# The value of cyber insurance to the UK economy

Prepared for
the Association of British Insurers

November 2020

www.oxera.com

oxera
compelling economics

# Contents

# 1 Foreword

We live in a rapidly changing society in which the way we work and carry out our lives is becoming ever more dependent on digital infrastructure. This digital transformation has brought great strides in efficiency to the workplace and opened the way for countless new jobs and investment opportunities, bridging what once seemed vast oceans between nations and continents in my adult lifetime. In 2020, with the onset of COVID-19, and the world beset by a global pandemic, we have seen decades of change in corporate practices and business structures evolving in a matter of weeks, all utilising the technology available to the full and pushing capabilities further than they have previously gone.

Huw Evans, Director General of the ABI

With increasing dependence on digital infrastructure comes increased risk. Our society, economy and lives have never been more reliant on the security and resilience of the computer systems on which our world now depends. Over the coming years, cyber threats will continue to plague businesses of all sizes and new threats will emerge, with the risk of a data breach or ransomware attack increasing and the impact of those attacks becoming ever more devastating.

It is in this context that the role of insurance can be seen more clearly as a key facilitator in the promotion of the increased cyber resilience of businesses and individuals, and in providing the financial support needed to get affected businesses back on their feet. This report seeks to provide insight into this fast-developing and growing insurance market, to set out the risks and challenges posed by increased digitisation, and to look to the future and the opportunities yet to be explored. What is clear is that the need to manage cyber risk is becoming ever more important for businesses of all sizes, and that cyber insurance will form a key part in the cyber resilience of business in the future.

# 2 Introduction

The Association of British Insurers ('ABI') has commissioned Oxera to assess the impact of cyber insurance on the UK economy.

In today's world, firms across all sectors of the economy rely on some level of digital infrastructure for their everyday operations. The abrupt transition to more remote forms of working and the digitisation of the economy more generally brought about by the COVID-19 pandemic has reinforced this trend. From small start-ups to global giants, businesses are increasingly dependent on networked devices in one form or another. While this presents businesses with huge benefits and opportunities, the increasing reliance on technology also increases the potential harm posed by cyber risks.[1]

Cyber risks encompass a multitude of sources of risk affecting the information and technology assets of a firm, governments or individuals. They come in a wide range of forms that change over time, including data breaches due to human error, the disclosure of sensitive information, identity theft, and highly sophisticated installation of ransomware and business interruption. These risks can have long-lasting and far-reaching consequences. As they grow, so too does the demand for protection against them.

Cyber insurance is one vital component of any strategy aimed at mitigating risks and improving cyber security. In addition to paying out in the event of a cyber incident, insurance makes an important contribution to the management of cyber risks by promoting awareness about exposure to cyber losses, sharing expertise on risk management, encouraging investment in risk reduction and offering support in responding to cyber incidents.[2] Cyber insurance has grown significantly in recent years, and it continues to adapt to the evolving nature of cyber risks. Further development is expected, at least in part due to the recent introduction of the EU's General Data Protection Regulation (GDPR).

This report considers the benefits and importance of cyber insurance policies for UK businesses and the UK economy more broadly. The focus of the report is on **stand-alone cyber insurance**, rather than cyber insurance that might be an implicit part of other coverage.

The analysis presented in this report complements existing research from the Department for Digital, Culture, Media & Sport, the OECD, and EIOPA, among others, with new insights from UK cyber risk insurers and insurance brokers. References are provided throughout. Insights from these existing research pieces are cited in this report. Also, as part of our research, Oxera collected data and conducted interviews with six UK cyber risk insurers, insurance brokers and representatives from Lloyd's syndicates. Where reference is made to UK cyber market stakeholders these are the insights being referred to.

The report is structured as follows.

- Section 3 provides an overview of cyber risks and the need for insurance, drawing on the history of insurance and the emergence of cyber threats.
- Section 4 describes the growth and trends in the cyber insurance market in the UK.
- Section 5 assesses the direct benefits of cyber insurance for UK businesses.
- Section 6 assesses the indirect benefits of cyber insurance to the wider UK economy.

# 3 Cyber risks and the need for insurance

## 3.1 A history of insurance

Throughout history, individuals, businesses and nations have looked for ways to spread and mitigate risks. The formal concept of insurance, and the practice of underwriting, emerged in the UK in the 1500s in the marine industry, where the risk of losing whole shipments was of serious concern.[3] In the UK, the Great Fire of London in 1666 changed public opinion as to the merits and necessity of insurance.[4] Although the insurance industry has developed greatly over time, its underlying purpose has not changed.

### The purpose of insurance

Insurance provides protection against events that are potentially difficult to predict at an individual level, but that can be estimated at a group level. All forms of insurance contain a risk-pooling element and a risk-transfer element. These allow insurance to transfer risk from individuals and businesses to third parties that can combine and 'pool' various risk exposures together.[5]

While the concept of insurance and its function of risk mitigation have remained the same over time, policies have had to adapt to stay relevant and accommodate the changing nature of risks. This includes insurance firms providing services throughout an insurance contract, beyond solely paying out for claims as was traditionally the case. As a result of this evolution, several new

[1] 'Cyber risks' are defined as any risk emerging from the use of information and communication technology that compromises the confidentiality, integrity or availability of data, systems or services.
[2] OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
[3] Swiss Re (2017), 'A History of UK insurance', p. 5.
[4] Ibid.
[5] Baranoff, E., Brockett, P. E. and Kahane, Y. (2009), *Risk management for enterprises and individuals*, Flat World Knowledge, ch. 6.

forms of insurance have emerged—cyber insurance being one of them. Cyber risks have developed and gained increasing attention over the last 10−20 years in light of our increasing reliance on technology and connectivity.

Cyber insurance caters for a spectrum of risks. At one end, there are higher-frequency, 'daily life'-type risks, such as data fraud, theft or other privacy breaches. At the other end, there are 'extreme scenario'-type risks, such as NotPetya and Wannacry, which can result in severe disruption to many businesses. These high-profile examples are summarised in Box 2.1 below. Cyber insurance can help to mitigate these risks.

## 3.2 Characteristics of a cyber-attack

There are various forms of cyber-attack, reflecting the evolving nature of cyber risks. Most attacks are basic, with attackers indiscriminately targeting as many systems as possible, exploiting any potential vulnerabilities.[6] The random nature of attacks means that whoever is unlucky enough, and without adequate defences, will be hit. In 2018, 32% of businesses reported having some kind of cyber security breach or attack.[7] The UK cyber insurance market stakeholders that spoke to Oxera reported that the incidence of a less common form of attack has been increasing in recent years—namely more sophisticated attacks that are targeted at specific companies and might be based on ideology, pride or national interests.

**In 2018, 32% of UK businesses reported having some kind of cyber security breach or attack.**

There are various 'types' of attackers, which can be grouped into: (i) criminal, (ii) pranksters, and (iii) state-sponsored.

While the techniques and methods used are similar, the impacts of the different forms of attack are usually very different, ranging from negligible losses if the attack is unsuccessful in penetrating a system (low-risk, high-frequency attacks) to severe damage and potentially a firm going out of business (high-risk, low-frequency attacks).

The case studies in the Box 4.1 demonstrates the devastating and far-reaching effects that an extreme cyber-attack can have.

**Box 3.1 Two extreme high-risk, low-frequency cyber-attacks**

**NotPetya[8]**

In June 2017, companies across the globe reported that they had been struck by a major ransomware cyber-attack—the NotPetya attack.

