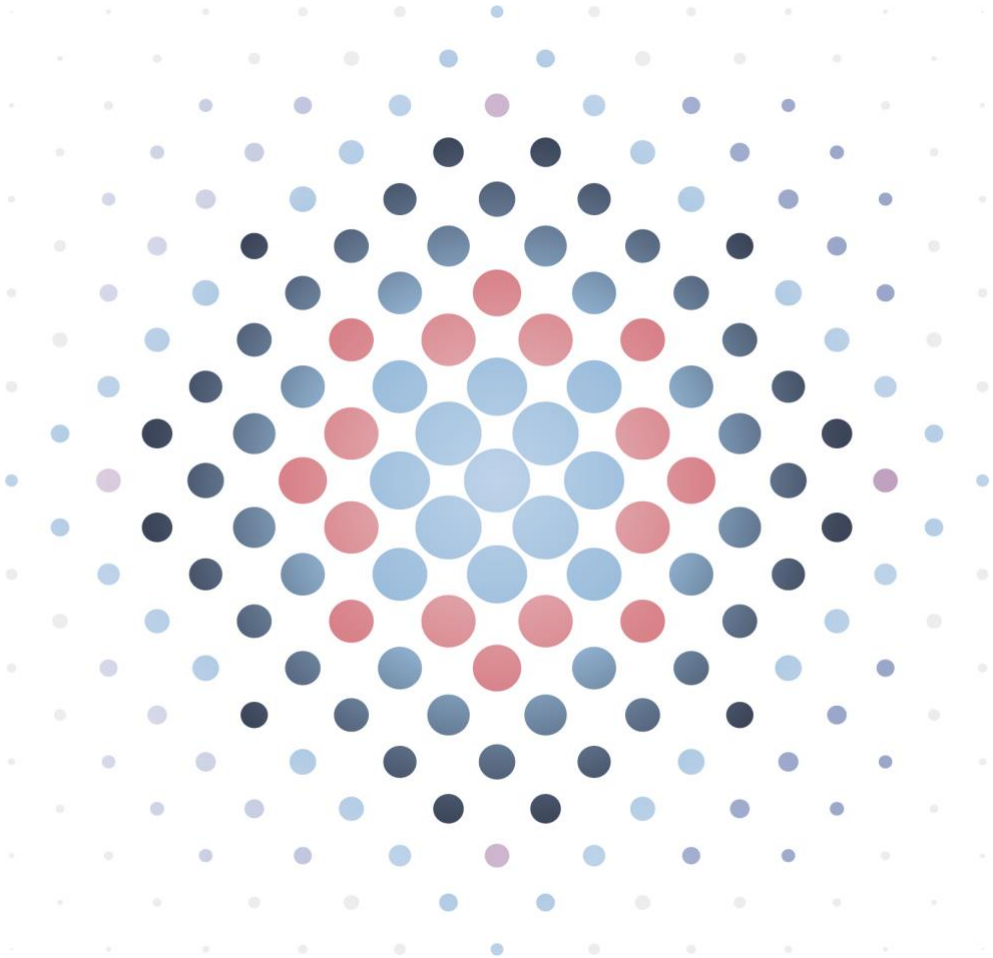
Economic Impact of Intellectual Property and Knowledge Assets Theft from Cyber Attacks in the UK

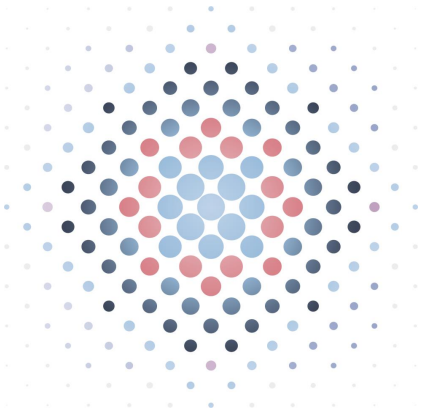
Final report

Prepared for the Department for Science, Innovation and Technology (DSIT)

July 2025



alma economics



About the authors

Alma Economics combines unparalleled analytical expertise with the ability to communicate complex ideas clearly.

www.almaeconomics.com

Expert panel

Alma Economics received expert advice throughout this research from Dr Anna Cartwright (Oxford Brookes University), Professor Edward Cartwright (De Montfort University), Dr Nicola Searle (Goldsmiths, University of London), Associate Professor Kris Stoddart (Swansea University), and Dr Daniel Woods (University of Edinburgh). All conclusions in this report are those of Alma Economics and do not necessarily represent those of partners.

Commissioning organisation

Department for Science, Innovation & Technology

This research was supported by the Department for Science, Innovation & Technology and the R&D Science and Analysis Programme at the Department for Culture, Media & Sport. It was developed and produced according to the research team's hypotheses and methods. Any primary research, subsequent findings or recommendations do not represent Government views or policy.

Table of Contents

Executive summary

Intellectual Property (IP) and knowledge assets theft has become an increasingly significant threat in today's digital age, particularly due to the rise in cyber attacks targeting businesses and their intangible assets (The IP Press, 2025). A growing number of UK businesses and charities have reported experiencing cyber breaches, with phishing being the most common type of attack (DSIT, 2024). These attacks not only compromise data security but also put vital knowledge assets and IP at risk. IP is a critical driver of innovation and competitive advantage, and its loss can have severe consequences for businesses and future innovation within the economy. However, the financial impact of such losses remains underexplored.

Alma Economics was commissioned by the Department for Science and Technology (DSIT) to conduct research on the economic impact of IP and knowledge assets theft resulting from cyber attacks on UK businesses and the broader economy. This research is part of a broader initiative to better understand and quantify the costs of cyber attacks in the UK.

Methodology

This research included a multi-step approach combining qualitative and quantitative methods to estimate the economic impact of IP and knowledge assets theft from cyber attacks to UK businesses. The methodology included a literature review, quantitative analysis, case studies and estimates of economy-wide impacts.

The literature review involved a desk-based search of academic databases to identify relevant research on IP and knowledge assets theft as a result of cyber attacks. Following the review, a workshop with sector experts helped refine findings and identify gaps.

For the quantitative analysis, two key datasets were used: the Advisen Ltd. Cyber Loss Data (provided by Zywave, Inc.), which tracks cyber attacks, and the FAME database (provided by Moody's), which provides financial data on UK companies. The analysis focused on understanding the prevalence of IP and knowledge assets theft from cyber attacks and its financial consequences, particularly on company performance in terms of sales and profitability. A regression model was employed to assess the impact of IP and knowledge assets theft from cyber attacks on these financial metrics, distinguishing between Small to Medium Enterprises (SMEs) and Large Enterprises (LE).

In addition to the quantitative analysis, case studies of IP and knowledge assets theft incidents were developed to provide qualitative insights into the broader impacts on businesses. Lastly, the research team estimated the economy-wide impacts of IP and knowledge assets theft through cyber attacks by integrating findings from both the literature review and quantitative analysis, contributing to a comprehensive understanding of the broader economic implications.

Findings

The literature review highlighted that while cyber attacks are increasingly common, IP and knowledge assets theft remains relatively difficult to detect. When it does occur, businesses

may experience operational disruption, reputational damage, and lost revenue, with potential for bankruptcy. Consumers, in turn, may experience counterfeit goods, lower quality, and higher prices, but in the short term, counterfeit goods may offer cheaper alternatives. State-sponsored attacks have increased over time (Priyandita et al., 2022; Tran, 2018), though attribution remains challenging, as non-state actors often use state-developed tools or operate with indirect state support. Stolen IP is primarily used to replicate products and undercut prices, for broader financial and strategic purposes such as sabotage and misinformation. Existing estimates of the value of stolen IP in the UK are outdated, with the most recent assessment suggesting annual losses of around £9 billion (Cabinet Office, 2011).

Our econometric analysis indicates that, across all firms, a cyber attack involving IP and knowledge assets theft is associated with an estimated 2% decline in sales growth in the year of the attack,[1] relative to the growth that would have been achieved without it. Our results also suggest that, although sales decrease, EBIT either increases or remains constant. This means that companies may be actively reducing costs – disproportionately to the drop in sales – in order to maintain profitability.

For SMEs, the impact was much more pronounced, with a statistically significant reduction of 16% in sales growth within the year of the attack. However, the estimated drop in profits was similar to the decline in sales, suggesting that these firms achieved cost-cutting measures in line with their fall in sales. Overall, this points to a proportionate loss of economic activity.

Furthermore, for both the full sample and the SME subset, our results indicate that firms seem to recover from the negative financial shock of a cyber attack in the following year, rather than facing long-term sales losses. This suggests that cyber attacks tend to have a temporary financial impact.

When focusing on identifying case studies that illustrate the impact of IP and knowledge assets theft due to cyber attacks, we found that most firms continued to grow despite such incidents, with 80% of companies in our sample seeing growth in either sales or profits in the year following the attack. When considering firm size, large companies generally experience little to no revenue decline after cyber attacks, while some smaller firms could experience severe consequences, especially those that rely on a narrow range of valuable IP and knowledge assets for most of their revenue. Our case studies showed that in extreme cases, IP theft could pose an existential threat to SMEs – particularly when stolen IP is used to develop rival products, enabling larger firms to compete more aggressively on price or leverage stronger marketing and post-sales support. However, SMEs typically generate relatively little news coverage, rarely file long-form annual reports, and often do not provide detailed accounts (DSIT, 2024; Reuters, 2024; The UK Government, n.d.). As a result, publicly known cases are limited and likely underrepresent the true scale of the issue. Among the SME case studies we identified, some recovered quickly by implementing cost-cutting measures, while others faced prolonged financial struggles. In extreme cases, businesses contracted so significantly that they were reclassified from Large Enterprises to SMEs, highlighting the potential long-term effects of cyber attacks.

[1] Results non-significant ($p < 0.65$)

While the best available data was used for our analysis, it is not entirely clear what proportion of the cyber attacks in the dataset were successful in achieving IP and knowledge assets theft. Assuming all attacks were successful provides a lower-bound estimate of the economy-wide impact of IP and knowledge assets theft due to a cyber attack, suggesting that IP and knowledge assets theft cost the UK economy £1 billion in 2024, or 0.04% of the total UK Gross Domestic Product (GDP) in 2024. Conversely, if the dataset captures all cyber attacks, regardless of success, the upper-bound estimate indicates that IP and knowledge assets theft from cyber attacks resulted in a loss of £8.5 billion in 2024, equivalent to 0.30% of the total 2024 UK GDP.[2] Based on these estimates, this study concludes that cyber attacks attempting IP and knowledge assets theft cost the UK economy between 0.04% and 0.30% of the total UK GDP per year.

Future research suggestions

A key limitation of this study is the lack of comprehensive data on the subject. However, many of the challenges identified throughout the report could be addressed with better data. In particular, access to a larger sample of identifiable cases involving IP and knowledge assets theft resulting from cyber attacks would significantly enhance the analysis. Greater detail on existing cases would also be valuable – especially clearer descriptions of what occurred and precisely what was stolen.

