The business and economic consequences of inadequate cybersecurity

A research report prepared for Veracode

June 2015

Report contents

This report was produced by the Centre for Economics and Business Research (Cebr) for Veracode.

Cebr is not licensed in the conduct of investment business as defined in the Financial Services and Markets Act 2000. Any client considering a specific investment should consult their own broker or other investment adviser. Any views on investments expressed by Cebr, or on behalf of Cebr, are intended to be generic only. Cebr accepts no liability for any specific investment decision which must be at the investor's own risk.

Whilst every effort has been made to ensure the accuracy of the material in this report, neither the authors nor Cebr will be liable for any loss or damages incurred through the use of this report or associated materials.

Executive Summary

- **60% of CTOs** believe the government is not doing enough to prevent cyberattacks.
- **Top concerns** about cyberattacks are **breach cost** (e.g. forensics, clean-up, legal), and **reputation and brand damage** due to customer data loss and **lost revenue due to downtime**.
- **Cyberattacks cost UK firms £34 billion in revenue losses and subsequent increased IT spending**
  - Cyberattacks cause firms in the UK to **lose approximately £18 billion in revenue**.
  - UK firms increase their annual **IT spending as a result of cybercrime by almost £16 billion**.
- Royal United Service Institute predicts **more damage in the future** and **businesses aren't waiting for government** to rescue them
  - More than half (57%) of **CEOs hold themselves accountable.**
  - 88% have **increased annual IT spending as a result of breaches.**
- 70% of all **CTOs believe that their current cybersecurity policies block innovation** in some way.
- **Theft of corporate intellectual property (IP) as their sixth priority,** yet **34% of cybercrime in UK businesses is tied to IP theft**.
  - Interestingly, the concern over IP theft is in **stark contrast to US perceptions**, where board members ranked amongst their top three.

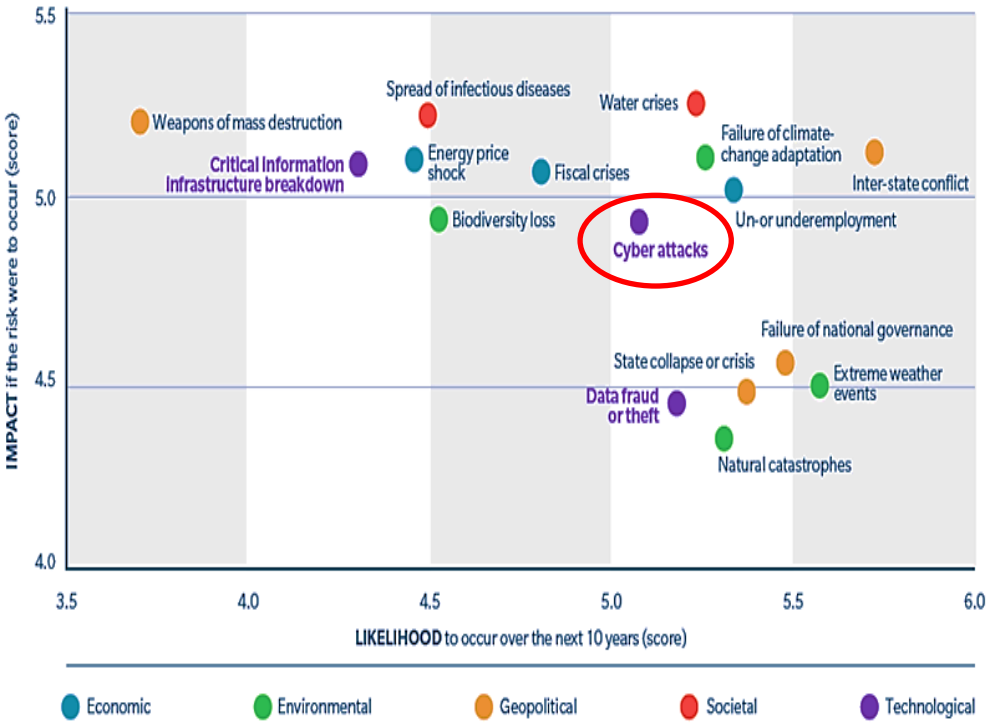
Literature review

Cebr

Cybersecurity has become a major business risk

- Both globally and in the UK, cybercrime has become a major threat to governments, companies and individuals.
- All businesses are in danger – regardless of size and sector. According to the Information Security Breaches Survey (ISBS) **81% of large and 60% of small businesses** in the UK suffered a **cybersecurity breach in 2014.**
- The economic **cost of cybercrime in the UK ranges in the *billions* of pounds**. According to the "most-likely scenario" of the Detica report (in partnership with the Office of Cyber Security and Information Assurance in the UK Cabinet Office) the cost of cybercrime in the UK is estimated at **£27bn per annum.**
- The cost of the most severe security breaches to large UK companies in 2014 **was between £600,000 and £1.15 million** (ISBS).

Top global risks according to the World Economic Forum



Note: Top 10 risks in terms of impact and the top 10 risks in terms of likelihood. Four Risks rank in the top 10 in terms of both impact as well as likelihood. Respondents were asked to rate each risk, based on its impact and likelihood, on a scale from 1 to 7.