The NotPetya attack is estimated to have had an economic cost of $10bn.

In the NotPetya attack, the virus froze the user's computer and demanded a ransom to be paid.

Businesses with strong trade links with Ukraine, such as the UK's Reckitt Benckiser, Dutch delivery firm TNT, and Danish shipping giant Maersk were affected.

As a result of the attack, Maersk reinstalled over 4,000 servers, 45,000 PCs, and 2,500 applications over a ten-day period. This was estimated to cost Maersk up to $300m.

**WannaCry[9]**

In May 2017, there was a worldwide attack by the WannaCry ransomware crypto-worm, which is estimated to have hit over 230,000 computers across at least 150 countries. The attack used a specific Microsoft Windows vulnerability to encrypt data and demand ransom payments. Among the range of sectors and industries hit, one of the largest agencies to suffer was the NHS, which was still largely reliant on outdated software and operating systems, making it vulnerable to attack. The effects of the attack included:

- 80 out of 236 hospital trusts across England being affected;
- 19,000 appointments being cancelled;
- around 1% of all NHS care disrupted over the course of a week;
- a cost to the NHS of approximately £92m, although this is likely to be an underestimate as no data was collected on the costs of recovering IT systems or the extent of patient disruption.

The increasing interconnectedness of systems means that a breach at one business can have repercussions for the supply chain. This contagion effect can lead to the suppliers, customers and strategic partners of a targeted business being as vulnerable to an attack as the

[6] National Cyber Security Centre (2016), 'Common cyber attacks: reducing the impact', January.
[7] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July, p. 2.
[8] CyRiM Report (2019), 'Bashe attack: Global infection by contagious malware'.
[9] Department of Health & Social Care (2018), 'Lessons learned review of the WannaCry Ransomware Cyber Attack', February.

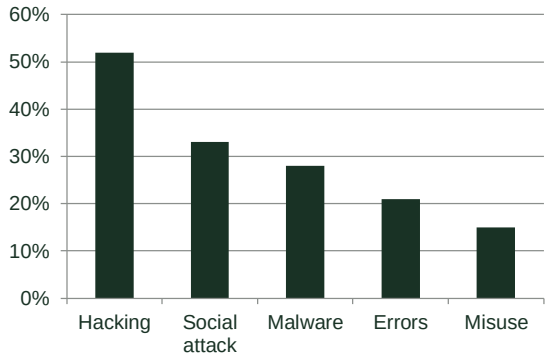
primary target itself. Similarly, if a hacker has managed to break through one firm's cyber security, it may be that other firms have similar vulnerabilities that the hacker can take advantage of. This was seen with the WannaCry attack hitting a number of large private companies, from US-based delivery company FedEx, to Spanish telecommunications firm Telefonica and German railway operator Deutsche Bahn.[10]

Furthermore, in contrast to traditional types of risk such as fire, cyber risks may be transferred between companies in very different locations. The international nature of the internet means that a breach in Tokyo could have repercussions in Chicago and London, as well as for other companies located near the firm that is the primary target.

UK cyber insurance market stakeholders have also observed that while the main targets of cyber-attacks were historically large businesses, this is changing. This trend may reflect shifts in the types of cyber-criminal, as well as a change in the tactics and objectives of cyber-criminals. For example, the WannaCry attacks demonstrated that SMEs, as well as large businesses, were vulnerable to attack.[11] Further, criminals seeking ransom and who are less interested in causing widespread disruption and concern may find that higher-frequency but lower-profile attacks are more effective. The ever-evolving nature of cyber risks, and the potentially significant cost of an attack to a business, is making it increasingly difficult for companies to self-insure against cyber risks.

In addition to external deliberate attacks, cyber risks include accidental errors, internal deliberate actions (such as employees manipulating data), and IT system failures. Figure 3.1 provides an overview of the main tactics used in cyber breaches. While hacking is the main tactic, it shows that errors (21%) and misuse contribute to cyber breaches.[12] Phishing attacks are involved in 32% of breaches.[13]

**Figure 3.1 Sources of cyber risk**




Source: Verizon (2019), '2019 data breach investigations report'.

### Implications for cyber insurance

The variety of cyber risks, the potential for international contagion and the evolving types of attacks make understanding cyber risks complex, and pricing cyber insurance appropriately requires particular expertise. As a major exporter of cyber insurance, the UK insurance industry is proving to have a competitive advantage in this respect.[14]

As reported in section 4.4, as the understanding of the sources of cyber risks improve, UK cyber insurers are adapting and improving their risk mitigation and containment processes (alongside UK cyber security firms). By sharing these techniques with businesses, UK cyber insurers can help to reduce the risks posed by cyber incidents.

The complexity of cyber risks also means that reinsurance can play an important role in expanding the supply of cyber insurance. We discuss this further in section 4.5.

## 3.3 The cost of an attack

Cyber-attacks represent a huge cost to the global economy, with estimates ranging from tens of billions to a trillion dollars or more.[15] In particular, the Centre for Strategic and International Studies and McAfee estimated that cybercrime cost the world almost $600bn in 2018,[16] equivalent to

[10] *The Telegraph* (2017), 'NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history'.
[11] NIG (2017), 'WannaCry attack offers wake-up call to SMEs'.

[12] Hacking refers to the involuntarily extraction of sensitive information, where a perpetrator takes over a computer system—for example, through the use of stolen credentials. Social attacks are malicious activities accomplished through human interactions. They use psychological manipulation to trick users into making security mistakes or giving away sensitive information—e.g. phishing. A malware attack is when cybercriminals create malicious software that's installed on someone else's device without their knowledge. Errors are to incidents in which unintentional actions directly compromise a security attribute of an asset. Examples include sending data to the incorrect recipient. Misuse captures any unapproved or malicious use of organisational resources.

[13] Verizon (2019), '2019 data breach investigations report'.
[14] In 2017, 25% of global GWP being written through Lloyd's syndicates. Source: EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[15] CSIS (2018), 'Economic Impact of Cybercrime − No Slowing Down', February, p. 6.
[16] Lewis, J. A. (2018), 'Economic Impact of Cybercrime: At $600 Billion and Counting − No Slowing Down', Centre for Strategic & International Studies, 21 February.

0.7% of global GDP or 14% of the value of the worldwide internet economy.[17]

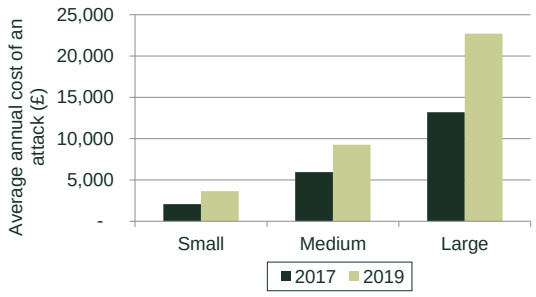
**Globally, cybercrime cost $600bn—c. 14% of the internet economy.**

Given that indirect costs, long-term costs, opportunity costs and intangible costs of breaches (such as lost productivity and reputational damage) tend not to be included in such estimates, the true cost of cyber security breaches is likely to be higher.Given that indirect costs, long-term costs, opportunity costs and intangible costs of breaches (such as lost productivity and reputational damage) tend not to be included in such estimates, the true cost of cyber security breaches is likely to be higher.