However, given the increasing frequency of cyber attacks – whether due to a rise in actual incidents, better reporting, or a combination of both – improving the availability and quality of data will be critical for advancing research in this area. Our sample revealed a 47% average increase in reported cyber attack cases from 2014 to 2023, with a sharp 150% rise between 2022 and 2023. This upward trend highlights either the growing prevalence of cyber crime, the increased reporting of such cases, or both. While our estimates provide an initial assessment, replicating this analysis in future years with a larger sample will be highly valuable for a better understanding of the evolving threat landscape and its broader economic consequences. This will ultimately help develop more effective strategies to mitigate risks and strengthen the cyber security posture of businesses, particularly those most vulnerable to these threats.

[2] To capture the range of possible economic impacts, we present a lower-bound estimate based on the assumption that all attacks in the dataset were successful, and an upper-bound estimate that assumes the dataset includes both successful and unsuccessful attacks. Although this may seem counterintuitive, focusing only on successful attacks results in a lower estimated prevalence across all UK firms, because most cyber attacks are unsuccessful. Including unsuccessful attacks dilutes the overall theft rate, raising the implied economic cost.

Introduction

Background

A cyber attack is defined as 'an attempt to damage, disrupt or gain unauthorised access to computer systems, networks or devices' (National Cyber Security Centre). The DSIT 2024 Cyber Security Breaches Survey found that half of businesses (50%) and around a third of charities (32%) reported having experienced some form of cyber security breach or attack in the past 12 months. However, this likely underestimates the true scale of cyber attacks in the UK, as the survey only captures attacks that organisations were able to identify and willing to report. Other surveys of UK businesses have suggested that the number of cyber attack incidents has increased over time (Cloudflare, 2024).

The increasing prevalence of cyber attacks poses a significant threat to both intellectual property (IP) and knowledge assets. In this research, we adopt a broad definition that includes the theft of both. IP generally refers to "creations of the mind for which specific property rights are available in law," such as trademarks and patents (Intellectual Property Office, 2017). A "knowledge asset" is a type of intangible asset (that is not physical in nature), that relates to knowledge, information, intelligence and creativity, which can be exploited for strategic, political or economic gain.

The most commonly reported type of cyber attack in the 2024 Cyber Security Breaches Survey was phishing, which could lead to a data breach that, in turn, could significantly harm a firm's IP and knowledge assets. According to Proofpoint (2024), 32% of successful phishing attacks in 2023 resulted in the loss of data or intellectual property. IP is a crucial asset of competitive advantage in the domestic and international markets. The loss of IP through cyber attacks could threaten a firm's survival, and beyond individual business impacts, it could have economy-wide impacts, given the central role of IP-intensive businesses in the UK economy.

A study by the European Union Intellectual Property Office (EUIPO) found that firms in the EU that own at least one patent, registered design or trademark generate 55% higher revenues per employee than those without IP rights (EUIPO, 2021). Research has also shown that strengthening IP protection has a positive impact on firm Research and Development (R&D) investment and innovation, particularly in the private sector (Fang et al., 2017). While there is limited empirical research on the value and economic impacts of trade secrets, they are widely used in various sectors, particularly manufacturing, as a strategic tool for capturing the returns on innovation (Intellectual Property Office, 2021). Additionally, research published by the UK Intellectual Property Office (IPO) found that patents and trademarks arising from UK Research and Innovation (UKRI) grants are frequently commercialised, suggesting that IP rights could foster new business opportunities and contribute to economic growth (Intellectual Property Office, 2023). Extensive evidence also indicates that IP protection has broader positive effects on innovation, economic growth (Bielig, 2015; Neves et al., 2021), as well as exports (Yang and Huang, 2009).

Research aims and objectives

While it is recognised that the theft of IP and knowledge assets through cyber attacks could present challenges to businesses and the broader economy, the cost of such losses in the UK has not been recently quantified. There is currently no established methodology to measure the economic impact of IP and knowledge assets theft from cyber attacks, nor is there a consensus on how to quantify the overall cost of cyber attacks to the economy.

Alma Economics was commissioned by the Department for Science, Innovation and Technology (DSIT) to estimate the impact of IP and knowledge assets theft resulting from cyber attacks on UK businesses and the wider economy. This research forms part of a broader initiative aimed at assessing the economic cost of cyber attacks on the UK economy.

The study seeks to address the following research questions:

- What impacts on businesses and consumers arise from IP and knowledge assets theft through cyber attacks?
    - Do impacts differ by type of IP?
    - Do impacts differ from incidents not associated with cyber attacks?
    - What case studies are there that show the harm of IP and knowledge assets theft?
    - Where are the economic impacts felt across businesses and consumers (e.g. damage to reputation or brand; reduction in R&D)? How can these be categorised into ‘costs in response’ versus ‘costs as a consequence’? (e.g. mapped according to a typology)
    - What is the impact on the future revenue or profit of the company that lost the IP?
- How frequently is IP stolen during a cyber attack?
    - This should be split out by type of IP and the impact it has when stolen.
    - Does the pattern of IP and knowledge assets theft through cyber attacks differ from wider IP and knowledge assets theft?
- How many of these attacks come from state vs non-state actors (where known or suspected)? Are any specific characteristics or motivations known about these actors?
- How is this stolen IP used? (e.g. Is it used to steal market share?)
- What is an estimated range for the value of IP that has been stolen from cyber attacks in the UK?
- What is the best methodology to model the cost of IP and knowledge assets theft facilitated by cyber attacks?

The report is structured as follows:

- **Methodology** – Provides an overview of the methodology.
- **Literature review** – Summarises key findings from the literature review in relation to the research questions.
- **Econometric results** – Discusses our econometric modelling and presents relevant findings.

- **Case studies** – Outlines anonymised examples illustrating the different impacts of IP and knowledge assets theft on various companies.
- **Economy-wide impacts** – Presents estimates of the impact of cyber attacks leading to IP and knowledge assets theft on GDP.
- **Conclusions** – Summarises the key findings and overall conclusions.

Methodology

This chapter provides an overview of the methodology used in this research. The core components of our analysis included: (i) a literature review, (ii) quantitative analysis of IP and knowledge assets theft from cyber attacks, (iii) case studies, and (iv) estimating economy-wide impacts.

Literature review

The first step involved a desk-based review of existing research to address the key research questions. Given the difficulty in identifying relevant evidence on this topic, we used various databases for our search but prioritised Google and Google Scholar due to their broader range of sources. Searches were conducted using keywords corresponding to the research questions, such as "IP theft," "cyber attack," and "cost," which were combined in different ways. We then documented search results that yielded relevant findings. Additionally, we applied snowballing techniques, where references from identified papers were used to locate other relevant sources.

Our team identified approximately 40 papers addressing aspects of IP and knowledge assets theft resulting from cyber attacks, highlighting the limited existing literature on this subject. Our academic partners also recommended additional relevant literature to help answer the research questions.

Following the literature review, we held a workshop with sector experts, including representatives from DSIT, the Home Office, IPO, National Cyber Security Centre (NCSC), and UK Research and Innovation (UKRI). This workshop allowed us to present key findings from the literature review, validate them through expert feedback, and identify additional sources or gaps in the literature. The findings from the literature review were subsequently refined to incorporate insights from the workshop.

Limitation: The limited availability of research specifically addressing IP and knowledge assets theft resulting from cyber attacks – particularly in a UK context – posed a challenge in gathering relevant evidence. While we identified useful sources, the scarcity of comprehensive studies highlights a gap in the literature that future research could address.

Quantitative analysis of IP and knowledge assets theft from cyber attacks

To assess the economic impact of IP and knowledge assets theft on firms, our approach focused on two key components: prevalence and impact. First, we needed to determine how widespread IP and knowledge assets theft from cyber attacks was by understanding the frequency of such incidents and the characteristics of affected firms. Second, we quantified the financial consequences for these firms, particularly in terms of changes to their economic performance, such as sales and profitability, following a cyber attack. To achieve this, we used two key datasets, one containing information on cyber attacks and another providing financial performance data for UK companies:

- **Advisen Ltd. Cyber Loss Data (provided by Zywave, Inc.)**: This dataset contains publicly available information on cyber attack incidents, along with details on affected companies, attack types, and threat actors. It offers insights into the frequency of IP and knowledge assets theft events and helped us identify the firms that have experienced these attacks. For our research, we used cases categorised under "Data – Malicious Breach". This label refers to situations where personal confidential information or digital assets have been or are at risk of being exposed or stolen by unauthorised internal or external actors (Shevchenko et al., 2023). Advisen compiles its cyber incident database through ongoing global monitoring by a dedicated team of researchers. The data is sourced primarily from two channels: i) individual cyber events identified through public and subscription-based platforms, and ii) information provided by governmental and regulatory bodies.
- **FAME database** (provided by Moody's): A comprehensive database containing financial and company information for all public and private UK firms, including sales, Earnings Before Interest and Taxes (EBIT),[3] and Standard Industrial Classification (SIC) codes.

To prepare the FAME database for analysis, several filtering steps were taken. Companies with negative sales[4] in any year were removed, and those without postcodes were excluded. Only active companies and top-level holding companies in the UK were retained, and firms without complete sales and EBIT data for the entire period were excluded. Additionally, only companies that consistently reported financial information on December 31 each year were included to ensure comparability. At the time of analysis, the most recent financial data available for companies with a December year-end was from 2023. The dataset covered a 10-year period from 2014 to 2023, forming a balanced panel.

Next, we merged the FAME dataset with the Zywave, Inc. dataset, which contains records of UK companies that have experienced cyber attacks. Since Zywave, Inc. data lacks specific indicators for IP and knowledge assets theft, we used a proxy by restricting our sample to cases classified as 'Data – Malicious Breach', following consultations with Zywave representatives. Because the two datasets did not share a unique company identifier, we merged records by matching the first four characters of company names (accounting for potential variations in company names between datasets) and using full postcodes (without spaces) to ensure accuracy. We retained FAME companies successfully merged with the Zywave, Inc. dataset, as well as those included only in the FAME database. However, firms appearing solely in the Zywave, Inc. dataset without matches were excluded, as they were likely not UK-based companies.

Through these processes, we began with approximately 7,000 UK firms from the Zywave, Inc. dataset and 5,800 from the FAME dataset. Among the firms in FAME, around 3% lacked a postcode, fewer than 1% reported negative sales in at least one year between 2014 and 2023,

[3] Earnings before Interest and Tax. This provides an estimate of the profitability of a business that is broadly similar to the National Accounts concept of Gross Operating Surplus.

[4] Negative sales are unusual and may indicate exceptional circumstances, such as the issuance of credit notes, customer refunds, or accounting adjustments due to contract reversals.

and 64% reported financial data as of the end of December. After applying these filters, and merging both datasets, our final regression analysis was conducted on a sample of 3,600 firms.

For the regression analysis, we examined the impact of cyber attacks that led to 'Data-Malicious Breach' on key financial metrics such as sales, profit measured by EBIT, and changes in both sales and EBIT, while differentiating the analysis between Small to Medium Enterprises (SMEs) and Large Enterprises (LE). Further details on specific regression models are discussed in Chapter 'Econometric results'.