Verizon DBIR 2015 study finds that data breaches cost businesses around the world $400 million*

- Verizon's 2015 Data Breach Investigations Report also found that:
  - The **overall number of incidents that ended in data breaches has been increasing** over the last 8 years
  - Not much had changed since the 2014 report in terms of the **top three industries affected**, which still were: **Public sector, Information sector, and Financial Services**.
  - In **70% of cases, cyberattackers are not interested in the primary victim** (i.e. the owner of the website they extract data from), but their main motive is to use the **extracted information to generate the "real attack",** such as hacking a website to deliver malware to specific targets.
  - The DBIR 2015 found that in **60% of cases, cybercriminals** attacking an organisation are able to **compromise systems *within minutes* and web application attacks remain a top threat.**
  - **99.9% of software vulnerabilities exploited in breaches were already known for more than a year**, indicating a need for more rigorous patching processes.
  - The industries **most affected by cyberespionage** are **manufacturing, public sector and professional services.**
  - The top five controls that help **prevent cyberbreaches are web application testing, two-factor authentication, patching web services,** verifying need for Internet-facing devices, logging and verifying outbound traffic.

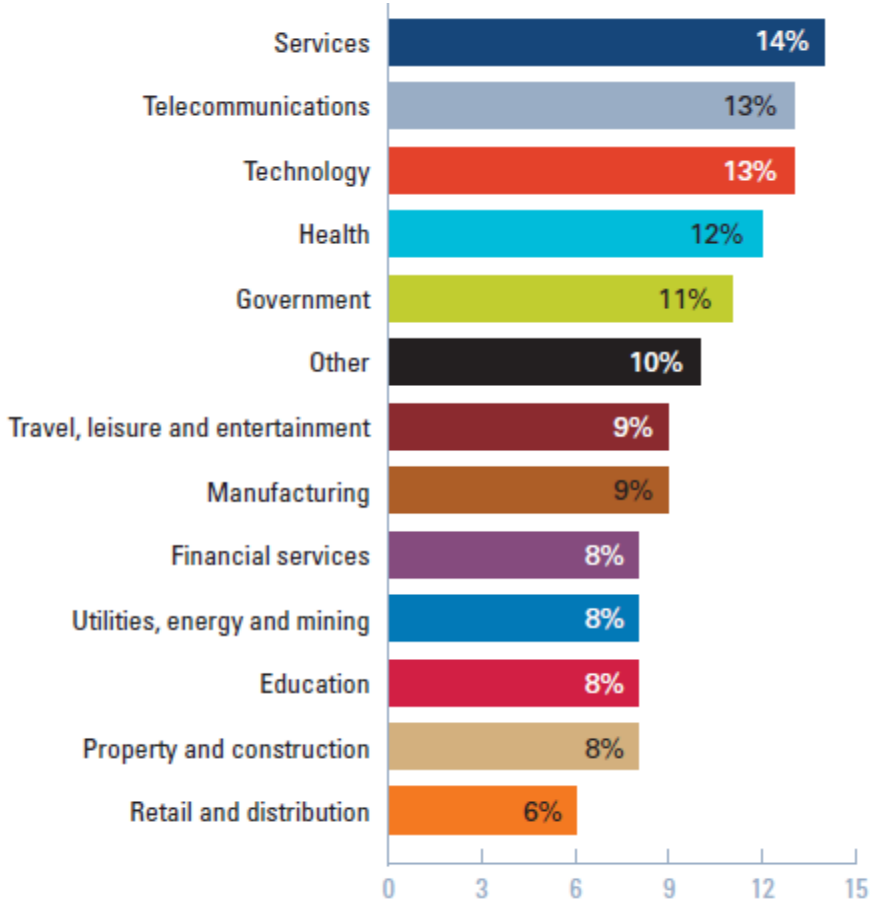
Source: Verizon 2015 Data Breach Investigations Report

**Estimate based on 70 organisations from across the world with 700 million data records compromised, costing them $400 million.*

Which sectors are spending the most on cybersecurity?

- **Spending on cybercrime (according to the 2014 Information Security Breaches Survey):**
  - **Services and telecoms** are both among the industries most seriously affected, and are also the biggest spenders on cybersecurity.
  - **Financial services are spending little on cybersecurity (relative to their overall IT budget)**, relative to other industries such as travel, leisure and entertainment.
- Are the industries that are mostly affected by cyberattacks also the ones spending the most on cybersecurity?
  - **Government is only the fifth largest spender on cybersecurity**. Even though the 2014 Information Security Breaches Survey shows that **77% of the total cost of cybercrime** in the UK is **related to security breaches in the government**.
- According to the 2011 report by Detica in partnership with the Office of Cyber Security & Information Assurance industries can face a variety of cybersecurity threats:
  - The mining sector is targeted for **espionage** to learn how processes work, while pharmaceuticals and biotech are more affected by **IP theft**, targeting proprietary designs.
  - Overall, **34% of cybercrime** in UK businesses **is related to IP theft**.

Percentage of the IT budget being spent on cybersecurity



Source: 2014 Information Security Breaches Survey, Commissioned by BIS conducted by PwC, Infosecurity Europe, and Reed Exhibitions.

Secrecy or transparency: what is more costly?

- **Many companies hesitate to admit that a cybercrime has taken place**, not only out of fear of reputational damage and litigation, but also because revealing their technical weak spots could leave them even more exposed to future cyberattacks.
- Various organisations, however, are calling for more **disclosure (laws)** to communicate these threats. In particular they demand:
  - Require firms to **report breaches in a timely fashion** and **fine companies for not reporting breaches.**
  - Encourage companies to **implement best practices** when dealing with cybersecurity.
- The following organisations are among those encouraging cybersecurity breaches to be communicated to the relevant stakeholders or authorities:
  - **EU watchdog**, made up of representatives from national data protection authorities, issues guidance on the notification of data breaches to individuals.
  - The **Cyber Security Information Sharing Partnership**, which is a joint industry-government initiative to share information to increase awareness of cyberthreats.
  - The **Centre for the Protection of National Infrastructure,** which in its threat assesment criticises the lack of reporting breaches to stakeholders and provides a Cyber Incident Response (CIR) service.
  - The **Information Commissioner's Office (ICO)** published a guidance explaining when and how to report a cybersecurity breach.