Figure 3.2 shows the substantial and increasing costs of cyber-attacks for UK firms, drawing on the UK government's 'Cyber Security Breaches Survey 2019'.[18]

For all UK businesses, the average annual cost as reported in this survey grew by more than 50% in just two years, reaching £3.6k for small businesses, £9.3k for medium businesses and £22.7k for large businesses in 2019.[19] Given that indirect costs, long-term costs, opportunity costs and intangible costs of breaches (such as lost productivity and reputational damage) tend not to be included in such estimates, the true cost of cyber security breaches is likely to be higher.[20]

**Figure 3.2 Average cost of a cyber-attack**

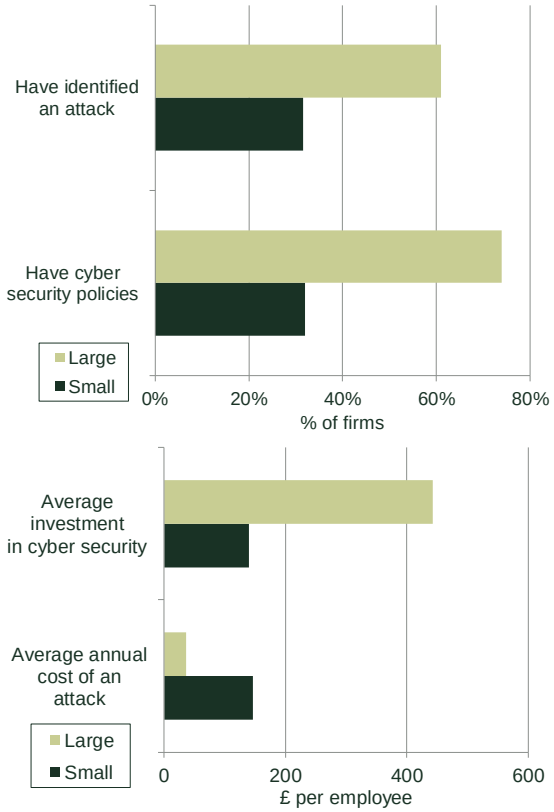



Source: Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July; (2017), 'Cyber Security Breaches Survey 2017', April.

**In 2019, cybercrime costs reached £23k for large UK businesses.**

Figure 3.3 shows that although large businesses suffer more attacks (60% compared to 32%) and incur higher losses in absolute terms, the financial impact of an attack is disproportionately high for small firms. The average annual cost of an attack per employee is more than four times larger for small firms, amounting to £146 for small firms compared with £36 for larger businesses.

**Figure 3.3 Comparison between small and large UK businesses in the UK, 2019**




Note: The value per employee has been estimated using the mid-point of the number of employees for each firm size. Cyber security policies include, among others, what staff are permitted to do on an organisation's IT devices and document management systems, what can be stored on removable devices, use of new digital technologies, remote or mobile working, use of personally-owned devices for business activities, and data classification.

Source: Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019'.

Figure 2.3 also shows a marked disparity in spending patterns and investment in cyber security, with 71% of larger businesses having cyber security policies in place, and investing £443 per employee in protection, compared to 32% of small businesses, meaning that, on average, an investment of only £140 per employee.

[17] Based on global GDP of $84.93tn in 2018 (IMF DataMapper, 'GDP, current prices', accessed 9 December 2019) and the value of the worldwide internet economy of $4.2tn in 2016 (source: BCG (2012), 'The Internet Economy in the G-20', March).
[18] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.
[19] Small firms are defined as firms with fewer than 50 employees, and large firms are defined as firms with more than 250 employees. Source: European Commission (2003), 'Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)'.
[20] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July, p. 3.

**Larger businesses are more likely to take precautions**

- **71% of large businesses have security policies in place, compared to**
- **32% for small businesses**

This disparity suggests that a substantial proportion of smaller firms may be struggling to keep up with larger firms when it comes to addressing cyber threats and taking measures to enhance security. As the threat of a cyber-attack grows and small firms become increasingly vulnerable, we may see this gap closing.

# 4 Cyber insurance: a growing market

## 4.1 Introduction

One of the important solutions to the increasing threats from cyber risks is cyber insurance.

The cyber insurance market continues to grow as companies become increasingly aware of cyber risks. To date, US companies have accounted for the majority of cyber insurance, in part reflecting the larger size of the US economy.[21,22] However, in recent years cyber insurance has become increasingly popular in the UK, with year-on-year growth of between 25% and 50% reported for the UK cyber insurers that participated in this study. We explore the key drivers and trends that have resulted in this growth in this section.

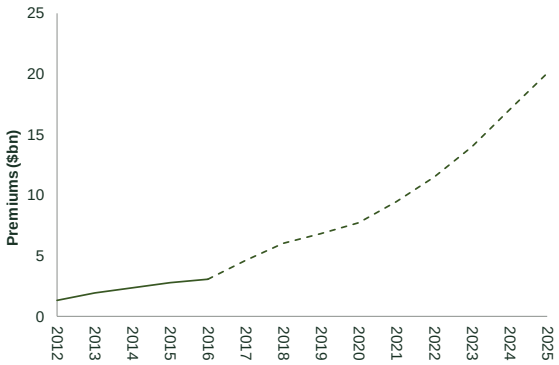
## 4.2 The global market; the UK market

### Global trends

Although generally believed to be a completely new market, cyber insurance products have been around since the late 1990s.[23] Cyber insurance started as a predominantly US product, born partly in response to the introduction of data breach notification laws. Legislation started in California where the Mandatory Data Breach Disclosure Law was first signed in 2002, and effective from 2003, making firms legally obliged to notify affected parties in the event of a data breach.[24] Similar legislation was subsequently introduced in other states between 2005 and 2016. As such, the products were initially developed as an add-on cover or bundled into existing policies for technology, media and telecom (TMT) firms and professional services firms, which required coverage to protect themselves against the inadvertent transfer of malware and loss of confidential client information.

The products have since developed, as has their function, reflecting the evolving nature of cyber risks—today they go further than simply offering a risk-transfer solution, and demand is rising from all sectors of the economy.[25,26] The global market for cyber insurance has grown markedly in recent years, with annual growth rates of 20−25%,[27] and this growth rate is expected to accelerate going forward, as shown in Figure 4.1.

**Figure 4.1 Value of cyber insurance premiums written worldwide ($bn)**




Note: OECD based on data from Advisen, PwC, Betterley, Marsh, Thomas and Finkle, Insurance Information Institute, Allianz, ABI and Swiss Re.

Source: OECD (2017), 'Enhancing the role of insurance in cyber risk management'.

Figure 4.1 shows the growth of the cyber insurance market. Historically, this growth has mostly been driven by growth in the US, which is currently the most developed marketplace for specific cyber insurance products and accounts for 90% of the global stand-alone cyber premium market.[28] This is in part a reflection of the size of the US economy, which accounted for 24% of global gross domestic product in 2018,[29] but is also a difference in penetration, with 15% of US companies having purchased cyber insurance.[30]

A key reason for the different maturities of the US and European cyber insurance markets has been the earlier adoption of regulation in the USA. In comparison to the introduction of mandatory data breach disclosure laws in the US starting in 2002, the EU equivalent, the General Data Protection

[21] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[22] In 2018, the USA accounted for 15% of global GDP. Source: Statista (2019), 'United States' share of global gross domestic product (GDP) adjusted for purchasing power parity (PPP) from 2014 to 2024'.
[23] Aon (2017), 'Global Cyber Market Overview: Uncovering the Hidden Opportunities', June.
[24] Aon (2017), 'Global Cyber Market Overview: Uncovering the Hidden Opportunities', June.
[25] Insight from Oxera interview with insurance stakeholder.
[26] OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
[27] KPMG (2018), 'Cyber Insurance − How insuretechs can unlock the opportunity', p. 3.
[28] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[29] Based on 2018 GDP figures of $20.58tn for the US and $84.93tn for world GDP (source: IMF DataMapper, 'GDP, current prices', accessed 9 December 2019.
[30] Aburish, N., Fixler, A. and Hsieh, M. (2019), 'The Role of Cyber Insurance in Securing the Private Sector', 13 September.