Limitations: The filtering criteria applied to the FAME dataset may have implications for our results. For instance, firms without complete financial data were excluded, potentially removing businesses that may have been significantly impacted by cyber attacks. Also, the merging of the Zywave, Inc. and FAME datasets relied on name and postcode matching, which may have introduced errors or resulted in some affected firms being excluded from the final dataset. Another key limitation is the lack of detailed information in the Zywave, Inc. dataset regarding the nature of each cyber incident. The analysis would benefit from more granular data, such as specifics of the event, whether the attack was successful, a description of what precisely was stolen, and how the IP or knowledge assets were exploited.

Case studies

To complement the quantitative findings, we conducted case studies to develop a broader narrative on the potential consequences of cyber attacks leading to IP and knowledge assets theft. Due to limited publicly available information, we used information from the Zywave, Inc. dataset to identify cyber attacks and analysed company performance in terms of sales and EBIT both before and after the attack using the FAME database. Additionally, we included the well-known Sinovel vs. AMSC as a case study. While direct links between cyber attacks and financial performance (such as sales declines or EBIT reductions) were difficult to establish, the case studies provide contextual understanding of the risks businesses face in an increasingly digital economy.

Limitations: The availability of case study data was limited, particularly for SMEs. Many firms do not publicly disclose incidents of IP and knowledge assets theft, and media coverage of cyber-enabled IP and knowledge assets theft is often focused on larger firms. As a result, our case studies may not fully represent the experiences of smaller businesses.

Estimating economy-wide impacts

The final step of our analysis involved estimating the broader economic impact of cyber attacks leading to IP and knowledge assets theft. This was achieved by combining estimates from existing literature with findings from our quantitative analysis. By integrating these sources, we estimated the impact on GDP, providing a more comprehensive understanding of the economic risks associated with cyber-enabled IP and knowledge assets theft.

Limitation: To estimate the economy-wide impacts, we needed to determine the prevalence of IP and knowledge assets theft due to cyber attacks in UK firms. However, the Zywave, Inc. dataset does not distinguish between cyber attacks that are successful or unsuccessful in

achieving IP and knowledge assets theft. To account for this uncertainty, we provided upper and lower-bound prevalence rates rather than a single-point estimate. Future research incorporating more granular data on attack outcomes would enhance the accuracy of these estimates.

Literature review

A literature review was conducted to identify existing research addressing the research questions for this study. This review focused particularly on sources that could assist with the remainder of the study in one of two ways: (a) by providing quantitative estimates that could be used to benchmark results against, or (b) by offering insights into methodological approaches.

Key findings

Impacts of IP and knowledge assets theft on businesses and consumers: Businesses may face operational disruption, reputational damage, and lost revenue, with potential for bankruptcy. Consumers may experience counterfeit goods, lower quality, and higher prices, but in the short term, counterfeit goods may offer cheaper alternatives.

Frequency of IP and knowledge assets theft in cyber attacks: Data theft is the most common form of cyber attack, with the UK heavily targeted; however, IP and knowledge assets theft remains relatively rare and hard to detect.

State vs Non-State actors in IP and knowledge assets theft: State-sponsored cyber attacks have increased, but attribution is challenging, as some non-state actors use state-developed tools or operate with state support. Non-state actors usually target financial gain, while state actors may also pursue geopolitical objectives.

Use of stolen IP: Stolen IP is typically used to replicate products, undercut prices, or for sabotage and misinformation, often for financial or geopolitical gain.

Estimated value of stolen IP in the UK: The only quantitative estimate of the value of IP stolen through cyber attacks in the UK is from the Cabinet Office (2011) study, which is now over a decade old. It suggested the UK loses an estimated £9.2 billion annually, with industries like pharmaceuticals and electronics most affected.

Methodology to model IP and knowledge assets theft costs: Methods include case studies, econometric analysis, stock market reactions, and top-down approaches to estimate the impact of IP and knowledge assets theft on businesses and the economy.

Identified sources by research question

RQ1. What impacts on businesses and consumers arise from IP and knowledge assets theft through cyber attacks?

Channels for impacts on businesses

The literature identifies several channels through which cyber crime impacts businesses. Cabinet Office (2011) provides four categories for the impacts of cyber crime more generally:

- **Costs in anticipation of cyber crime**, primarily security measures, i.e. prevention and insurance costs,
- **Costs as a consequence of cyber crime**, which take into account direct losses, including business continuity and disaster recovery response costs,
- **Costs in response to cyber crime**, such as regulatory fines from industry bodies and indirect costs associated with legal or forensic issues, and
- **Indirect costs associated with cyber crime**, which include such factors as reputational damage.

Focusing specifically on the costs following an incident of IP theft, Deloitte (2016) presents a case study that includes the following categories: (i) technical investigation, (ii) public relations costs, (iii) legal fees and litigation, (iv) cyber security improvements, (v) insurance premium increases, (vi) operational disruption, (vii) value of lost contract revenue, (viii) devaluation of trade name, and (ix) loss of intellectual property. In their stylised case study, Deloitte (2016) found that the last four factors accounted for approximately 99% of the total costs of the theft. In descending order, Deloitte (2016) estimated that the value of lost contract revenue would account for around 49% of total costs, operational disruption would account for 37% of costs, devaluation of trade name would be 8.5% of costs and loss of IP would be 4.5%. Costs related to technical investigation, public relations, attorney fees and litigation, cyber security improvements, and insurance premium increases would total less than 1%.

Ettredge et al. (2018) emphasised the role of loss of trade competitiveness, which would fit with Deloitte's category of losing contract revenue. Curti et al. (2023) focused on the negative impacts on innovation, which they econometrically estimated as being relatively large: "the average targeted firm loses around $31 million in patent value per year, relative to the full-sample average annual production of $155 million". Aina et al. (2023) mentioned that data breaches and IP theft can lead to significant loss of revenue for people, businesses and the government. This type of crime could affect the expansion of companies and hinder their competitiveness, which could, in turn, impact the economic growth at the macro level.

Palmer (2021)[5] suggested that, beyond direct financial costs, cyber crime also imposes severe reputational costs on compromised victims. These damages can have a negative impact on investments, further contributing to revenue losses. Palmer also reported a Centrify and Ponemon Institute (2018) study, which found that 61% of managers from 43 companies reported reputational damage as the most significant cost of cyber crime.

Sector experts suggested additional channels of impact, such as challenges related to legal resources and identifying perpetrators. Unlike traditional IP and knowledge assets theft, IP and knowledge assets theft resulting from a cyber attack is often harder to detect and prosecute because stolen innovations in the form of trade secrets or confidential processes are difficult to track when misused by competitors. Furthermore, sector experts suggested that another potential impact of IP and knowledge assets theft due to cyber attacks could be bankruptcy.

[5] Palmer, K. "The Aggregate Impact of Cybercrime on Economic and Geostrategic Security". In Akdemir, Lawless and Turksen (2021). Cybercrime in action, An International Approach to Cybercrime.

Quantitative estimates of impacts on businesses

Quantitative estimates of the impact of IP and knowledge assets theft on businesses are scarce, with very few identified in the literature. This applies to both estimates at the level of specific businesses and at the economy-wide level.

At the level of individual businesses, there are few cases where estimated impacts could be derived from damages sought in court cases or the loss of company value following known instances of IP and knowledge assets theft (whether via a cyber attack or not), mostly from US examples.

For example, Proofpoint (n.d.) cited Facebook's 7% loss in share value after the Cambridge Analytica data breach as a proxy for the impact of when "a brand is perceived as not taking adequate measures to protect its intellectual property, it may lose the trust of its customers, investors, and stakeholders". Academic studies also provide insights into the financial effects of breaches. For instance, Campbell et al. (2003) found that breaches involving unauthorised access to confidential data often lead to significant negative market reactions. Similarly, Du et al. (2024) highlighted that breaches involving larger volumes of sensitive data, such as high-profile cases, lead to more pronounced drops in stock prices.

Searle and Vivian (2021) suggested that the financial impact of IP theft on firms is often smaller than anticipated, with most cases not resulting in abnormal returns. However, there are some notable case studies where the impact is substantial. Sector experts highlighted that UK cases of IP theft are harder to track than US cases due to differences in legal frameworks. In the UK, many instances fall under breach of contract rather than explicit IP laws, making them less publicly visible. Some notable examples are discussed as case studies in the report.

There are also a number of estimates that instead take a top-down approach, the most relevant of which is covered in the section below addressing RQ5.

Impacts on consumers

While most literature focuses on the impacts on businesses, fewer sources examine the effects on consumers. The following channels have been identified as potential negative impacts on consumers (Cabinet Office, 2011; F12.net, 2024):

1. **Product quality concerns**: In cases where IP and knowledge assets theft leads to counterfeit goods, consumers may suffer from inferior product quality.
2. **Market saturation**: Counterfeit products flooding the market can make it harder for consumers to access genuine products at competitive prices.
3. **Potential price increases**: As businesses invest in enhanced security measures or face financial losses due to IP and knowledge assets theft, these costs may be passed on to consumers in the form of higher prices.

However, these effects are not always straightforward, and the impact on consumers can vary depending on both the short-term and long-term perspectives.

In the short term, IP and knowledge assets theft may have some beneficial effects, such as lower prices for consumers. In some cases, counterfeit goods – especially in sectors like fashion – can satisfy status-signalling needs at lower price points, providing consumers with

more affordable options. Searle (2011) noted that in such cases, the target groups for genuine and counterfeit products rarely overlap, meaning that counterfeit goods may not cause significant harm to consumers.

However, in the long term, the consequences are more likely to be harmful. According to sector experts, if IP and knowledge assets theft undermines businesses' ability to protect their innovations, it may reduce their incentive to invest in future product development and differentiation. This can lead to less innovation and fewer high-quality products entering the market, ultimately harming consumers. While the evidence on whether IP protections foster investment is mixed, it is clear that over time, weakened IP protections could deter investment in innovation (Williams, 2017).

The effects of IP and knowledge assets theft on consumers are also dependent on various factors, such as market structure and concentration. For example, in highly competitive or fragmented markets, counterfeit goods might drive innovation as firms race to differentiate themselves from low-cost imitators. Gmeiner (2019) highlighted how theft in some market structures can fuel innovation as companies compete to outpace counterfeiters. Similarly, Qian (2008) argued that counterfeit entry can spur innovation by increasing competitive pressure and speeding up the pace of innovation races.

Difference from incidents not associated with cyber attacks

There is limited research comparing the costs of IP and knowledge assets theft linked to cyber attacks versus other forms of IP and knowledge assets theft. Deloitte (2016) identified multiple cost categories for IP theft, most of which apply regardless of whether a cyber attack is involved. The main exception is cyber security improvements, which are specific to cyber-enabled incidents, although firms are still likely to incur costs for other preventative measures against non-cyber forms of IP theft.

The primary difference appears to be in prevalence, as cyber attacks are increasingly a leading cause of IP and knowledge assets theft, as further discussed in RQ2. Sector experts highlighted that cyber-enabled theft is often more difficult to detect and prosecute compared to traditional methods, as stolen innovations – particularly trade secrets – can be exploited without leaving clear evidence. Unlike physical theft or contract breaches, cyber theft allows for rapid replication and distribution, making recovery and legal action more challenging.

