford Economics/Ponemon Institute

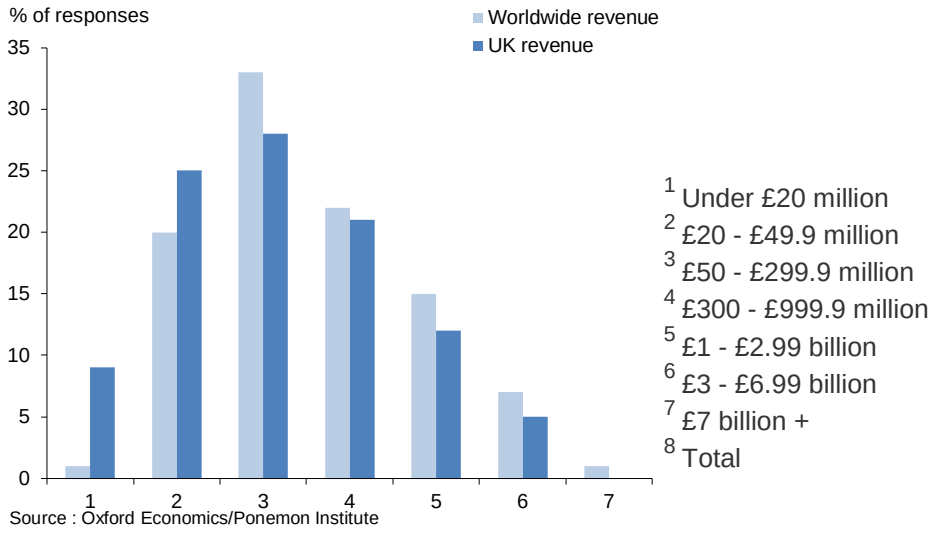
Chart A2.11: D4 "What is the UK headcount of your organisation?"



Source : Oxford Economics/Ponemon Institute

Chart A2.12: D5 "What is the worldwide revenue of your organisation for the last fiscal year? If you're unsure, please provide a rough estimate."

D6 ""What is the UK revenue of your organisation for the last fiscal year? If you're unsure, please provide a rough estimate."



Source : Oxford Economics/Ponemon Institute

9 Appendix 3 – Survey results – Question 17

Business impact of cyber insecurity on UK companies: Contextual responses to Q17

Presented by Dr. Larry Ponemon in paraphrased format

No#	Q17. How has the loss of intellectual property or other commercially sensitive business information affected your firm's propensity to make investments in research and development?
5	It did not affect my company's propensity to invest in innovations and product research
7	I cannot tell and do not what to guess
24	[My company] had to increase R&D budget to make up lost ground
30	Blank
36	I don't see any changes in our investments in innovations and technologies
41	We are more careful in protecting our sensitive and confidential information and IP
49	Blank
51	Blank
55	Blank
58	The theft of confidential commercially sensitive data has no [impact] on investments in research and development
63	Blank
64	I really do not know
75	Blank
76	Blank
80	I really don't think it affects our investments now or in the future
83	Blank
96	Investments in R&D security will substantially increase
101	Cannot tell, but it likely made us more cautious
102	I cannot determine
103	Blank
104	I cannot determine as yet. But I think it will diminish investments in the future
106	Blank
107	Blank
120	Blank
143	Definitely caused my management to re-think our total investment strategy
144	I don't see how this will affect investments going forward
146	Blank
149	This is a big problem. Our MD/board is now considering the long term impact. However, I don't see any change in investments or R&D activities
153	I think we are still committed and may be more so as a result of the [IP] theft
159	Blank
167	Beyond investments in new security procedures, I did not see any change in our propensity to invest.
169	Research and development continues at the same level as before the incident
171	R&D investments had to increase
174	Blank
179	I don't see any changes in R&D spend as yet
183	I do not see any change in our investment propensities
185	While management is more cautious, we had to investment more to maintain competitive ground
196	Cannot tell
212	Blank
215	Blank