Share price declines of US and UK listed companies following cyberattacks

Company name	Announcement of cyber security breach	Drop in share price following breach (%)	
		Three days	One month
Ebay	21 May 2014	1.48%	7.35%
AOL	28 April 2014	1.70%	23.56%
Target	19 Dec. 2013	2.41%	5.79%
Adobe	3 Oct. 2013	2.91%	4.04%
KT Corporate	29 July 2013	1.30%	5.82%
Ubisoft	2 July 2013	2.48%	2.48%
Betfair Group	30 Sept. 2011	13.67%	13.67%
Heartland Payment Systems	20 Jan. 2009	46.30%	49.54%
TK/TJ Maxx	17 Jan. 2007	1.82%	6.49%

Source: Slaughter and May, Cyber security – corporate insights for companies and their directors, March 2015 Briefing

Experts' expectations on likely trends in cybercrime threats

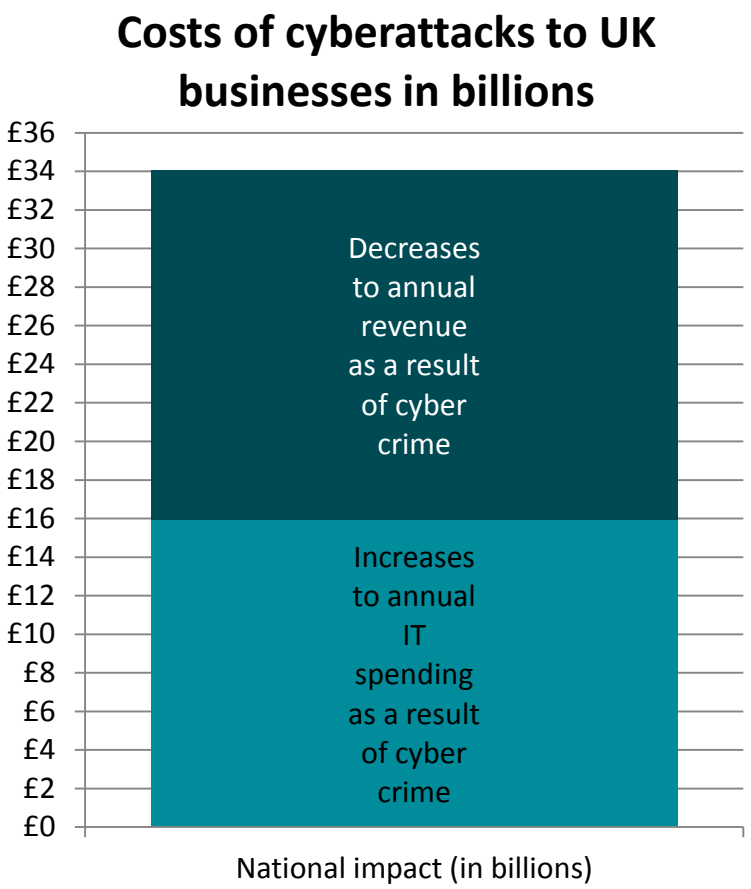
- The Royal United Service Institute (RUSI) Threat Assessment of Cybercrime to the UK predicts that the **attacks carried out in the future are likely to cause much more damage**. This does not necessarily mean that the frequency of attacks will increase, but that they are likely to be conducted in a more targeted manner by exploiting better intelligence.
- RUSI also indicates that the **cybercriminals will continue to operate on very sophisticated levels , adopting business like approaches** to drive profits, improve efficiencies, and increase their return on investments.
- According to the Verizon 2015 Data Breach Investigations Report*:* One prediction which might **make cybercrime an even more complex issue is that "internet of things" devices will increase to over 5 billion by the end of the decade**, according to Verizon experts.
- The **EU will remain a key target for cybercrime**. This is because of the increasingly **internet dependent economy and infrastructure**, the **high degree of internet penetration** amongst the population and the high levels of **wealth** that might be extracted through cybercrimes. A study in the International Journal of Cyber Criminology found that there seem to be **cybercrime hot spots with links to organized crime in Eastern European countries and the former Soviet Union**. Overall, there has been a shift from amateur individuals to sophisticated organised crime groups.

The cost of cybercrime to business and the economy

Cebr

Cyberattacks cost UK firms £34 billion in revenue losses and increased IT spend following a cyberattack[1]

- Overall **costs of cybercrime to UK businesses amounts to £34 billion** taking into account both lost revenues and increased IT spending following an attack.
- **15% of UK firms** questioned claimed they had a cybersecurity breach through which they **lost revenue.**
- **88% of UK firms** questioned claimed they had to **increase their annual IT spend** in order to react to cybersecurity breaches.
- The sectors that incur the highest losses and also need to invest the most into IT spending as a result of cybercrime are:
  - **Technology & telecoms** (including electronic and electrical equipment, software and computer services); and
  - **Financial services**