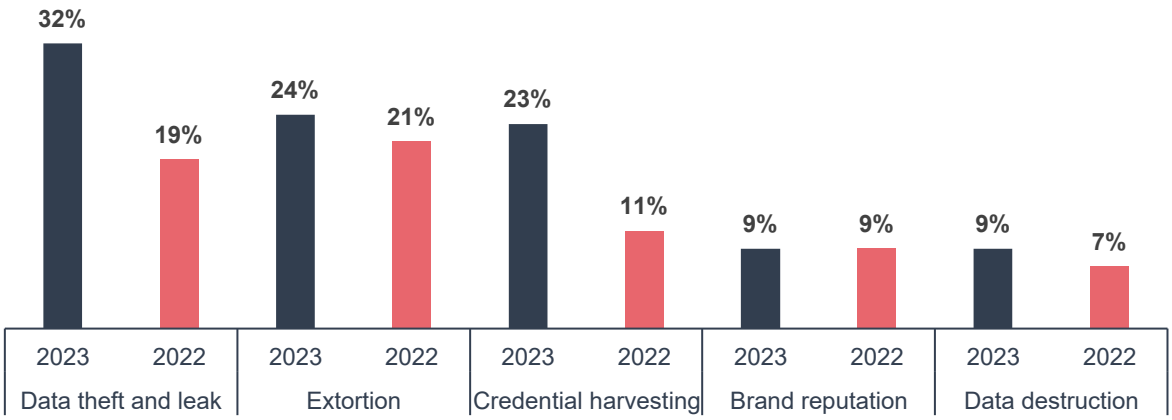
Sector experts also noted that the timing of thefts plays a key role. If cyber theft occurs at an early stage of innovation, before patents are secured, it can provide competitors with a significant advantage. In contrast, traditional IP theft more commonly involves infringing public IP, such as patents, where enforcement mechanisms are clearer.

Finally, sector experts emphasised differences in legal challenges. While non-cyber IP theft cases often fall under contract or trade secret laws, cyber-enabled IP theft frequently lacks direct legal precedents, especially in the UK, making it harder to pursue damages. The complexity of attributing cyber attacks further complicates enforcement, particularly when state-sponsored actors are involved.

RQ2. How frequently is IP stolen during a cyber attack?

We identified only two grey literature sources addressing this research question, one of which, conducted by DSIT, focuses on the UK context.

Figure 1. Prevalence of cyber crime types, 2022 and 2023



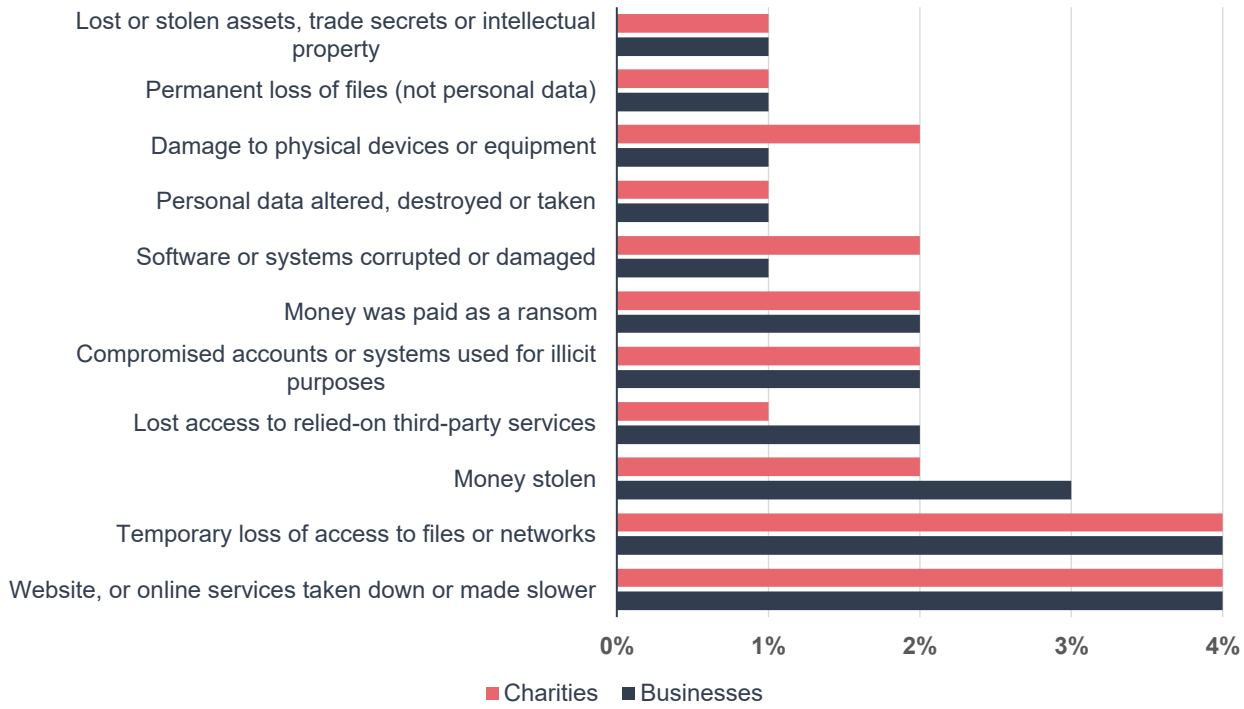
Source: IBM, X-Force Threat Intelligence Index 2024

IBM (2024) noted that globally, data theft is now the most common form of cyber attack on organisations. According to their 2023 data, it accounts for 32% of reported cyber incidents impacting companies, surpassing extortion-based attacks. Based on IBM data, Europe was the most targeted area for detected cyber attacks in general, with the UK being the most attacked country in Europe (accounting for 27% of detected cases). They note that, “Europe’s high use of cloud platforms may also result in a potentially larger attack surface compared to other regions, especially if attackers are able to obtain valid cloud accounts to gain initial access. In 30% of incidents, attackers used valid accounts, whether cloud, domain or local, to compromise European organizations.”

Narrowing the focus to IP and knowledge assets theft, the DSIT (2024) Cyber Security Breaches Survey noted that approximately half of businesses (50% of the 2,200 UK businesses surveyed) and around a third of charities (32% of the 1,000 UK charities surveyed) reported having experienced any kind of cyber security breach or attack in the last 12 months. Of these, approximately 13% indicated having a negative outcome as a result of the breach. The report mentioned that this relatively low proportion suggests that most of the cyber attacks have little impact. Additionally, the report identified that among the 13% that identified a negative consequence of the breach, fewer than 1% of businesses and charities indicated that the breach resulted in a “lost or stolen asset, trade secrets or intellectual property”. The following graph illustrates the reported frequency of negative outcomes resulting from data breaches in 2024.

However, the challenge in proving such incidents remains due to the secretive nature of cyber attacks and IP and knowledge assets theft.

Figure 2. Percentage of companies that had any of the following outcomes, among the organisations that have identified breaches or attacks in the last 12 months (2024)



Source: DSIT, Cyber security breaches survey 2024

RQ3. How many of these attacks come from state vs non-state actors?

Our review of publicly available information has led to limited estimates of the proportion of IP and knowledge assets theft through cyber attacks attributed to state vs non-state actors. We identified two grey literature papers and one monitoring database. One reason for the lack of quantitative estimates is the difficulty of attribution. As Tran (2018) notes, “State-sponsored cyber attacks are on the rise and show no signs of abating. Despite the threats posed by these attacks, the states responsible frequently escape with impunity because of the difficulty in attributing cyber-attacks to their source”.

Available evidence suggests that state-sponsored cyber operations have increased over time. Based on the Council on Foreign Relations’ Cyber Operations Tracker, Priyandita et al. (2022) reported that the number of documented state-sponsored cyber incidents rose from fewer than 40 between 2014 and 2016 to over 100 by 2020. According to sector experts, this increase may also be attributed to the fact that some major cyber security providers have begun publicly attributing cyber incidents to nation-states.

However, the distinction between state and non-state actors is becoming increasingly blurred. The 2024 Cyber Security Report by Check Point (2024) highlighted that some state-developed cyber tools are accessible to private actors, and certain non-state groups may operate with state approval or indirect sponsorship. This complicates efforts to quantify the exact share of attacks attributed to each group. According to sector experts, non-state actors are also increasingly using "living-off-the-land" techniques, which involve exploiting existing system utilities (e.g. those within MS Windows).

While non-state actors are also highly active in cyber crime, they typically operate with different motives, focusing on financial gain rather than economic cyber espionage for national advantage. However, it is also important to note that, according to sector experts, profit-making could also be a significant motive for some state actors. Due to a lack of comparative data on non-state actor involvement, it remains difficult to assess their role relative to state-sponsored attacks.

RQ4. How is this stolen IP used?

We identified only two grey literature documents addressing this question. Stolen IP, primarily sought for financial gain, could be used through several routes (Deloitte, 2016; TERAMIND, 2024):

1. Using stolen IP to replicate another company's offerings, which can be with or without undercutting on price, given that the lower cost of stolen IP relative to IP generated via in-house innovation or R&D. This could involve a state actor assisting or acting on behalf of domestic companies. Additionally, stolen IP could be used not just for replication but also to enhance internal processes, improve efficiency, and gain a competitive market advantage. Competitors, both domestically and internationally, may target IP for this purpose.
2. Selling the stolen IP to a company that can benefit from point 1 above.
3. Sabotage or misinformation: Stolen IP can be manipulated to damage the original creator's credibility or disrupt operations. For example, North Korean hackers have targeted the defence and nuclear sectors to advance their military and nuclear goals (The Times, 2024).

Alternatively, there can be non-financial motivations, such as cyber warfare by state actors.

RQ5. What is an estimated range for the value of IP that has been stolen from cyber attacks in the UK?

We have only identified one attempt to quantitatively estimate the value of IP that has been stolen from cyber attacks in the UK, and that study is now over a decade old. Cabinet Office (2011) estimated that the cost to the UK of IP stolen through cyber attacks was £9.2 billion per annum out of a total annual cost of cyber crime of £27 billion per annum (both based on 2010 data). This was based on applying the probability of IP theft from cyber attacks to annual UK values of both total R&D spend and also an estimate of cash flows attributable to IP.

Of this £9.2 billion estimated total loss, four sectors were estimated to lose over £1 billion a year. In descending order, these sectors were (a) pharmaceuticals and biotech, (b) electronic and electrical equipment, (c) software and computer services, and (d) chemicals.

However, according to sector experts, it is essential to distinguish between the value of stolen IP and the cost of its theft. The financial impact of IP theft depends on how the stolen IP is used. For example, if an attacker steals IP but does not exploit it (or if the data is deleted rather than monetised), the IP still holds intrinsic value, but the direct cost to the original owner may be minimal. This distinction is crucial when interpreting past estimates and understanding the broader economic implications of IP theft.

RQ6. What is the best methodology to model the cost of IP theft and knowledge assets facilitated by cyber attacks?