Regulation (GDPR), was only announced in 2012 and introduced in May 2018.

Although cyber awareness, and demand for cyber insurance, began to rise in the EU with the announcement of GDPR in 2012, it remains low. The UK cyber insurance stakeholders that participated in this study expect that the introduction of GDPR, combined with the series of other trends set out in section 4.3, will stimulate further growth in cyber insurance in the UK, and that the gap between cover in the US and cover in the UK will begin to close. Consistent with these trends, other research suggests that the global cyber insurance market might reach $23bn by 2025.[31]

### The UK market

Cyber insurance in the UK comprises two key elements:

- cyber insurance written in the UK for UK businesses;
- cyber insurance written in the UK for non-UK businesses.

Estimates for the former—the share of global cyber insurance cover provided for UK businesses—range from c. 5% to 10%.[32] In comparison, the UK is a far more important contributor in terms of exports, with exports from Lloyd's syndicates accounting for approximately 25% of global gross written premium in 2017.[33]

**Not discounting the importance of cyber insurance exports for the UK economy, the remainder of this section focuses on the impact of cyber insurance for UK businesses.**

### Penetration of cyber insurance among UK businesses

Estimates for the cyber insurance market in the UK vary. Penetration rates, defined as the proportion of businesses with cyber insurance, in the UK range considerably, from ~2−20% to 40%.[34] Given that most estimates are based on surveys, differences in the business communities surveyed and in the wording of questions could account for part of this disparity,[35] as could whether the survey was capturing affirmative (stand-alone) cyber insurance only, or non-affirmative (implicit) cover as well.

Non-affirmative cover—e.g. cyber insurance coverage provided as an implicit part of a more general business interruption policy—is on the decline. This trend reflects the importance to both insurers and businesses of understanding what risks are being covered. Nonetheless, where non-affirmative cover remains, it can still provide a useful further back-stop for businesses without affirmative cyber cover.

## 4.3 Drivers of insurance for UK businesses

According to the stakeholders that participated in this study, there are three main factors that have driven the uptake of cyber insurance in the UK: the growth in cyber risk, the introduction of GDPR, and the growing awareness around cyber events. The importance of these three factors has been identified in other cyber insurance surveys and studies as well, as explained below.

### Growing risks

Cyber-attacks are increasingly threatening all business types, with firms being at risk if they:

- hold customer or employee data such as names, addresses, bank details or passport copies;
- use a computer to operate;
- have a website;
- take payment via card;
- store data in the cloud or rely on cloud-based services;
- make electronic payments.

This wide range of activities means that most, if not all, businesses are susceptible to some extent. For example, businesses are increasingly storing and processing vast amounts of personal and financial data (such as retailers and financial institutions). It is estimated that 32% of businesses experienced any kind of cyber security breach or attack in 2018.[36]

Increasing digitisation, accelerated by the COVID-19 pandemic, will further accelerate this trend, with the UK National Fraud & Cyber

[31] Adroit Market Research (2018), 'Global Cyber Security Insurance Market Size 2018 by Organization Size (SME, Mid-Market and Large Enterprises), by Industry (BFSI, ICT, Healthcare, Manufacturing, Retail and Others), Region and Forecast 2018 to 2025', 19 December.
[32] For example, Marsh and HM Government (2015), 'UK cyber security: the role of insurance in managing and mitigating the risk', March. The report estimated the UK's share of global cyber insurance to amount to 10% of global cover in 2014, whereas EIOPA (2018) estimated the EU in aggregate to amount to between 5−9% of global insurance cover in 2016.
[33] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[34] OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
[35] For example, the questions 'does your company have specific stand-alone cyber insurance?' and 'does your company have insurance for cyber risks?' could both be used to estimate cyber insurance penetration levels, but could result in different responses.
[36] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July, p. 2.

Security Centre reporting significant increases in cyber-attacks in 2020.[37]

Furthermore, the number of people developing software, the data consumed, the amount of code, and the number of malicious software products all continue to increase.[38] This means that the number of cyber-attacks is also likely to increase. The fact that companies are becoming more reliant on interconnectivity of systems and technologies, as well as cloud computing, increases the likelihood of a cyber-attack.

The growing threat of cyber-attacks is recognised by the UK government and is reflected in the government's 'cyber essentials' initiative, which aims to help organisations protect themselves against the most common cyber-attacks.[39] Insight from stakeholder interviews suggest that this is sometimes considered as a basic standard for businesses to meet in order to receive insurance. For example, one respondent with a primary focus on the SME market noted that businesses that undertook activities to align themselves with the cyber essentials programme (although not necessarily getting accredited) were placed in good stead to be eligible for insurance.

## GDPR

Participants to this study report that the announcement of GDPR in 2012 and its implementation in May 2018 has contributed to the uptake of cyber insurance in the UK. The cyber insurance stakeholders consider GDPR to have increased awareness of the risk and associated costs of data breaches.

This is consistent with the findings of the Cyber Breaches Survey, which found that 30% of businesses say they have made changes to their cyber security policies or processes as a result of GDPR.[40] However, this change has predominantly come from large (62%) and medium (51%) firms. Compared to just 18% of all micro and small firms surveyed saying they had made changes to their own policy following GDPR.[41]

As GDPR results in a higher number of breaches being publicised, interest in cyber management and coverage is expected to continue to increase, and this is likely to stimulate further demand for cyber insurance in the UK. For example, the OECD report that EU coverage of cyber insurance could double between 2016 and 2020, driven largely by the implementation of GDPR.[42]

## Growing awareness

Stakeholders report that an increasing level of awareness of the risks associated with cyber-attacks has been a key driver in the uptake of insurance. For example, some businesses have purchased cyber insurance because one of their peers has experienced a loss and this has brought to their attention the potential threat to their own business. Other companies have also purchased insurance after experiencing losses themselves, for example, insurers reported this as a common trend following the NotPetya attacks.

While in 2018 GDPR was the main driver for the purchase of cyber insurance, research from 2019 finds that this has now been replaced by media reports of cyber-attack, which also serves to raise awareness of the risks.[43]

UK cyber insurance stakeholders also report that the widespread coverage of privacy breaches and ransomware attacks, and their associated costs, have helped to drive the surge in cyber insurance. An example of this is illustrated in Box 4.1.

**Box 4.1 British Airways faces a proposed £183m fine for data breach**

A cyber breach at British Airways in September 2018 resulted in customer information being compromised, including log-in, payment card, and travel booking details, as well as names and addresses.

This incident involved user traffic to the British Airways website being diverted to a fraudulent site, allowing hackers to harvest customer details.

The proposed penalty is the largest fine issued by the ICO to date and was the first to be made public since GDPR was introduced. Up to that point, the biggest penalty was £500,000 imposed on Facebook, which was the maximum allowed under the old data protection rules that applied before GDPR.

BA's penalty amounts to 1.5% of its worldwide turnover in 2017, less than the possible maximum of 4% of turnover.