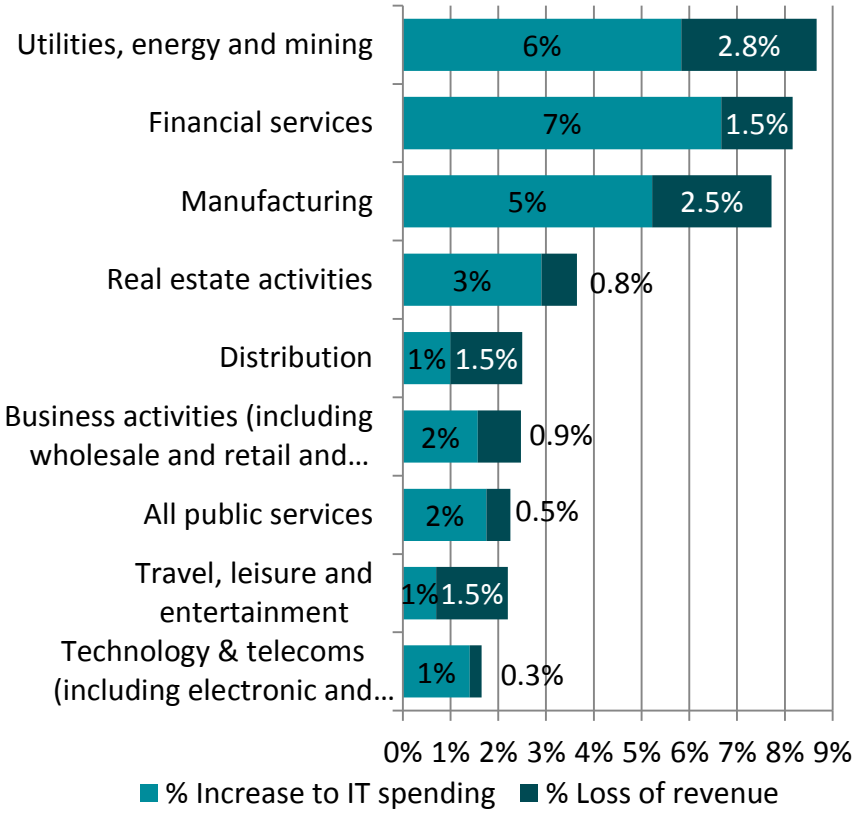


[1] These findings are based on a survey conducted by Opinium. These results differ to the 2014 Information Security Breaches Survey. This is down to several factors for example the sample size being larger (1,125 for the ISBS compared to 201 for the Opinium survey). In addition, respondents to the ISBS were drawn from more diverse job roles including IT professionals, business managers, executives, non-executive directors. The Opinium survey sampled C-suite executives only.

Cyberattacks cause firms in the UK to lose approximately £18 billion annually in revenue[2] and increase their annual IT spending by almost £16 billion[3]

- **Utilities, energy and mining** suffer the **largest declines in revenue following cyberattacks**, with the average loss of revenue being close to 3%.
- One needs to consider what revenues the firms in each industry are generating. For example **financial services firms are on average losing 1.5% of revenue due to a cybersecurity breach** (proportionately less than manufacturing), but given the revenues of a typical financial services firm, the losses are likely to be in the **range of several *billion* pounds**.
- Lost revenue is just one part of the story. **Firms also experience increased IT costs following a cyberattack.**
- **Financial service firms have the largest average increase (7%) in IT spending** as a result of a cybersecurity breach.
- Overall, **utilities and mining firms** are among the most affected by cyberattacks, not only having one of the **largest declines in revenue (3%)**, but also one of the **highest average increase in annual IT spending (by 6%)**.

Average % increase in IT spending / % loss of revenue following a cybersecurity breach



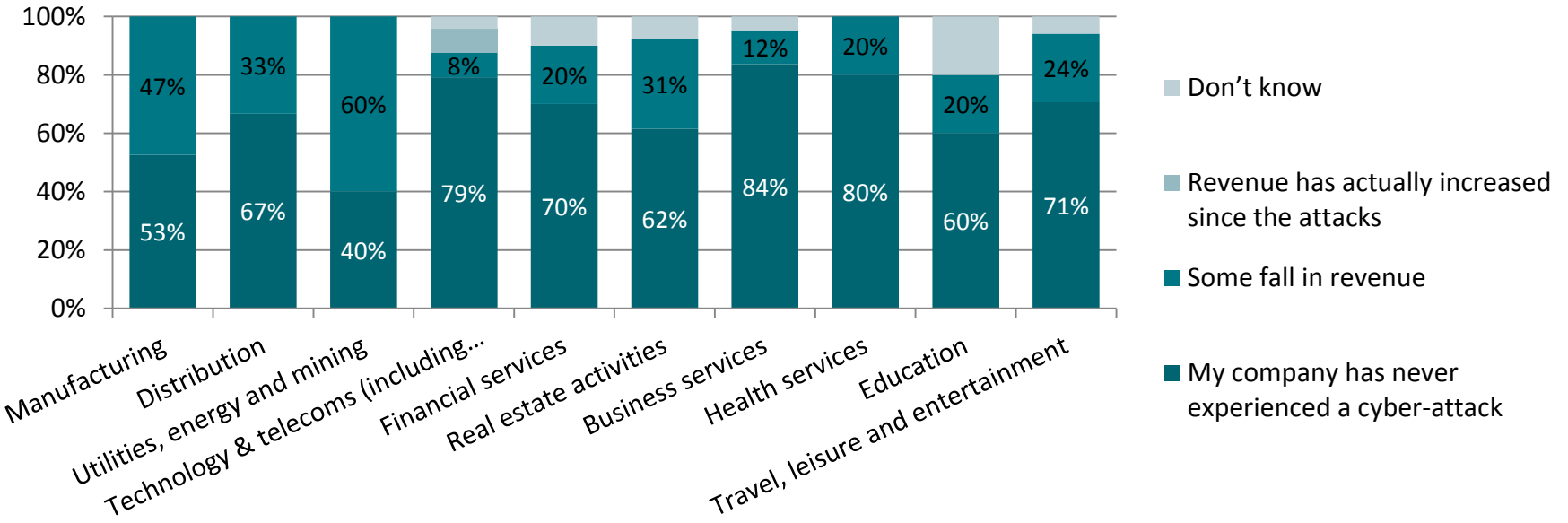
*[2] These findings only refer to the loss in revenue after a cyberattack across different sectors of the UK economy. Costs associated with prevention, education/training, or subsequent costs incurred from (e.g.) extortion using stolen data, were not considered in these calculations. Hence, the **total cost** of cybercrime to the economy is likely to be significantly higher.*

[3] This captures some spending on prevention, which gives a more complete picture of the total cost of cybercrime to the economy. As previously noted, this total cost is likely to be higher than revenue losses only.