Among the academic and grey literature sources reviewed in this section, a number of methodologies were employed to attempt to produce empirical estimates of the cost of IP and knowledge assets theft through cyber attacks:

1. **Case study approaches**: Under this methodology, specific known cases of IP and knowledge assets theft through cyber attacks are studied for specific businesses to estimate the costs for individual businesses, which can then be used to estimate economy-wide impacts based on the number of businesses affected. For example, Deloitte (2016) followed a case study approach.
2. **Econometric analysis**: Curti et al. (2023) used firm-level data to estimate the relationship between firms targeted by IP theft and their innovation outcomes, e.g. R&D spend and patent registration. Relatedly, Ettredge et al. (2018) used firm-level data to estimate the impact of firms holding trade secrets and their likely targeting for theft of corporate data.
3. **Stock market reaction studies**: Another widely used approach for estimating the financial impact of IP and knowledge assets theft due to a cyber attack is to analyse how stock prices react to publicly disclosed incidents. This method provides a market-based estimate of cost, capturing investor perceptions of financial damage. Campbell et al. (2003) found that markets tend to react negatively to security breaches, particularly those involving sensitive corporate information. More recently, Du et al. (2024) found that firms experiencing high-profile breaches involving significant IP losses tend to suffer larger declines in share value.
4. **Top-down approaches**: The Cabinet Office (2011) followed a top-down approach to estimate the UK-wide impact of IP theft through cyber attacks. The Cabinet Office applied the probability of IP theft from cyber attacks to annual UK values of both total R&D spend and an estimate of cash flows attributable to IP.

Econometric analysis of the impact of cyber attacks

The impact of cyber attacks on firms has been the subject of various econometric studies, which seek to quantify both immediate and long-term consequences on firm-level performance indicators, such as performance, productivity and operational efficiency. Below, we discuss some key findings from a relevant study, highlighting what was estimated and the conclusions drawn.

A study by Kamiya et al. (2018) investigated the characteristics of firms more prone to cyber attacks and their post-attack financial performance. The study estimated the impact of attacks on firm performance, risk, and corporate policies by conducting a difference-in-differences analysis on a sample of firms three years before and three years after a cyber attack. Only cyber attacks resulting in financial information loss were included. Propensity-score matching was used to pair treatment firms (those experiencing a cyber attack) with control firms (those

not attacked) based on firm size, stock performance, volatility, leverage, and institutional block holders. Industry-year and firm fixed effects were included for variability over time and across industries.

$$\mathrm{OP_{it}} = \alpha + \beta(\mathrm{Post_{it}} \times \mathrm{CyberAttack_{it}}) + \gamma_t + \omega_i + \varepsilon_{it}$$

where:

- OP_{it} represents the operating performance (measured as Return on Assets (ROA), Return on Equity (ROE), cash flow/assets, and sales growth) for firm i at time t,
- $Post_{it}$ representing the post-attack years (year t, t+1, t+2),
- $CyberAttack_{it}$ is a binary variable indicating whether the firm experienced a cyber attack,
- γ_t indicates the industry-year fixed effects,
- ω_i represents the firm fixed effects, and
- ε_{it} is the error term.

The findings indicated that there was no significant effect on ROA, ROE, or cash flow-to-assets, but sales growth declined significantly, reflecting disruptions in revenue generation. Subsample analysis revealed that large firms experienced significant decreases in ROA, cash flow-to-assets, and sales growth, with the latter dropping by 3.4 percentage points compared to an 8% pre-attack average. Industry-specific results show that firms in durable goods sectors suffer notable declines in ROA and cash flow, likely due to the high costs of supply chain disruptions, while retail firms experience a 5.4 percentage point decline in sales growth, emphasising the vulnerability of customer-facing industries. These findings highlighted the heterogeneity of cyber attack impacts across firm sizes and industries, underlining the need for targeted cyber security strategies.

Econometric results

This chapter discusses the findings from our quantitative analysis, which includes both descriptive statistics (to understand the prevalence and characteristics of IP and knowledge assets theft from cyber attacks) and regression modelling results.

Key findings:

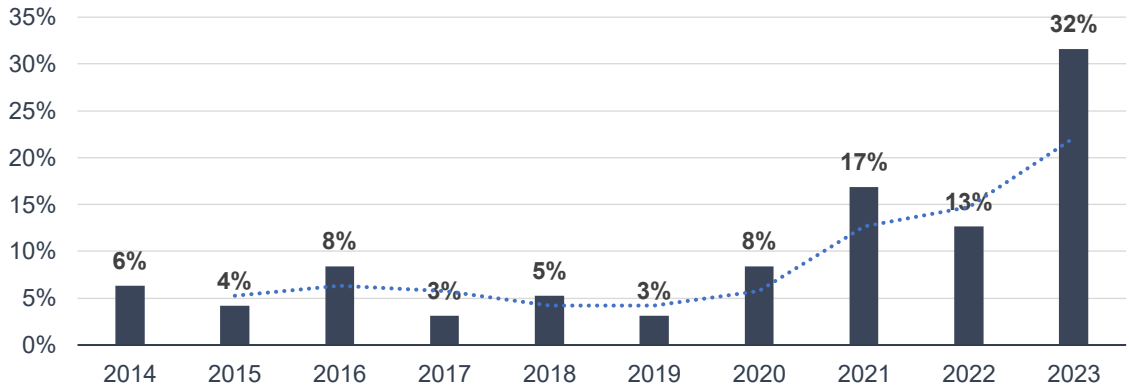
- Across all UK firms, the econometric analysis suggests that, on average, a cyber attack seeking IP and knowledge assets theft is associated with around a 2% fall in firm-level activity in the year of the attack, although this was not statistically significant.
- For SMEs, a cyber attack resulted in a 16% decline in sales growth, which is much more economically significant than the all-firm result and statistically significant, i.e. it is more statistically robust evidence of the extent of the impact. The estimated fall in profits, specifically Profits Before Interest and Tax, was similar to the loss of sales, suggesting that firms achieved cost-cutting measures in line with their fall in sales. The overall impact is best interpreted as a proportionate loss of economic activity.
- The increasing frequency of cyber attacks in our sample (whether driven by a rise in actual incidents, better reporting, or a combination of both) highlights the growing threat to businesses, especially SMEs, i.e. this is an issue of growing significance.

Summary statistics

Our final sample consisted of 3,570 unique UK companies. Of these, 78 unique companies (2% of the sample) experienced a cyber attack resulting in a ‘Data – Malicious Breach’ during the period of interest. Some of these firms were attacked multiple times, resulting in a total of 95 recorded cases of ‘Data – Malicious Breach’. On average, these 78 firms experienced 1.2 cyber attacks, with a maximum of seven reported attacks.

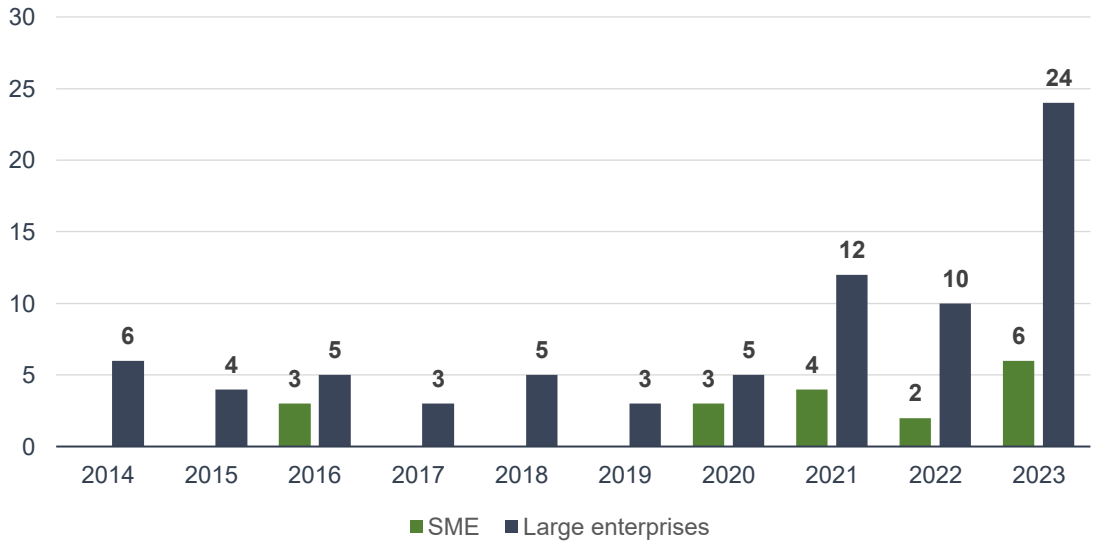
The following graph shows how these 95 cases are distributed over the period of analysis. As shown, the percentage of cases increases over time, with the highest proportion (32%) occurring in 2023. This trend may be due to a rise in cyber attacks over time, improved reporting of such incidents, or a combination of both. While our current data sample is relatively small, the observed growing number of recorded cyber attacks suggests that future iterations of the Zywave, Inc. dataset could capture more incidents. Repeating this analysis in the future would expand the available sample, allowing us to refine our understanding of the economic impact of IP and knowledge assets theft and provide valuable insights into the ongoing escalation of cyber attacks.

Figure 3. Percentage of cyber attack cases by year in our sample (n = 95)



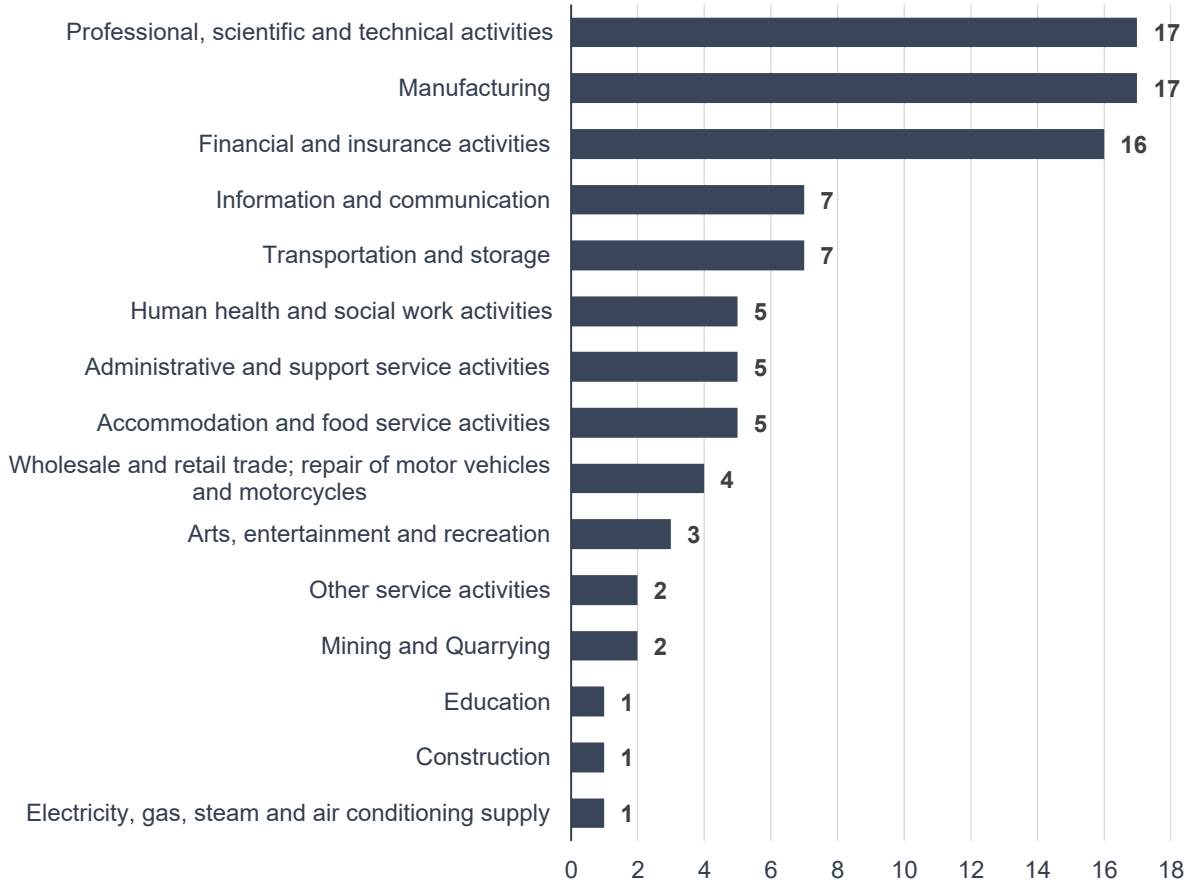
Using the Government Commercial Function (2023) definition of Small to Medium-sized Enterprises (SMEs), which classifies firms with a turnover less than £44m as SMEs, we identified the following: (i) 18 cyber attack cases affected 18 unique SMEs (each SME experienced 1 attack) and (ii) 77 cyber attack cases affected 60 unique Large Enterprises. The graph below shows the distribution of these cyber attack cases over the period of interest.