UK Information Commissioner Elizabeth Denham said:

> People's personal data is just that—personal. When an organisation fails to

[37] NCSC (2020), 'Advisory: COVID-19 exploited by malicious cyber actors', 8 April.
[38] Lewis, J. A. (2018), 'Economic Impact of Cybercrime: At $600 Billion and Counting − No Slowing Down', Centre for Strategic & International Studies, 21 February.
[39] National Cyber Security Centre (2019), 'Cyber Essentials: About', accessed 9 December 2019.
[40] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.
[41] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.
[42] OECD (2017), 'Supporting an effective cyber insurance market', May, p. 5.
[43] Baccus, M. (2019), 'Cyber Research 2019: The findings', *Insurance Post*, 29 May.

> protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear—when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.

Source: BBC News (2019), 'British Airways faces record £183m fine for data breach', 8 July; ICO (2019), 'Intention to fine British Airways £183.39m under GDPR for data breach', 8 July.

The aforementioned WannaCry attack drew a lot of media coverage, serving to further increase the awareness of cyber risks among businesses.[44]

## 4.4 Trends in cyber insurance for UK businesses

This section provides an overview of the key trends observed in the cyber insurance market for businesses in the UK, as reported in our interviews with UK cyber risk insurance stakeholders, and within the cyber surveys conducted by public bodies such as the OECD and the Department for Digital, Culture, Media & Sport.

These trends are grouped as follows:

- changes in the type of policy coverage that businesses are able to insure themselves against;
- changes in policy coverage;
- changes in prevalence of cyber insurance among companies, particularly for larger corporations ('market penetration');
- changes in the value of cyber insurance ('gross written premium' and 'policy limits').

### Type of attack

There has been a shift in the type of claims for which insurers are paying out, reflecting the changing nature of cyber risks. One interview respondent noted that while in the last 2−3 years most pay-outs related to the breach of personal information, an increasing proportion of claims now relate to ransomware and the locking down of a business. This includes paying a ransom as well as the operational disruption to businesses arising from shutting down their IT systems. Claims can now include business interruption losses and systems damages combined with ransom payments. Interview respondents report that this trend is set to continue.

A 2019 study of over 2,000 cyber claims from firms in the US, Canada and the UK reports that claims from ransomware attacks increased from seven in 2014 to 151 in 2018.[45] Along with frequency, according to the claims data, the size of ransom demands has also increased, with the 2018 average ($72k) being twice that of the five-year average ($36k).[46]

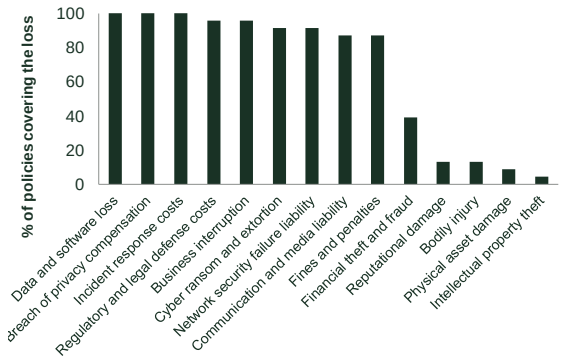
### Policy coverage

Until recently, cyber insurance products covering business interruption losses and physical damage were only offered by a few insurers. Now, however, 96% of insurers cover business interruption losses (see Figure 3.2) and an increasing number of insurers are also offering coverage for first-party losses.

Coverage is continually changing and expanding to reflect the dynamic nature of cyber risks and trends. For example, one interviewed insurer reported that since the introduction of their cyber insurance product in 2012, they were already on their fourth generation of coverage, in order to keep pace with the changes in the market. Another insurer reported that changes to policy coverage can also be attributed to brokers engaging with businesses to understand their concerns and the risks that they want to insure.

As the variety of cyber incidents and types of losses that can be covered by cyber insurance increases, the benefit to UK businesses of investing in cyber insurance will also increase. Cyber insurers and brokers are also becoming better able to understand a particular company's insurance needs, tailoring cover appropriately.

**Figure 4.2 Categories covered by stand-alone cyber insurance policies**




Note: OECD, based on policies from SHA, QBE, CFC Underwriting, Munich Re, General Re, Zurich Insurance, Delta Insurance, CNA Insurance, AIG, Chubb, ISO, Tokio Marine HCC, XL Catlin, Tokio Marine Kiln, Marsh, Hiscox, Beazley, Allianz, Specialty and Swiss Re.

Source: OECD (2017), 'Enhancing the role of insurance in cyber risk management', Figure 3.2.

Linked to policy coverage, insurers are increasingly emphasising the service element of their insurance proposition. For example,

[44] Examples of coverage include Allegretti, A. (2018), 'Cost of WannaCry cyber attack to the NHS revealed', 11 October.

[45] NetDiligence (2019), 'Cyber claims study: 2019 report', p. 36.

[46] NetDiligence (2019), 'Cyber claims study: 2019 report', p. 36.

the provision of forensic IT specialists and legal experts.

## Market penetration

The prevalence of cyber insurance among UK businesses varies by business size and sector.

- Large corporations tend to buy more insurance than smaller businesses. Approximately 35% of large businesses in the UK have cyber insurance, compared to just 1.2% of micro and small firms. Of medium firms, 31% had purchased cyber insurance, altogether resulting in 11% of businesses overall having cyber insurance.[47]
- Cyber insurance has traditionally been more prevalent among large financial services and technology companies that deal with a large quantity of data. However, such insurance is becoming increasingly relevant across all sectors of the economy.
- Supply chain risks pose particular concerns for larger companies. Cyber insurance is increasingly required as part of contractual agreements with third parties in certain industries, such as marketing and technology.[48]
- Cyber insurance is becoming increasingly important for larger companies as part of their risk governance strategy.

Similar trends are reported globally, with uptake highest for larger businesses and firms that qualify as cyber risk experts,[49] with 59% of such firms having cyber cover compared to the global average of 41%.In addtion, survey results indicate that more firms intend on adopting cyber insurance in the next 12 months, with 30% reporting plans to do so up from 25% a year ago.[50]

## Gross written premium

Trends in gross written premium (GWP) demonstrate that cyber insurance is still only in the emergent stage, but has been growing year-on-year.

In 2016, the stand-alone cyber insurance market reached an estimated $3.5bn in written premiums, although nearly $3bn of this was written on behalf of US companies, and just $300m for European companies. The total figure has been predicted to be more than double by 2020, primarily due to growth in Europe following GDPR.[51]

## Policy limits (exposure)

Trends in policy limits can be viewed from the perspective of both the insurer (supply side) and the businsess itself (demand side). Comparing the insurer and the business limits provides an indication of spare capacity in the market. We explore these in turn below.

### Insurer limits

Insurer limits capture the total amount of insurance, in monetary terms, that the insurer is willing to provide to the market and is at risk for. In essence, it is a measure of exposure. Overall, policy limits in the industry have increased.[52]

### Business limits

Business limits relate to the maximum policy limit a firm of a given size can take out to cover its risks.

Insight from the interviews with insurers suggest that there is a difference in opinion over the level of capacity, with respect to policy limits, available to larger corporations. On the one hand, an insurer reported that the largest corporates buy as much insurance as the market makes available, with the current limits inadequate to cover appetite. In particular, for the heavily exposed (data-heavy) companies, there is a race to get to a billion dollars' worth of capacity. On the other hand, another insurer reported that capacity is not, for the most part, an issue for businesses. In any case, it was reported that corporate governance is increasingly influencing the levels of cyber insurance purchased by large corporations.

The insurers interviewed were fairly unanimous on the trends in policy limits purchased by small companies. Namely that they buy relatively low amounts, and when buying cover for the first time, they tend to buy a small limit to start with and then gradually increase at renewal.