15% of UK firms said they had a cybersecurity breach through which they lost revenue[4]

- **The utilities, energy and mining industry was most commonly affected** with 60% said there was some fall in revenue. On average firms in the industry reported a 3% fall of revenue following a cybersecurity breach.
- The **experiences of firms differ greatly depending on their industry**. Between 8% and 60% of firms, depending on industry, reported a cyberattack that lead to a decline in revenue.

Has the turnover of your business been affected as a result of any cyberattacks[1] ?

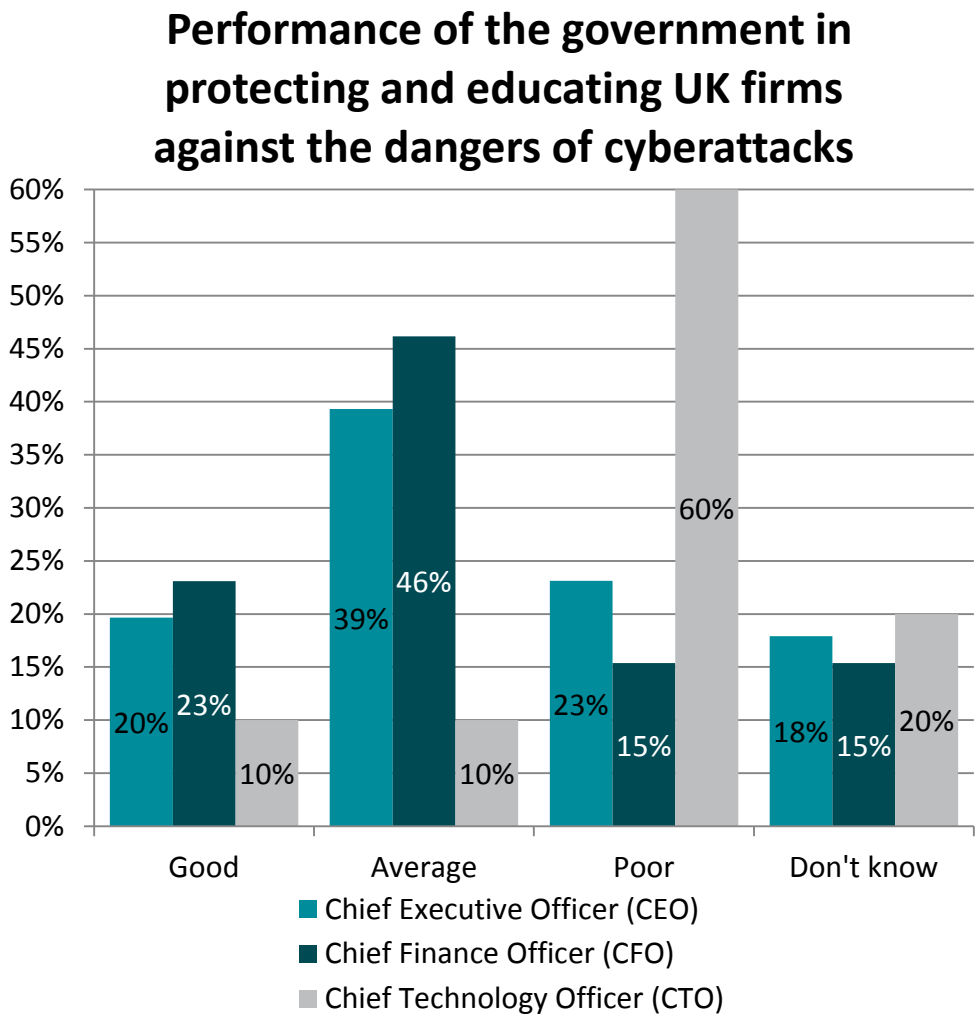


[4] These findings are based on a survey conducted by Opinium. These results differ to the 2014 Information Security Breaches Survey. This is down to several factors for example the sample size being larger (1,125 for the ISBS compared to 201 for the Opinium survey). In addition, respondents to the ISBS were drawn from more diverse job roles including IT professionals, business managers, executives, non-executive directors. The Opinium survey sampled C-suite executives only.