Figure 4. Number of cyber attack cases by year in our sample (n = 95), by type of company



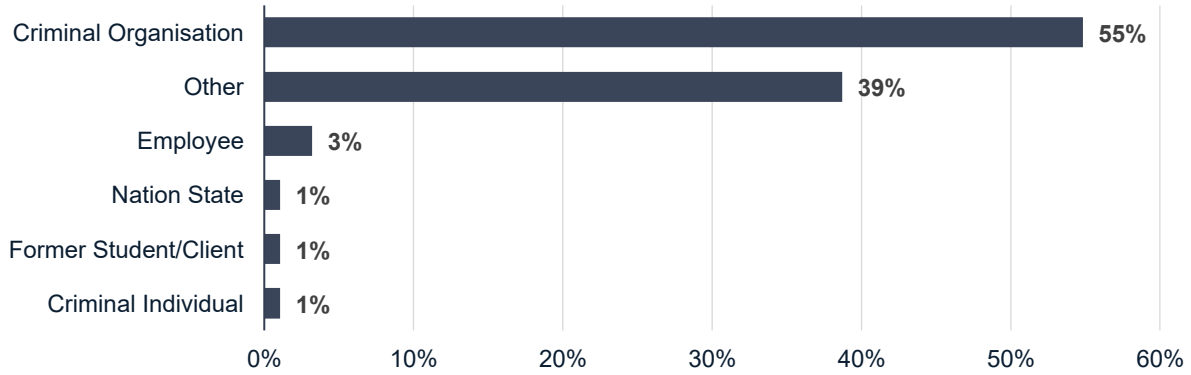
Additionally, the FAME database allows categorising of companies using their primary Standard Industrial Classification (SIC) codes. We grouped firms at the highest level (sections) based on the Companies House classification. Between 2014 and 2023, three sectors were the most affected by cyber attacks in our sample: Professional, scientific and technical activities (17 cases); Manufacturing (17 cases) and Financial and insurance activities (16 cases).

Figure 5. Number of cyber attack cases by industry in our sample (n = 93), all years



The Zywave, Inc. database categorises cyber attacks according to the type of actor responsible. In our sample, 93 incidents had an identifiable perpetrator. The figure below shows the distribution of cyber attacks by actor type. As shown, the majority (55%) were attributed to criminal organisations, while only 1% were linked to nation-states. However, it is important to note that the "other" category may include state actors, suggesting that the proportion of nation-state-led cyber attacks could be higher than 1%.

Figure 6. Cyber attack cases by type of actor (n = 93), all years



Regression results

To estimate the impact of a cyber attack on firms, we used the following model:

$$\Delta \ln(\text{sales})_{it} = \beta_1 * \text{CyberattackDummy}_{it} + \alpha_i + \gamma_t + \epsilon_{it}$$

Where:

- $\Delta \ln(sales)_{it}$: First difference of the natural logarithm of sales for firm i at time t
- $CyberattackDummy_{it}$: Dummy variable equal to 1 if a cyber attack occurred for firm i at time t, 0 otherwise.
- α_i: Firm fixed effects, capturing time-invariant characteristics of each firm
- γ_t: Year-fixed effects, capturing factors that vary by year but are the same for all firms in a given year.
- ϵ_{it}: error term

The goal of this model is to estimate the effect of IP and knowledge assets theft as a result of a cyber attack on firms' sales growth. Fixed effects are included to control for unobserved heterogeneity between firms. To assess robustness, we ran specifications both with and without year fixed effects. Additionally, we corrected for potential heteroskedasticity by using robust standard errors. This approach is useful in the context of a fixed effects model, because the variability of the error term may be different across firms over the period of interest. By implementing robust standard errors, we mitigate the risk of inefficient standard errors and improve the reliability of our statistical inferences regarding the impact of cyber attacks.

Our results suggest that there is an indication that firms having their IP and knowledge assets stolen as a result of a cyber attack could see a 2% decline in sales growth within the same year. This effect is not statistically significant, meaning that we cannot reject the hypothesis that IP and knowledge assets theft as a result of a cyber attack has no impact on sales growth. Nevertheless, given that existing literature suggests a small but measurable effect (Searle and Vivian, 2021), our estimate remains the best available based on our data. In this sense, we consider this figure a reasonable approximation of the impact of cyber attacks on firm performance.

We also applied the same fixed effects model to examine changes in profitability, using percentage changes in EBIT as the dependent variable.[6] The results indicated a positive change of 6.5% for the full sample, while again not being statistically significant. We interpret this as a scaling down of the overall business without a loss in profitability, suggesting that costs were reduced at least as rapidly as sales declined. Alternatively, it may indicate an increase in efficiency that helped cut costs. We explain this relationship in the box below.

[6] We used the first difference of the natural logarithm of EBIT as dependent variable.

Case 1: Overall sample - Decreasing sales, constant or increasing EBIT

The relationship between sales and EBIT can be expressed as:

$$\text{EBIT} \approx \text{Sales} - (\text{Fixed and variable costs})$$

In this case, although sales are decreasing, EBIT is either increasing or remaining constant. As the equation suggests, companies may be actively reducing costs – disproportionately to the decline in sales – in order to maintain profitability.

We conducted a sub-sample analysis to determine whether the effects of cyber attacks differ based on firm size. For Large Enterprises, the results are similar to the full sample, with an impact of approximately 2% in the year of a cyber attack, but this effect remains statistically non-significant.

However, for SMEs, the effect is both larger and statistically significant. Specifically, among SMEs, a cyber attack leads to an average decrease of 16% in sales growth within the year, with this result being statistically significant at the 1% level (p = 0.009). Regarding EBIT change, the impact of IP and knowledge assets theft was a -17% change (not statistically significant), showing that EBIT is falling as quickly as sales. This aligns with Intellectual Property Office (2021) report, which notes that the loss of a trade secret can be particularly devastating for small firms, which may have few alternative innovations to rely on.

Case 2: SME sample - Decreasing sales, Decreasing EBIT

As seen in case 1, the relationship between sales and EBIT can be expressed as:

$$EBIT \approx Sales - (Fixed\ and\ variable\ costs)$$

For SMEs, both sales and EBIT are declining. This indicates that the drop in profits closely mirrors the decline in sales, suggesting that firms have implemented cost-cutting measures proportionate to their revenue losses.

Table 1. Fixed effects results on sales growth

Variable: $\Delta \ln(sales)$ -	Full sample (1)	Full sample (2)	LE sample (1)	LE sample (2)	SME sample (1)	SME sample (2)
Cyber attack Dummy	-0.022	-0.023	-0.023	-0.018	-0.164***	-0.160***
p- value (robust standard errors)	0.625	0.583	0.550	0.626	0.009	0.003
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	No	Yes	No	Yes	No	Yes
Within R-squared	0.00	0.03	0.00	0.03	0.00	0.08
Observations	32,130	32,130	7,290	7,290	18,261	18,261
Number of firms	3,570	3,570	810	810	2,029	2,029

Note: *** indicates an estimate statistically significant from zero at the 1% level.

Note: (1) Model without fixed effects by year, (2) Model including year fixed effects.

We also used the same fixed effects model with a lagged variable for cyber attacks to see if a cyber attack from the previous year has a delayed effect on sales growth.[7] This helped us consider medium- to long-term impacts, as some effects may take time to be fully realised. Our results indicated that firms seem to recover from the negative financial shock of a cyber attack in the following year, rather than experiencing long-term sales losses. This suggests that cyber attacks tend to have a temporary financial impact. While the immediate consequences could be severe, the findings also highlight that firms can rebound from such events.

Table 2. Lagged fixed effects model

Variable: $\Delta \ln(sales)$	**Full sample**	**Full sample**	**LE sample**	**LE sample**	**SME sample**	**SME sample**
-	**(1)**	**(2)**	**(1)**	**(2)**	**(1)**	**(2)**
Cyber attack Dummy	-0.023	-0.032	-0.029	-0.028	-0.142**	-0.146***
p- value (robust standard errors)	0.613	0.453	0.503	0.496	0.019	0.007
Lagged Cyber attack	0.050	0.013	0.041	0.028	0.140	0.074
p- value (robust standard errors)	0.315	0.788	0.330	0.473	0.258	0.558
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	No	Yes	No	Yes	No	Yes
Within R-squared	0.06	0.09	0.06	0.09	0.03	0.12
Observations	28,560	28,560	6,480	6,480	16,232	16,232
Number of firms	3,570	3,570	810	810	2,029	2,029

Note: ** indicates an estimate statistically significant from zero at the 5% level.

Note: (1) Model without fixed effects by year, (2) Model including year fixed effects.

Note: This model includes the lag of the first difference in sales as an independent variable, which reduces the number of usable observations compared to the unlagged version. To compute this regression, the model needs three consecutive years of data for each panel: (i) two years are needed to calculate the first difference in sales (e.g. the change from year t–1 to t), and (ii) one additional earlier year is required to compute the lag of that first difference (i.e. the change from year t–2 to t–1). As a result, this regression can only be run starting from year 3 onwards, while the previous model can start from year 2.

We believe our estimates are not likely to be affected by key econometric issues that could compromise causal interpretation. Specifically:

- **Reverse causality:** For causality to primarily be reverse causality, it would need to be the case that cyber attacks were specifically targeting SMEs with declining sales. This

[7] We used the first difference of the natural logarithm of sales as dependent variable.

is highly unlikely because there would be more benefit in attacking growing companies. Furthermore, it is relatively unlikely that cyber attacks could systematically target SMEs with falling sales, as this would be very difficult to predict.