Business impact of cyber insecurity on UK companies: Contextual responses to Q17

Presented by Dr. Larry Ponemon in paraphrased format

No#	Q17. How has the loss of intellectual property or other commercially sensitive business information affected your firm's propensity to make investments in research and development?
219	I think we are investing resources and personnel at the same level.
222	My company had to increase this year's research budget because of competitor gains
223	No changes
224	Our board is concerned that the theft of IP demands renewed commitment in IP investment
233	Blank
237	Blank
241	Blank
246	Just as before. I don't think it affects our research and development efforts
254	I cannot tell for certain, but I don't see any long term consequences on investment and spending
258	I think investment had to increase in the short run only
259	Blank
264	Blank
268	It is difficult to estimate the propensity to invest. I think the theft of IP caused my company to invest less.
278	Blank
281	New product research has to continue
295	I cannot determine as yet. But I think it will diminish investments in the future
297	Blank
302	Blank
304	Everything appears to be the same. I cannot tell for certain
307	Blank
312	I do not really know but I predict we will spend less in the future
314	We are investing just as before. Why should it have any influence on our propensity to invest?
316	Blank
317	I don't know or see any true changes.
338	Blank
342	Blank
349	Blank
352	In the short run, no impact whatsoever. In the longer term, I don't know
357	Our management is considering this issue at presentl
361	We are likely to decrease our expenditures on R&D given the huge loss in IP
363	Blank
364	Management is pissed off. But we are not cutting investments.
365	Blank
367	My organisation has stepped up spending on security controls over IP and business confidential information
372	Blank
376	The research and development activites had to step up because of economic espionage by the Chinese
378	Blank
382	My belief is that we had to increase investment to keep pace with our competitors
389	Despite the theft, we are just as committed to new product innovations. So, I don't see or predict any change in investments.
391	I can't comment on the particulars, but we did not change our investment level just our strategies

Business impact of cyber insecurity on UK companies: Contextual responses to Q17

Presented by Dr. Larry Ponemon in paraphrased format

No#	Q17. How has the loss of intellectual property or other commercially sensitive business information affected your firm's propensity to make investments in research and development?
396	It is difficult to determine but my intuition is that it will cause us to change our research and development strategies
399	Blank
412	We wil likely spend less on IP and more on IP security
415	Blank
418	I did not observe any substantive changes in investments or spending levels
419	Blank
423	Blank

10 Appendix 4 – Event analysis sample database

Company	Industry	Disclosure Date
AT&T	Telecoms	25/08/2006
TJX (T K Maxx/T J Maxx)	Retail	17/01/2007
Monster.com	Professional Services	21/08/2007
Delhaize Group	Retail	27/02/2008
Trend Micro	Technology	13/03/2008
Intercontinental Exchange	Financial Services	08/07/2009
Nasdaq OMX	Financial Services	08/07/2009
Citigroup	Financial Services	22/12/2009
Adobe	Technology	12/01/2010
Google	Technology	12/01/2010
Intel	Technology	05/02/2010
BHP Billiton	Mining	19/04/2010
Fortescue Metals	Mining	19/04/2010
Rio Tinto	Mining	19/04/2010
EMC	Technology	18/03/2011
Sony (Playstation Network)	Technology	26/04/2011
Lockheed Martin	Aerospace & Defence	28/05/2011
Citigroup	Financial Services	09/06/2011
AMSC	Energy - Power Generation	15/09/2011
Mitsubishi Heavy Industries	Aerospace & Defence	19/09/2011
Symantec	Technology	02/02/2012
VeriSign (Symantec Corp)	Technology	02/02/2012
Nissan	Automotive	23/04/2012
Under Armor	Retail	23/04/2012
Adobe	Technology	27/09/2012
Korn Ferry International (KFY)	Professional Services	11/10/2012
Coca Cola	Other	04/11/2012
New York Times	Creative and Media	30/01/2013
News Corp	Creative and Media	31/01/2013
Baker Hughes	Energy - Oil & Gas	24/02/2013
BP	Energy - Oil & Gas	24/02/2013
Conocophillips	Energy - Oil & Gas	24/02/2013
Exxon	Energy - Oil & Gas	24/02/2013
Marathon Oil Corp	Energy - Oil & Gas	24/02/2013
Shell	Energy - Oil & Gas	24/02/2013
JP Morgan Chase	Financial Services	13/03/2013
American Express	Financial Services	22/03/2013
Wells Fargo & Co	Financial Services	26/03/2013
QinetiQ	Aerospace & Defence	01/05/2013
Disney	Creative and Media	15/06/2013
New York Times	Creative and Media	27/08/2013
Dun & Bradstreet Corp	Technology	25/09/2013
Reed Elsevier's LexisNexis Inc.	Technology	25/09/2013
United Business Media (UBM)	Creative and Media	16/10/2013
JP Morgan Chase	Financial Services	05/12/2013

Source: Oxford Economics

OXFORD
Abbey House, 121 St Aldates
Oxford, OX1 1HB, UK
Tel: +44 1865 268900

LONDON
Broadwall House, 21 Broadwall
London, SE1 9PL, UK
Tel: +44 207 803 1400

BELFAST
Lagan House, Sackville Street
Lisburn, BT27 4AB, UK
Tel: +44 28 9266 0669

NEW YORK
817 Broadway, 10th Floor
New York, NY 10003, USA
Tel: +1 646 786 1863

PHILADELPHIA
303 Lancaster Avenue, Suite 1b
Wayne PA 19087, USA
Tel: +1 610 995 9600

SINGAPORE
No.1 North Bridge Road
High Street Centre #22-07
Singapore 179094
Tel: +65 6338 1235

PARIS
9 rue Huysmans
75006 Paris, France
Tel: + 33 6 79 900 846

email: mailbox@oxfordeconomics.com

www.oxfordeconomics.com

OXFORD ECONOMICS