A number of the insurers interviewed noted that an implication of the evolving nature of cyber insurance meant that businesses, particularly the smaller ones, sometimes faced difficulty in understanding the appropriate limits to take out to adequately cover their risks.

Overall this suggests that large companies are near capacity, while there is considerable spare capacity for smaller businesses, albeit with a level of uncertainty relating to the appropriate level of insurance to take out.

[47] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July. large businesses have 250 employees or more.
[48] Insight from Oxera interview with insurance stakeholder.
[49] To qualify as an expert a firm must score highly in both execution and strategy in terms of their approach to a cyber threat. See, Hiscox (2019), 'Cyber Readiness Report 2019', 23 April, p. 8.
[50] Hiscox (2019), 'Cyber Readiness Report 2019', 23 April.
[51] OECD (2017), 'Supporting an effective cyber insurance market', May, p. 5.
[52] Insight from Oxera interview with insurance stakeholder.

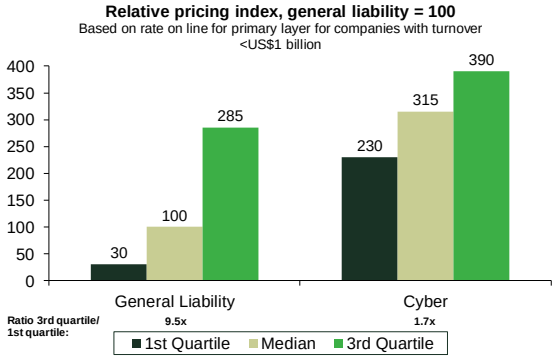
## Pricing

The evolving and varied nature of cyber risks makes pricing cyber insurance complex. However, UK insurers appear to be at the forefront of understanding cyber risks, with exports from Lloyd's syndicates accounting for approximately 25% of global gross written premium in 2017.[53]

Analysis by Marsh and the UK government finds that cyber insurance prices remain high relative to other types of risks, and considers that this may be slowing growth in the take-up of cyber insurance.

Figure 4.3 below shows that the median 'rate on line'—i.e. premiums divided by the limit of indemnity purchased—is three times higher for cyber insurance than for general liability cover, for the primary layer of insurance—i.e. the part of the policy that pays first in the event of a loss. However, as also shown in Figure 3.3, cyber insurance pricing is much flatter—i.e. the difference between the cheapest rates and the most expensive rates is much more muted than for general liability. This suggests that the reason for the higher rates in cyber insurance is uncertainty over the risks associated with cyber compared to more traditional covers. As insurers understand cyber risks better, we can expect rates to fall.

**Figure 4.3 Relative insurance prices**




Note: HM Government chart showing relative prices of cyber insurance compared to general liability at the median, 1st and 3rd quartiles.

Source: HM Government (2015), 'UK Cyber Security: The role of insurance in managing and mitigating the risk', Figure 10.

Insight from interviews with insurers indicate that the price of cyber insurance has, on average, decreased over the last couple of years. However, it is also the case that some insurers have had to increase their rates as they learn from past claims. Insurers attribute the general downward trend to the increasing availability of insurance on the market.

Over time, as competition between cyber insurers intensifies and claims data becomes more available, the price of cyber insurance is likely to fall and become less varied. Consistent with EIOPA's survey of European insurers in 2018, most of the insurers that participated in this study currently primarily rely on qualitative models to price cyber insurance policies;[54] however, as more data is available, quantitative methods are becoming more accurate and popular.

EIOPA's survey also identified entry by InsureTech start-ups as a positive and important development in the European cyber insurance market.[55] Another catalyst for new entrants is the recently implemented GDPR rules in Europe, although the increase in demand is expected to be gradual as the new regulation is understood, as are changing customer needs and risk profiles.[56] Competition can be expected to result in efficiencies and more innovative products—all of which would create an opportunity to underwrite cyber insurance more accurately.

The general view of businesses participating in the UK Cyber Security Breaches survey was that the UK cyber insurance market had become more developed, with policies appearing to be more accessible than before, and with some organisations saying that insurance premiums had decreased. [57]

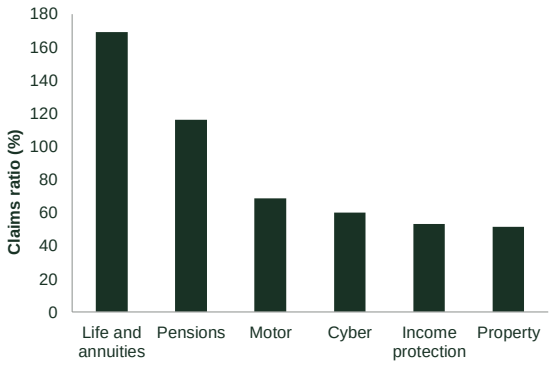
## Claims ratios

Information on cyber claims ratios is not generally available but we were provided some indicative estimates from the participants in this study.

In particular, one insurer reported a cyber claims ratio in the region of 60%. This is in line with the claims ratios reported in motor (69%), income protection (53%) and property insurance (51%). Insurance for life and annuities and pensions have higher claims ratios (169% and 116% respectively). This is demonstrated in the figure below.

[53] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[54] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[55] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[56] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[57] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.

**Figure 4.4 UK claims ratios by insurance sector**




Source: Information on cyber claims ratio sourced from Oxera interview with insurance stakeholder; the remainder of the information is sourced from ABI Industry data (2017).

## 4.5 The reinsurance market

As the cyber insurance market continues to grow and develop, concerns about potential risk aggregation and the impact that a systemic event could have will continue to grow as well. This has resulted in insurers looking for simple reinsurance mechanisms to offload some of their exposure, and the development of the cyber reinsurance market.

While the reinsurance market is still in its early stages, in 2015 the global market was estimated to be worth $525m in annual premiums and more than 15 reinsurers actively writing stand-alone cyber treaties, with the number increasing year on year.[58]

Insight from our stakeholder interviews indicates that the reinsurance market is developing rapidly, with reinsurers offering increasing capacity and innovative solutions.

### Value chain

The cyber insurance value chain is captured in Figure 4.5 below. Brokers play an important role in the purchase of cyber insurance by identifying and quantifying a businesses' exposure, and then assigning the appropriate insurance to reflect this.[59]

**Figure 4.5 The cyber insurance value chain**


Source: Oxera.

Further, there are additional players in the value chain not captured above. For example, law and PR firms deal directly with the insurer, forming part of the additional service provision to the client; risk consultants liaise with insurance brokers to identify risks and provide separate consulting services.

An insurer interviewed reported that larger businsses tend to deal with a specialist team of cyber brokers, while smaller companies deal with generalist brokers.