Attitudes towards cybersecurity

Cebr

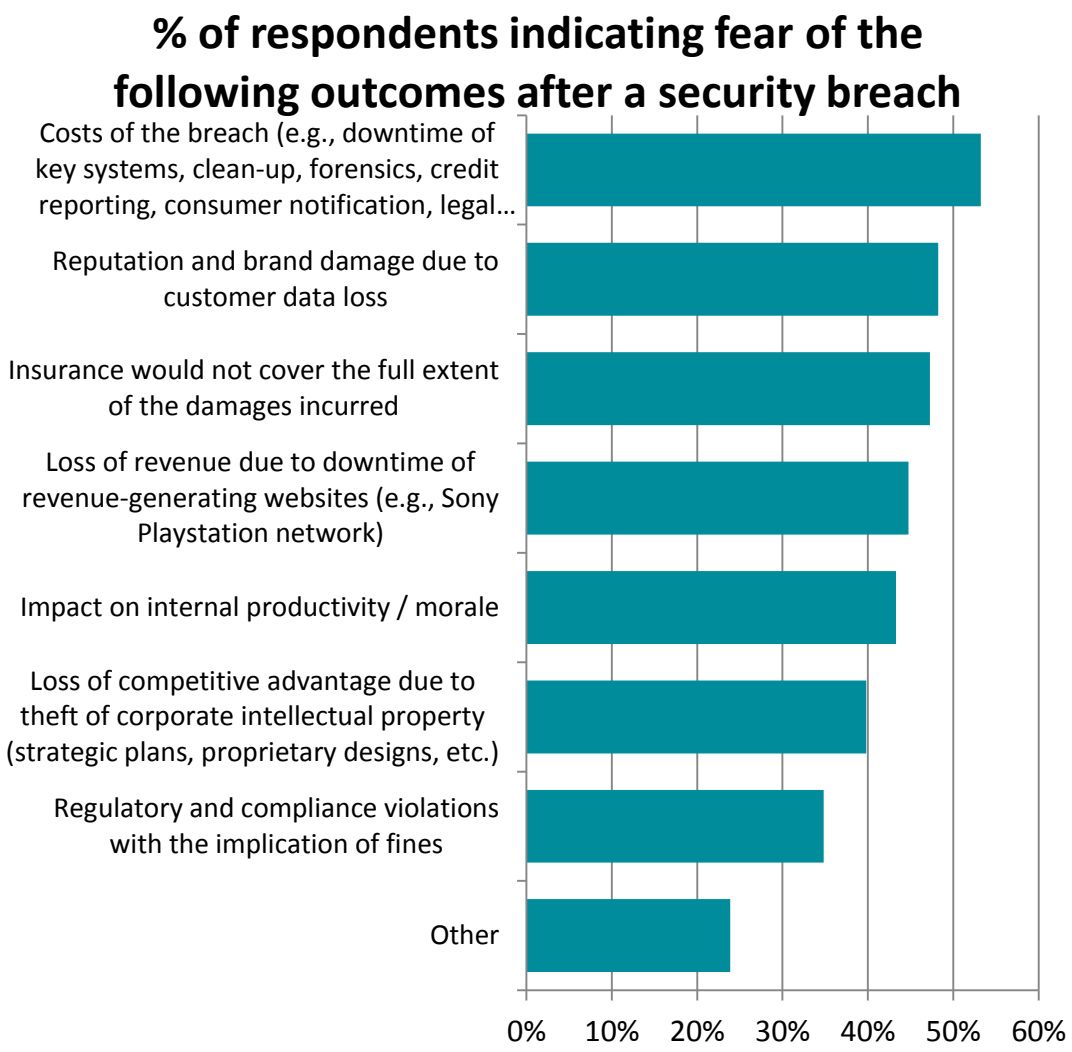
60% of CTOs believe the government not doing enough to prevent cyberattacks



- A majority of **CTOs (60%) believe that the government is performing poorly** in educating and protecting UK firms from cyberattacks.
- **CFOs are the most likely to be positive about the government's performance**, with 23% believing the government is doing a good job. In comparison, only 20% of CEOs and even fewer CTOs (10%) share the same belief.

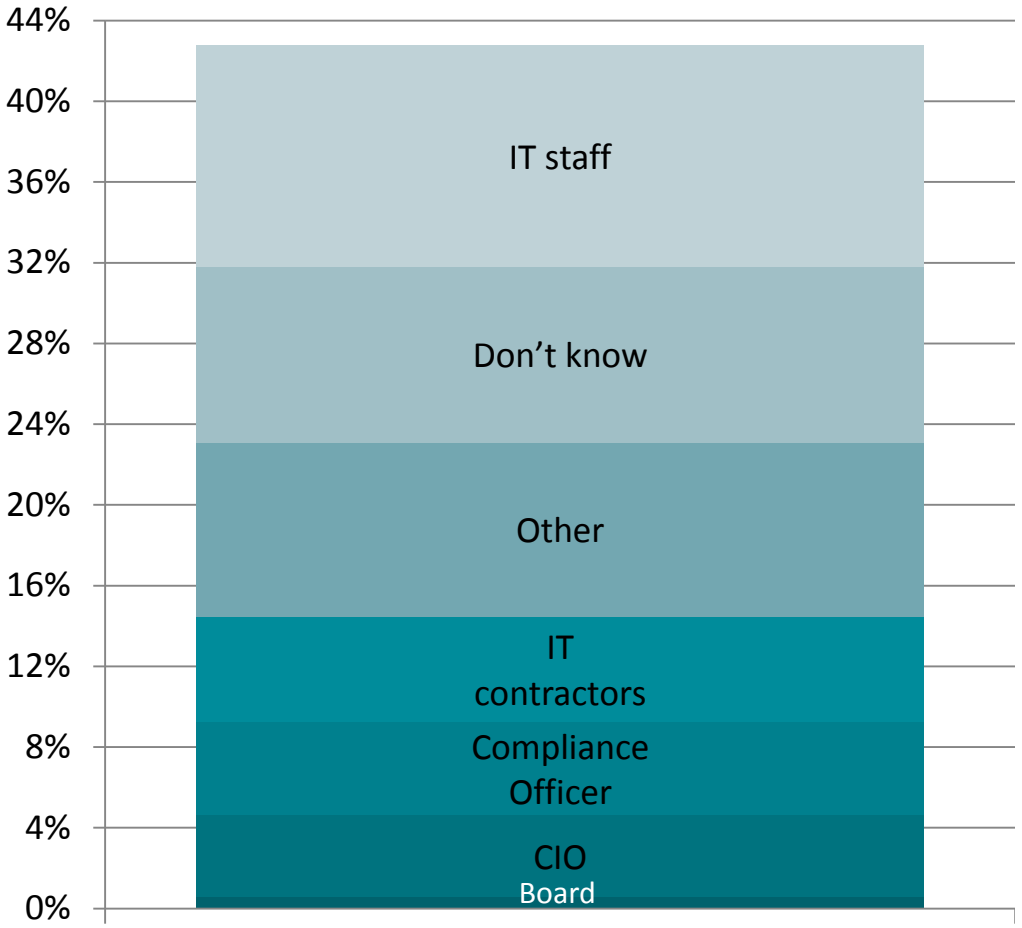
Top concerns: breach costs (forensics, clean-up, legal, etc.), reputation / brand damage, and lost revenue due to downtime