- **Omitted variables:** This issue arises when a relevant variable is not included in the econometric model, leading to biased estimates if the omitted variable is correlated with both cyber attacks and firm performance. In our case, one possible factor could be a firm's internal IT policies, which might influence both the likelihood of experiencing a cyber attack and serve as an indicator of business performance. However, factors like IT policies are relatively stable over time within a firm. Since our model includes firm and year-fixed effects, we effectively control for time-invariant characteristics, reducing the risk of omitted variable bias. In the absence of any identified omitted variables of concern, it is unlikely that this is a significant issue.

Key findings

For the analysis across all UK firms, the estimated impact of a cyber attack seeking IP and knowledge assets theft was not statistically significant, but nonetheless, there was an indication of an average loss of economic activity (i.e. reduction in sales growth) of around 2% in the year of the attack.[8] This finding aligns with Searle and Vivian (2021), who also suggested that the impact of trade secret breaches on firms is small. For EBIT change, the results showed a positive change of 6.5% for the full sample, though it was not statistically significant. We interpret this as a scaling down of the overall business without a loss of profitability, meaning companies reduced costs disproportionately to the decline in sales to maintain profitability.

Our analysis showed that among SMEs, a cyber attack leads to an average decrease of 16% in sales growth within the year, a statistically significant effect at the 1% level. Regarding EBIT change, the impact of IP and knowledge assets theft was a -17% change (not statistically significant), indicating that EBIT is falling as rapidly as sales. This suggests that the primary consequence of IP and knowledge assets theft from cyber attacks is a loss of economic activity rather than the direct costs of prevention or repair. The results suggest that SMEs are particularly vulnerable to cyber attacks. This could be because SMEs are increasingly reliant on digital technologies and often lack the resources to effectively invest in robust cyber security measures (Cartwright et al., 2023). As evidenced by a 2023 survey, 19% of SMEs reported that a cyber attack causing damages of £4,200 could lead to bankruptcy, while an additional 50% indicated that they would need to lay off staff or deplete their financial reserves to cope with the financial fallout (WPI Strategy, 2023). This underscores the vulnerability of small businesses, which face disproportionate financial consequences when targeted by cyber criminals.

[8] Although the result is not statistically significant, we consider it a credible estimate of the impact of cyber attacks resulting in IP and knowledge assets theft on firms. This is based on three considerations: (i) the coefficient is in the expected direction (negative); (ii) the findings are consistent with existing literature, which also reports small but significant effects; and (iii) as noted in the results section, we believe our estimates are unaffected by the main sources of bias that typically compromise causal inference in regression analysis (omitted variable and reverse causality). However, given the small number of treated cases, that is, firms which faced a successful cyber attack resulting in the theft of IP or knowledge assets, the lack of statistical significance is likely due to limited statistical power rather than the absence of an effect.

However, even for SMEs, our results indicate that cyber attacks leading to IP and knowledge assets theft in the previous year could be followed by a strong rebound in the subsequent year. SMEs lose around 14% in the year of the attack, but could recover it the following year. This suggests that SMEs tend to recover from the negative financial shock of a cyber attack within a year, rather than experiencing long-term sales losses. This could imply that IP and knowledge assets theft from a cyber attack might not have a lasting impact. Another possible explanation, according to sector experts, is that the market value of stolen IP and knowledge assets is time-dependent. As time passes, the stolen IP and knowledge assets lose value because they do not include subsequent innovations or developments made by the victim firm. This means that while the initial shock of theft is significant, firms may regain competitive advantage through continued R&D and adaptation.

Still, the frequency of the cyber attacks recorded on the Zywave, Inc. dataset is on the rise. In our sample, the number of recorded cases increased by an average of 47% from 2014 to 2023, with a 150% rise in 2022 and 2023, illustrating a growing trend in the prevalence of the recorded attacks. This trend suggests that the threat landscape for businesses, especially SMEs, continues to grow rapidly, with increasing numbers of firms falling victim to cyber crime. Replicating this analysis in future years will provide valuable insights into the continuing escalation of cyber attacks and improve our ability to track and identify new cases. Understanding these trends is essential for developing better strategies to mitigate the risks and strengthen the cyber security posture of businesses, particularly those that are most vulnerable.

Limitations

While our analysis provides valuable insights into the impact of IP and knowledge assets theft due to cyber attacks on UK firms, some limitations should be considered. First, the relatively small number of cyber attack cases identified in our sample (95 total cases), with only 18 cases affecting SMEs, may limit the robustness of our findings. Our econometric results are based on a relatively small subset of affected firms compared to the larger pool of firms that did not experience (or did not report experiencing) a cyber attack.

It is important to note that the frequency of cyber attacks has been accelerating (or the frequency of reporting such incidents, or both), with a significant rise in cases in recent years. This suggests that the number of attacks – and the data available for analysis – will likely continue to increase. Future research, especially as the Zywave, Inc. database expands and more cyber attack cases are recorded, could enhance the accuracy and reliability of these estimates, helping track this growing trend.

Another limitation is that we cannot be certain about the proportion of successful versus unsuccessful cyber attacks in the Zywave, Inc. dataset. While it is likely that most of the cases recorded were successful in achieving IP and knowledge assets theft, we do not know the exact breakdown between successful and unsuccessful attacks. We have taken this uncertainty into account, particularly when estimating the economy-wide impacts later in the report.

Furthermore, for our research, we used the Zywave, Inc. data, which includes cases categorised as “Data – Malicious Breach.” This label refers to situations where personal confidential information or digital assets have been, or are at risk of being, exposed or stolen

by unauthorised internal or external actors (Shevchenko et al., 2023). However, this category may not exclusively cover IP and knowledge assets theft, and it could also include other types of data that do not necessarily align with the definition of IP and knowledge assets. In some cases, the descriptions do not clearly specify the stolen asset, making it difficult to determine whether it involved the assets of interest.

Another limitation is that, to estimate the percentage change in sales resulting from a cyber attack, our sample includes only companies that survived the attack or showed continuous operations until at least 2023. This means our analysis does not account for firms that may have gone bankrupt as a result of the attack, which may underestimate our results.[9]

Additionally, our results suggest that the effect of a cyber attack on sales growth appears to be higher for SMEs. However, SMEs present unique challenges when assessing the impact of IP and knowledge assets theft due to a cyber attack. These businesses are generally harder to track due to their lower reporting requirements compared to larger firms (The UK Government, n.d.). SMEs tend not to be publicly listed, meaning they are not subject to the same disclosure obligations as larger firms. Moreover, SMEs often generate limited news coverage, further complicating efforts to monitor and identify affected companies (DSIT, 2024; Reuters, 2024; The UK Government, n.d.). This information gap makes it more difficult to capture the full extent of the impact on small businesses. Furthermore, the timing of the impact is hard to pinpoint, and lags between the incident and any observable financial impact could add to the complexity of the analysis.

Additionally, there are jurisdictional challenges in the UK regarding how IP theft is treated under the law, which could further complicate the identification and classification of cases. For example, trade secrets in the UK are not as explicitly codified as they are in the US; instead, they fall under tort and contract law. This difference means that cases of IP theft in the UK may not be classified in the same way as they would be in the US, potentially leading to underreporting or misclassification. The lack of a clear regulatory framework further complicates the identification and classification of IP theft cases. Additionally, cases that might involve IP theft in the UK could be categorised under breach of contract rather than within a dedicated IP regime.

[9] According to sector experts, bankruptcy is a potential consequence of a severe cyber attack.

Case studies

To provide context for our findings, we developed a series of case studies to show how IP and knowledge assets theft through cyber crime can affect businesses. Information about firms experiencing the problem, particularly concerning SMEs, was found to be limited. SMEs typically tend to generate relatively little news flow, rarely produce long-form annual reports and often do not publish detailed financial accounts (DSIT, 2024; Reuters, 2024; The UK Government, n.d.). As a result, publicly known cases of affected SMEs are relatively scarce and likely represent only the tip of the iceberg. In this sense, for the case studies, we have used information available in Zywave, Inc. data, FAME and data shared by our partners. All examples have been anonymised, except for Case Study 2, which is the well-documented Sinovel vs. AMSC case. This case is frequently cited in the literature.

Overall, the case study analysis aligned with our econometric findings: for most Large Enterprises in our sample, cyber attacks had no significant impact on revenue. In fact, many of these companies continued to experience revenue growth despite the incidents. However, smaller companies have generally experienced declines in both sales and profits (again using EBIT as a profits definition as with the previous chapter). Of the 95 identified incidents, 89 occurred after 2014, meaning financial data from the previous year is available to assess the impact of the cyber attack on sales and profits. Among these 89 cases, around 80% reported an increase in either sales or profits following the cyber attack, indicating that many continued to grow despite the attack.

Nonetheless, some IP and knowledge assets theft cases could pose an existential threat to companies, particularly smaller companies that rely on a small range of valuable IP for the vast majority of their revenues (Intellectual Property Office, 2021). This is particularly likely to be a problem when stolen IP is used by larger firms to create rival products that can undercut prices or outperform smaller companies in marketing and post-sales support. An example of this is the case of a small UK company operating in the manufacturing sector that suffered IP theft in 2008, described in the case study below.

Case study 1

In the late 2000s, a small private UK manufacturing company fell victim to IP theft by a large US firm. The US firm began replicating the UK company's technology and selling it without permission. As a result, the UK company was forced to make the majority of its workforce redundant while pursuing compensation through the US courts. The legal battle ended in the UK firm's favour, resulting in an eight-figure damages award.

Due to its private status, media coverage of the case has been limited, with most available information coming from publicly accessible court documents. The company is still in operation, and given its small size, it is likely that it would not have been able to continue without the compensation awarded by the court.

Another way in which stolen IP can be exploited is by integrating the stolen innovation into a company's internal operations rather than purchasing the legitimate product. This practice could significantly impact the victim company's revenue and future cash flow, even if no rival products are directly introduced to the market. The following case study illustrates this scenario:

Case study 2

In 2018, Sinovel Wind Group, a Chinese company that produces and exports wind turbines, was convicted of stealing trade secrets from AMSC, a US-based firm, in 2011. During the trial, it was proven that Sinovel stole AMSC's technology in order to produce its own turbines using the stolen IP. According to evidence presented during the trial, because of the theft, AMSC lost more than $1 billion in market value and almost 700 jobs, approximately half its global workforce.

Following the trial, a US Court imposed the maximum statutory fine of $1.5 million on Sinovel Wind Group LLC. The Court also confirmed that the parties had agreed on a restitution amount, and ordered a year of probation period until Sinovel had paid the full amount. As part of this agreement, Sinovel paid $32.5 million to AMSC and committed to pay an additional $25 million within the probation period. AMSC's market value has never recovered to the levels it was at prior to 2011.

As seen in the econometric results and reported by Intellectual Property Office (2021), IP theft and cyber crime disproportionately affect SMEs. Online cases involving these types of companies were challenging to locate. However, using the Zywave, Inc. data and FAME database, we identified cases in sectors such as manufacturing, arts, entertainment and recreation, and accommodation and food service.

In many instances, profits declined more sharply than sales, suggesting that companies were unable to implement rapid cost-cutting measures. Despite this, sales tended to recover the following year. To explore this pattern, we focused on attacks that occurred before 2023, as financial data for the subsequent year was unavailable. While sales often rebounded after an attack, they typically did not return to pre-attack levels. The following examples further illustrate this.