## 4.6 The future

The cyber insurance market is expected to continue to undergo major development and growth over the next few years, with the OECD estimating that EU coverage of cyber insurance could double between 2016 and 2020.[60]

Cyber risks have been identified as a key global risk for businesses in the coming years.[61] As such, demand for cyber insurance continues to grow, with an estimated 41% of global firms having cyber insurance in 2019, an increase from 33% in 2018.[62]

Over the longer term, coverage can also be expected to continue to expand, particularly in the context of increasing connectivity (e.g. Internet of Things, big data), in part hastened by the COVID-19 pandemic. In light of this connectivity, there is likely to be increasing interest from businesses across the economy, such as utilities and manufacturers.[63]

Alongside growth in demand, the supply of cyber insurance is also expanding, both in terms of the policy limits available, as well as the types of risks for which cover is available. As a reflection, although there are some instances of prices hardening reflecting greater than expected claims costs, the insurers that participated in this study consider that, on average, the price of cyber

[58] Aon (2017), 'Global Cyber Market Overview: Uncovering the Hidden Opportunities', June.
[59] In some instances, insurance is purely sold through brokers, such as MS Amlin.
[60] OECD (2017), 'Supporting an effective cyber insurance market', May, p. 5.
[61] EIOPA (2018), 'Understanding Cyber Insurance − a Structured Dialogue with Insurance Companies'.
[62] Hiscox (2019), 'Cyber Readiness Report 2019', 23 April.
[63] Insight from Oxera interview with insurance stakeholder.

insurance has fallen. These insurers also explained that, as the understanding of cyber risks by both insurers and firms has improved, so has the tailoring of insurance to better match a company's specific risks, resulting in better value for money coverage.

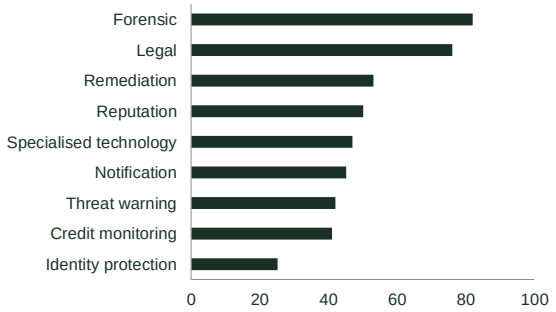
One insurer highlighted that an implication of the increasing prevalence of cyber insurance means that future large scale attacks are likely to have more of a significant impact on the insurance industry. In the past, the more limited uptake of insurance minimised the implications on insurers from events such as WannaCry. However, the increasing prevalence of insurance could mean that there would be a greater impact on insurers and could result in changes in the capacity of insurance avaialble.

# 5 Direct benefits

## 5.1 Introduction

The evidence we have gathered indicates that cyber insurance provides a number of direct benefits to UK businesses. As well as providing coverage for expenses incurred as a result of a cyber-attack, it is increasingly going beyond the traditional risk-sharing and risk transfer function of insurance to include additional services with the policies. These services, which are provided both pre- and post-breach, have important risk-mitigating and risk-containment effects by assisting businesses in protecting themselves, and getting back up and running after an event. Some of these services are captured in Figure 5.1.

**Figure 5.1 Value-added services provided by cyber insurers**




Note: Multiple responses allowed.

Source: Ponemon Institute (2017), 'Global cyber risk transfer comparison report'.

OECD research reports that businesses see value in these additional services, and even consider them to be as important as risk transfer in certain cases.[64]

Experiencing a cyber-attack does not prevent or lower the likelihood of experiencing a second attack immediately after; on the contrary, it often increases the vulnerabilities exposed. This is important in the context of the role of cyber insurance, as it highlights the role that insurance can have beyond providing risk transfer products. The direct benefits of cyber insurance can be significant, and will be explored in relation to two dimensions: pre- and post-attack benefits.

## 5.2 Before the attack

### Risk mitigation

Cyber insurance can play an important role in helping businesses better manage and mitigate cyber risks through the price discovery mechanism, whereby the design of coverage incentivises businesses to put 'the right' procedures in place.

Insurers are increasingly focusing on loss prevention activities. For example, the process of securing cyber insurance often requires organisations to quantify their exposure to cyber risks and consider the optimal level of investment to mitigate that risk.[65] This not only encourages businesses to increase their cyber awareness and assess the strength of their current security policies, it also promotes good practice by prompting businesses to install the right procedures and plans to prevent cyber threats.

Further, staff training, including e-learning platforms are increasingly being provided and offer significant benefits to companies. As previously mentioned, many cyber incidents can be attributed to some form of human error, so training can be crucial in ensuring that employees understand best practice. For example, an insurer reports that claims notifications for employee negligence doubled from between 2017 and 2018.[66] Better staff training helps staff recognise the style of potential phishing emails, as well as what to look for in email senders' details to help identify suspicious-looking emails. Since insurance places a cost on firms' risk exposure through the premiums they pay, the prospect of a reduced premium encourages firms to take steps to mitigate the risk.[67] To illustrate, 90% of US companies in 2016 made adjustments to improve risk management in order to meet cyber insurance coverage requirements.[68] Further, some insurers offer a reduction in the insurance premium if a certain proportion of a company's employees successfully complete their training programme.

[64] OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
[65] Based on insight gathered through interviews with insurance providers.
[66] AIG (2019), 'Cyber Claims: GDPR and business email compromise drive greater frequencies'.
[67] Marsh and HM Government (2015), 'UK cyber security: the role of insurance in managing and mitigating the risk', March.
[68] OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.

Through this price discovery mechanism, insurance plays an important role in helping businesses make informed decisions on investing in prevention and in reducing their risks. By putting a price on the risks, insurance can also improve the allocation of goods and services within an economy, and improve welfare directly through reduced ex ante uncertainty, helping support faster growth.

Given the novelty of the cyber insurance market, putting a price on the risk has the added benefit of helping insurers to build a dataset for rating future businesses, modelling cyber risks and underwriting and pricing future services. This generates information on cyber risks, and a by-product of this increased understanding is expertise in how to reduce the probability of attacks occurring and the extent of the resulting damages.

## 5.3 After the attack

The additional services that form part of the cyber insurance policy package can mitigate the impacts of risks once they materialise through risk containment measures as well as through initiatives that help get businesses up and running again. These are explored in turn.

### Risk containment

The services provided by insurance policies can help contain risks to businesses through a number of channels. For example, specialised IT security teams conducting a forensic investigation of the network once a breach has been notified, replacing lost business income, covering the legal defence and compensation costs relating to liability claims against an organisation.

The expert response help provided with the insurance is highly valued, especially for SMEs who tend to have less sophisticated IT systems than their larger counterparts.

A case study illustrating the value that insurance plays in risk containment is illustrated in Box 5.1.

**Box 5.1 Case study: phishing scam**

*Sector: Marketing*
*Turnover: Up to £1m*
*Claim cost: £39,000*

**Incident**
A PR company noticed a problem with its emails. Its regular IT contractor investigated and concluded that the most likely cause was malicious activity. The business contacted the insurer, which then deployed an IT forensics team site to investigate and confirmed the company had indeed been the victim of a malware attack. It also confirmed that the hackers who deployed the malware had accessed the insured's systems and that personal data was potentially compromised.

**Insurer response**
After investigating the extent of the breach, the IT team removed the malware and plugged the gap in the PR company's security that had allowed the breach. The insurer then engaged legal counsel to advise the insured on its notification obligations, and then arranged the notification of the regulator and relevant data subjects.

Source: Hiscox (2019), 'CyberClear'.

In a number of instances, businesses are required to contact insurers within a certain time frame after an attack to claim these benefits. As such, this incentive encourages a swift response by the company, resulting in quick implementation of a response and recovery plan as a result. This helps to reduce the impact of the attack and limit its spread.

This risk containment benefit goes beyond the firm directly affected, as it allows insurers to provide insight from claims across their client base, strengthening resilience and preventing other firms from suffering the same breach, which reduces total losses as a result.

### Getting the business up and running again

Cyber insurance can provide a layer of peace of mind in the case of a breach. As cyber insurance policy is designed to ensure business continuity, this ensures business operations continue when an adverse event occurs, thereby preventing or limiting business interruption losses.