- **Reputational and brand damages** is a major concern to businesses.
- Firms are fearful of a **loss of revenue** due to downtime and the **negative impact on internal productivity**.
- Compared to other fears outlined by firms, they are **least worried about the implication of fines due to regulatory and compliance violations**.
- Although **loss of competitive advantage due to theft of IP** is not a primary fear overall, some industries are very concerned with this possibility: in the **education sector 60%** consider loss of competitive advantage as a source of concern**. In manufacturing 58%** fear loss of competitive advantage, and the eqivalent proportion in **distribution is 50%.**



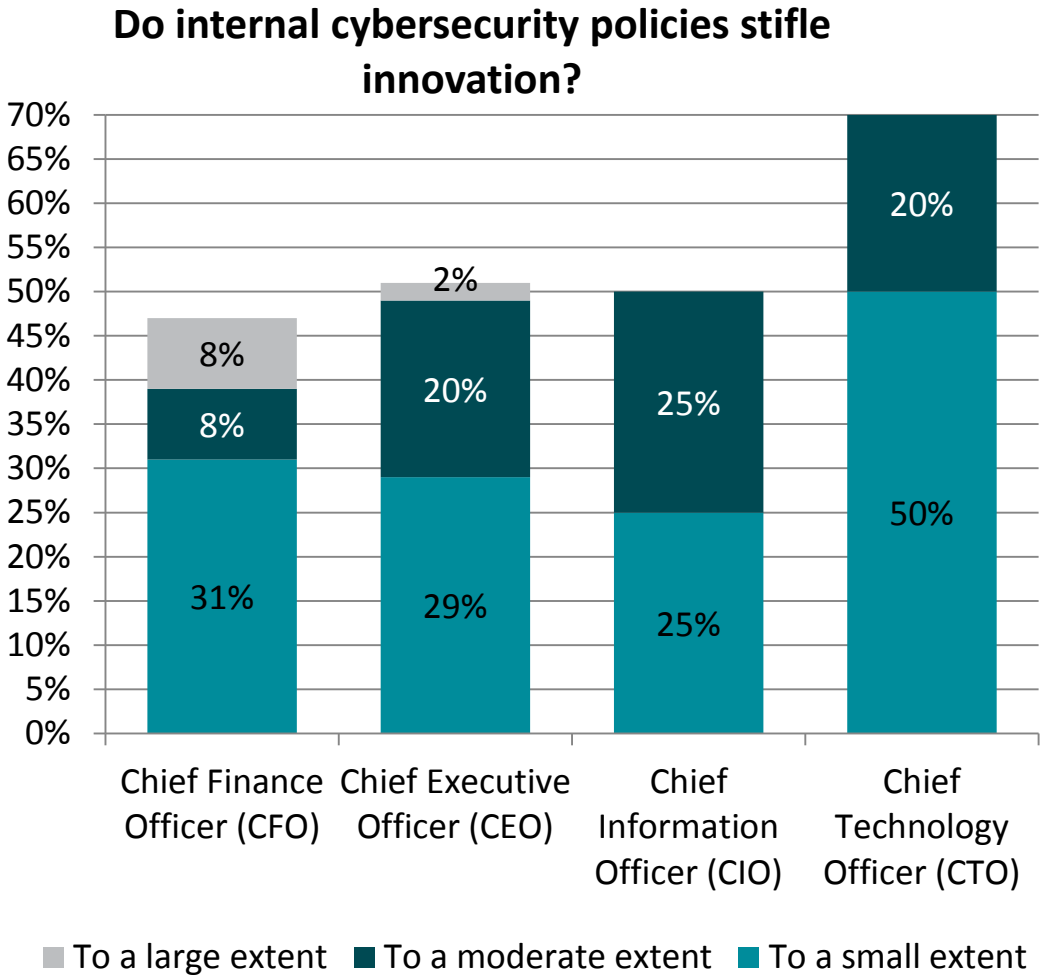
57% of CEOs hold themselves accountable for major cybersecurity breaches

- CEOs blame:
  - **57% of CEOs hold themselves accountable** for major cybersecurity breaches.
  - Some CEOs also hold **IT staff and IT contractors accountable** for major breaches in cybersecurity.
- CFOs blame:
  - CFOs mainly hold **IT contractors accountable**.
- However, there seems to be an **issue around accountability especially in large organizations**: there is no consesus among C-suite executives on who is to be held accountable.