The additional services cyber insurance can offer, such as reputation protection and forensic investigation are also important in getting the business up and running again and in ensuring business continuity. The positive effect that cyber insurance can have in ensuring business continuity is demonstrated in Box 5.2.

**Box 5.2 Case study: Ransomware attack**

*Sector: Food services*
*Turnover: £1m−£2m*
*Claim cost: £20,000*

**Incident**
A ransomware attack encrypted a restaurant's entire server, affecting its point of sale registers and meaning it was effectively unable to trade.

**Insurer response**
Having exhausted all other options, the insurer covered the cost of the ransom, together with the associated IT costs of ensuring that the business was back up and running. In addition to these costs, the insurer covered the business interruption suffered by the restaurant because of being unable to trade.

Source: Hiscox (2019), 'CyberClear'.

# 6 Benefits to the wider economy

Our research also suggests that cyber insurance is having positive effects on the wider UK economy. The main ways through which cyber insurance is benefiting the wider economy are described below.

## Raising the general level of security in the UK economy

In its 2016 National Cyber Security Strategy, the Government recognised the importance of ensuring the UK economy is resilient to cyber risks to allow businesses to continue to prosper and grow.[69] As part of this, the Government set out plans to work with the UK cyber security industry to capitalise on its existing strengths in these areas, particularly as applicable to artificial intelligence (AI) and the digital economy. Cyber insurance provides another, valuable layer of protection, helping achieve the Government's goal of making the UK one of the most secure places in the world to do business.

In addition to the financial security cyber insurance can provide, in the context of the Cyber Security Breaches survey, various organisations highlighted the extras that went alongside any liability cover, as their main drivers for taking up cyber insurance. The firms felt that these extras such as having access to a breach management team or a forensics team to analyse the breach would help them manage the reputational damage from a breach. Indeed, cyber insurance was seen as a useful 'badge of honour' by some respondents.

Given the potential contagion effect of cyber-attacks, an increase in the number of firms with cyber protection is likely to have positive externalities across the whole economy. Similar to stopping a forest fire from taking hold, by preventing a cyber-attack on one firm, other firms that might have been affected as a consequence, are also protected. Thereby, in addition to directly assisting and encouraging firms in improving their cyber security protection, where it breaks the chain of contagion, cyber insurance can have a broader impact.

## Supporting SMEs, the drivers of innovation in the UK economy

SMEs comprise a large part of the UK economy, accounting for 99% of all UK businesses.[70] They play a crucial role in creating job opportunities, driving innovation and spurring competition in the UK economy.

However, their more limited financial and technical resources, may mean that they are less well-protected to cyber-attack than larger firms. For example, while 88% and 97% of medium and large UK businesses have undertaken five or more of the Government's 10 Steps to Cyber Security guidance,[71] this falls to 51% and 72% for micro and small businesses.[72,] Similarly, investment in cyber security is substantially lower for UK small businesses than larger businesses. As reported in Figure 2.3, while large UK businesses invest on average £443 annually per employee (c. £277k in aggregate), small businesses invest on average £139 per employee (c. £3,490 in aggregate) on cyber security policies.

In addition, SMEs may be more credit constrained, and therefore, less able to weather a cyber incident 'storm'. In this context, cyber insurance may provide a critical lifeline, as well as providing helpful guidance as to how to prioritise cyber security spending.

Data on penetration of cyber insurance among small businesses is not available. However, given the differences in the prevalence of cyber security policies between small and large businesses (74% versus 32%),[73] it is likely to be somewhat lower for smaller businesses. To a certain extent this reflects that cyber incidents appear to be more common for larger businesses (61% compared to 30%) however, it may also reflect the price of cyber insurance. As the price of cyber insurance falls, which some businesses as well as insurers consider is already occurring,[74] penetration can be expected to rise. Alongside price reductions, insurers are increasingly offering cyber insurance that covers a broader range of losses and types of incidents, enabling firms to buy coverage most tailored to their specific needs.

Overall, by supporting businesses, in particular, SMEs cyber insurance is helping stimulate growth and innovation in the UK economy.

## Exports

Cyber insurance plays an important role in UK export strategy in two ways. Firstly, it makes a direct contribution to UK exports, and secondly, it helps ensure the resilience of the UK economy to cyber threats, attracting more inwards investment and therefore, indirectly contributing to exports.

[69] HM Government (2016), 'National Cyber Security Strategy 2016-2031'.
[70] House of Commons (2018), 'Business statistics', December.
[71] See National Cyber Security Centre (2018), '10 steps to cyber security', 17 November.
[72] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.
[73] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.
[74] Department for Digital, Culture, Media & Sport (2019), 'Cyber Security Breaches Survey 2019', 1 July.

London is a major centre for cyber insurance, with approximately 25% of global GWP being written through Lloyd's syndicates in 2017.[75] Overall, cyber insurance accounted for approximately 0.13% of the export of UK services and this is expected to grow.[76]

The general consensus is that the cyber insurance market is set to continue growing. Even the US cyber insurance market, which is the most developed, is far from reaching a point of maturity, such that global demand for cyber insurance is likely to increase substantially over the next few years. With readily available financial, advisory and technical services and its existing position in the global cyber insurance market, the UK is well positioned to benefit from this growth in global demand, bringing further benefits to the UK economy.

The indirect contribution from cyber insurance to UK exports is hard to quantify. However, as recognised by the Government, making the UK one of the most secure places in the world to do business, is an important part of expanding our economy and building a Britain fit for the future.[77]

# 7 Conclusion

Cyber insurance has and will continue to play an important role in the UK economy, both through the direct benefits to UK business as well as the impact on the economy more broadly.

Looking ahead, the cyber insurance market is expected to continue to undergo major development and rapid growth over the next few years, reflecting the increased awareness of risks as well as the likely increase in the frequency of cyber events driven by the broader trend of increasing digitisation of businesses, which in part, have been hastened by the COVID-19 pandemic.

This poses challenges for data security as the quantity of data susceptible to cyber-crime increases. To tackle the challenges that arise from increasing connectivity, it is expected that coverage of cyber risks will continue to expand. To reflect this, the relevance and importance of cyber coverage in the overall functioning of the economy is expected to increase significantly.

A deeper understanding of cyber risks is both required and expected as the market matures. This will be from both the demand side, as businesses better understand their own needs, as well as the supply side, as insurers get better at assessing and treating risks. There could be a broader role of other industry actors, such as government, to help facilitate this knowledge sharing and awareness raising currently required to understand risks properly.

It is expected that as more data becomes available, improved risk models will be developed. Current data limitations mean that at present, qualitative models are frequently used alongside quantitative ones to facilitate the estimation of price, risk exposure and risk accumulation.

By increasing the cyber-readiness of UK firms, employees and cyber-security professionals, cyber insurance is likely to help contribute to the UK's brand as a place to do business. This, in turn, may help stimulate further investment in the UK economy and boost exports.

As with all types of insurance, the risk transfer function of cyber insurance helps improve the allocation of goods and services within the economy, and can improve welfare directly through reduced uncertainty. This, combined with the factors described above, will help to support faster growth of the UK economy.

[75] EIOPA (2018), 'Understanding Cyber Insurance – a Structured Dialogue with Insurance Companies'.
[76] Based on 2014 trade figures from the ONS, and 2014 export figures from Marsh and HM Government (2015), 'UK cyber security: the role of insurance in managing and mitigating the risk', March.
Services exclude travel, transport and banking
[77] Gov.uk, 'The UK's Industrial Strategy (Archived)', accessed 9 December 2019.


www.oxera.com
oxera
compelling economics