Who do Chief Executive Officer (CEO) blame apart from themselves:

70% of all CTOs believe their current cybersecurity policies block innovation in some way

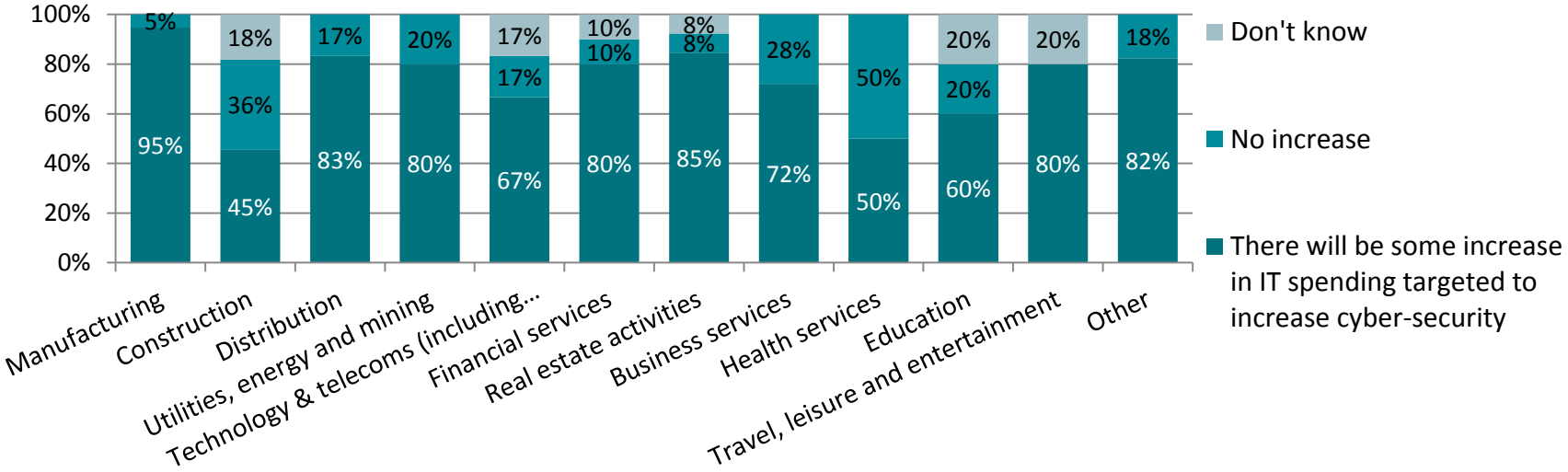


- The majority of CTOs (70%) surveyed believe that **internal security policies block innovation to *some* extent**.
- This indicates a need for more streamlined, automated risk processes to assess and manage risk.

71% of UK firms anticipate they will increase IT spending over the next 5 years to protect specifically against cyberattacks

- The **views** across industries regarding increased IT spending over the next 5 years to protect specifically against cyberattacks **varied largely**. Between 45% (in construction) and 95% (in manufacturing) of respondents expect an increase in IT spending to protect against cyberthreats.
- In the **utilities, energy and mining industry 60% of the firms** questioned claimed that they **expect to increase their IT spending by *6% or more*** to protect against breaches.
- **On average, firms in the utilities, energy and mining sector are anticipating the highest percentage increase in the IT budget (12%)**, followed by those in construction (4.5%), manufacturing (4%), travel, leisure and entertainment (3.8%) and real estate activities (3.6%).

Will IT spending be increased over the next 5 years to protect specifically against cyberattacks?



Concluding Remarks

- Cybersecurity is a global threat. All countries and all businesses are affected.
- **Cyberattacks are not isolated incidents, but events that have significant long-term implications and problems**. These include:
  - **Direct costs** for performing forensics, cleaning malware from affected servers, and implementing new protection controls such as monitoring and encryption.
  - **Loss of revenue** leading to a decline in valuation of the company.
  - **Decline in customer confidence and/or brand damage**, which are especially critical for online businesses.
  - **Exposure of weaknesses in a company's cybersecurity system, which can lead to further attacks** (some cyberattacks are "pilot" attacks which are specifically designed to identify weaknesses for the subsequent "real" attack).
- The **Internet of Things (IoT) could increase vulnerability to cyberattacks in the future**.
- Firms should prioritize cybersecurity more highly in their organizational strategies to avoid cybersecurity breaches and their long-term consequences.

Methodology

- A survey commissioned from Opinium provided insights into how C-suite executives view cybersecurity and how it has affected their revenues and costs. In addition, the survey asked about attitudes to the government's policy on cybersecurity. The total sample size was 201 C-suite executives. Fieldwork was undertaken between 23rd and 30th May 2015. The survey was carried out online.
- The survey, and data collected from the Annual Business Survey (ABS), allowed Cebr to estimate the number of businesses that were affected by cybercrime. Cebr also estimated the revenue lost due to cybercrime in the UK and the extent of the increase to IT spending in order to react to a cybersecurity breach.
- The percentage of respondents who selected they "don't know" the extent of the decreases to annual revenue / increases to IT spending, were distributed equally across the different "revenue decreasing"/ "IT spending increasing" options. For example, if 5% of respondents claimed they did not know the extent of revenue decreases, these responses would be distributed equally across the other options presented. This method is considered appropriate because respondents were presented with discrete options to indicate no revenue losses, or no experience of cyberbreaches.

Contact

For enquiries on this research please contact:

Oliver Hogan, Director

+44 (0) 20 7324 2842, ohogan@cebr.com

Julia Heilig, Senior Economist

+44 (0) 20 7324 2881, jheilig@cebr.com

Unit 1 4 Bath Street London EC1V 9DX
T 020 7324 2850 **E** pressoffice@cebr.com **W** www.cebr.com