Case study 3

An SME from the manufacturing sector suffered a cyber attack in 2021. This led to a sales decline of over 20% and a drop in EBIT of more than 90% that year. However, the company showed recovery in the following year, achieving over 10% sales growth and a 1,000% increase in EBIT. This recovery continued into 2023, with sales increasing again by approximately 10% and EBIT increasing by over 150%. This case illustrates the potential temporary impact of cyber attacks on companies, particularly SMEs. While the immediate financial consequences can be severe on their financial figures, it also demonstrates that SMEs can rebound from such events.

Case study 4

A similar case occurred with an SME in the arts, entertainment, and recreation sector that suffered a cyber attack in 2016. As a result, the company experienced a sales decline of over 40% and an EBIT drop of more than 100% that year. After the attack, the firm's financial figures showed significant fluctuations. In 2017, sales partly recovered, reaching 90% of their pre-cyber attack levels. This shows an example where much of the impact of a cyber attack appears to have been relatively short-lived.

However, not all firms experienced a sales rebound in the year following a cyber attack. In some cases, sales continued to decline, leading to further financial challenges and, in some instances, even causing the company to be reclassified from a Large Enterprise to an SME. This is evident in case study 5.

Case study 5

An SME in the accommodation and food service sector suffered a cyber attack in 2021. After years of steady growth in both sales and EBIT, the company experienced a sharp downturn, with sales falling by over 20% and EBIT by approximately 300% in the year of the attack. The financial impact worsened in the following year, with sales declining further by just under 20% again. Notably, the company's annual sales fell sufficiently to move from being classified as a Large Enterprise to an SME. This case underscores the severe and potentially lasting effects that a cyber attack can have on a business, not only in terms of financial performance but also in its market position.

Economy-wide impacts

An economy-wide model was developed to quantify the estimated economic impact of IP and knowledge assets theft resulting from cyber attacks on the UK GDP. The model assessed the proportion of GDP lost due to such incidents, distinguishing between their effects on SMEs and Large Enterprises. Data required for the model was obtained from our econometric estimates (detailed in Chapter 'Econometric results') and publicly available datasets.

The model applied the following equation to estimate this impact:

$$\%\ \text{of UK GDP lost in 2024} = \frac{(\text{Turnover loss from affected SMEs and Large Enterprises})}{\text{2024 UK GDP}}$$

Model mechanics

The percentage of the 2024 UK GDP that was lost because of IP and knowledge assets theft resulting from cyber attacks was calculated through the following steps:

- **Step 1 – estimating turnover loss:** We econometrically estimated the percentage reduction in sales from firms affected by IP and knowledge assets theft via cyber attacks, distinguishing between SMEs and Large Enterprises (see Chapter 'Econometric results').
- **Step 2 – calculating the UK market sector GDP in 2024:** For this study, we focused on the market sector GDP, which refers to the portion of the UK economy generated by private sector businesses, excluding the public sector. The proportion of GDP generated by the private sector was estimated using the ONS 2024 Supply and Use Tables. Private sector firms were found to account for 80.9% of GDP. This was then applied to the total UK GDP for 2024.
- **Step 3 – determining the prevalence of cyber IP and knowledge assets theft in UK firms:** While the best available data was used for our analysis, it is not entirely clear what proportion of cyber attacks recorded in the Zywave, Inc. dataset were successful in achieving IP and knowledge assets theft. As presented in the methodology section, Zywave, Inc. dataset contains publicly available information on cyber attacks, along with details on affected companies, attack types, and threat actors. To address this uncertainty, we present both lower- and upper-bound estimates of the prevalence of cyber IP and knowledge assets theft among UK firms.
    - **Lower bound**: Assuming that most cases recorded in the Zywave, Inc. dataset were successful attacks, we estimated the prevalence of IP and knowledge assets theft only among successful cyber attacks. According to the DSIT 2024 Cyber Security Breaches Survey and using Figure 4.6 from the survey, 50% of UK firms reported experiencing a cyber attack, 13% of those attacks were successful, and 7.7% of successful attacks resulted in IP and knowledge assets theft. Based on this, we estimate that approximately 0.5% of UK firms (7.7% × 13% × 50%) experienced a successful cyber attack that led to IP and knowledge assets theft.

- **Upper bound:** Since the Zywave, Inc. dataset does not distinguish between successful and unsuccessful attacks, we also considered a scenario in which the dataset represents all cyber attacks, regardless of success. To estimate the proportion of UK firms affected by cyber IP and knowledge assets theft in this broader context, we again relied on the DSIT 2024 Cyber Security Breaches Survey. We estimated that approximately 3.8% of UK firms experienced cyber IP and knowledge assets theft. This figure was derived from survey findings indicating that 1 in 13 (i.e. 7.7%) cases that experienced a cyber attack resulted in IP and knowledge assets theft. Since half (50%) of UK firms experienced a cyber attack, this equates to approximately 3.8% of all firms in the UK being affected by IP and knowledge assets theft (7.7% × 50%).

Note: Although it may seem counterintuitive, the lower bound estimate focuses only on successful attacks, while the upper bound includes both successful and unsuccessful attacks. One might expect that restricting the analysis to successful attacks would yield a higher prevalence. However, because we are estimating the prevalence across all UK firms – not just those attacked – it is necessary to adjust for the fact that many attacks are unsuccessful. The lower bound assumes the dataset includes only successful attacks, providing a conservative, more narrowly targeted estimate. The upper bound assumes the dataset captures all attacks, diluting the overall theft rate, as most attacks do not result in losses. This approach avoids overstating the prevalence by implicitly valuing unsuccessful attacks (which caused no theft) at zero.

- **Step 4 – estimating market sector GDP loss:** The estimated percentage decline in sales (Step 1) was multiplied by the 2024 UK market sector GDP (Step 2) and the estimated percentage of firms affected by IP and knowledge assets theft (Step 3), distinguishing between losses from SMEs and Large Enterprises.[10] Data from the Department for Business and Trade (2024) indicated that SMEs contributed 52% of UK turnover in 2024, which we use as an estimate of the SME contribution to market sector GVA.
- **Step 5 – calculating market sector GDP loss as a percentage of the total UK GDP:** The estimated lost turnover (Step 4) was divided by the total 2024 UK GDP to determine the proportion of GDP lost due to IP and knowledge assets theft through cyber attacks.

Results

Although our analysis relies on the best available data, the proportion of cyber attacks in the dataset that were successful in achieving IP and knowledge assets theft remains unclear. If all cyber attacks were successful, the lower-bound estimate suggests that IP and knowledge asset theft cost the UK economy £1 billion in 2024, or 0.04% of the total 2024 UK GDP. On the other hand, if the dataset captures all cyber attacks regardless of whether they were successful or not, the upper-bound estimate indicates losses of £8.5 billion, or 0.30% of the

[10] For this step, we use both significant and non-significant results from Table 1.

total 2024 UK GDP. Based on these estimates, this study concludes that cyber attacks targeting IP theft cost the UK economy between 0.04% and 0.30% of the total UK GDP annually.

Given the methodological considerations outlined earlier, the true economic impact is likely closer to this lower-bound estimate. This also aligns with evidence from the literature. For example, Ciuriak and Ptashkina (2021) suggested that the impact could be as low as 0.01% of GDP, although our estimates suggest that Ciuriak and Ptashkina (2021)'s figure is an under-estimate.

SMEs accounted for over 80% of this cost, with estimated impacts ranging from £0.9 billion (0.03% of the total UK GDP) to £7.5 billion (0.27% of GDP the total UK GDP). For Large Enterprises, the estimated impact ranges from £0.1 billion (under 0.01% of the total UK GDP) to £0.9 billion (0.03% of the total UK GDP).

Conclusions

IP and knowledge assets theft have become growing concerns in the digital age, with the rise of cyber attacks targeting businesses and potentially putting valuable assets at risk, which could have broader implications for innovation and the economy.

Our literature review highlighted several findings:

i. Although cyber attacks are becoming more frequent, the theft of IP and knowledge assets is still difficult to detect.
ii. When these thefts occur, businesses may face operational disruptions, damage to their reputation, and lost revenue, with potential for bankruptcy.
iii. Consumers may experience counterfeit goods, lower quality, and higher prices, but in the short term, counterfeit goods may offer cheaper alternatives.
iv. The frequency of state-sponsored cyber attacks has risen (Priyandita et al., 2022; Tran, 2018) but attribution remains difficult, as non-state actors often use state-developed tools or have indirect state support.
v. Stolen IP is typically used to replicate products and lower prices, for broader strategic purposes, such as sabotage or spreading misinformation.
vi. Current estimates of the value of stolen IP in the UK are outdated, with the latest assessment indicating annual losses of approximately £9 billion (Cabinet Office, 2011).

Our econometric analysis highlighted that, while the broader impact of IP and knowledge assets theft through a cyber attack on all firms was found to be relatively modest, some SMEs could experience significant negative impacts on their financial performance, underscoring their vulnerability to cyber crime. Specifically, our analysis indicated that, on average, a cyber attack resulting in IP and knowledge assets theft led to a 2% reduction[11] in firm-level activity across all firms in the year of the attack, compared to the growth they might have achieved in the absence of such an attack. This represents a relatively modest fall in economic activity. However, for SMEs, the impact was more pronounced, with a 16% decline in sales growth. This suggests that SMEs, which often have fewer resources to absorb such shocks, face a higher risk of substantial financial consequences from IP and knowledge assets theft. The fall in profits mirrored the decline in sales, suggesting that affected firms managed costs in line with revenue losses, indicating a proportional loss of economic activity. Furthermore, for both the full sample and the SME subset, our results indicate that firms seem to recover from the negative financial shock of a cyber attack in the following year, rather than facing long-term sales losses. This suggests that cyber attacks tend to have a temporary financial impact.

Case studies further supported these findings, illustrating that while most companies continued to grow post-attack, some could face severe consequences, particularly when the stolen IP and knowledge assets were crucial to their business model. For SMEs in particular, the theft could pose an existential threat, highlighting the varying degrees of impact depending on the nature of the business and its reliance on IP.

[11] This estimate is not statistically significant.

While the best available data was used for our analysis, it is not entirely clear what proportion of the cyber attacks in the dataset were successful in achieving IP and knowledge assets theft. Assuming all attacks were successful provides a lower-bound estimate of the economy-wide impact of IP and knowledge assets theft due to a cyber attack, suggesting that IP and knowledge assets theft cost the UK economy £1 billion in 2024, or 0.04% of the total UK GDP in 2024. Conversely, if the dataset captures all cyber attacks, regardless of success, the upper-bound estimate indicates that IP and knowledge assets theft from cyber attacks resulted in a loss of £8.5 billion in 2024, equivalent to 0.30% of the total 2024 UK GDP. Based on these estimates, this study concludes that cyber attacks attempting IP and knowledge assets theft cost the UK economy between 0.04% and 0.30% of the total UK GDP per year.

Although our analysis provides valuable insights into the impact of IP and knowledge assets theft due to cyber attacks on UK firms, it has some limitations. The small sample size (95 cases, with only 18 affecting SMEs) may limit the robustness of our findings. Nevertheless, cyber attacks recorded in the Zywave, Inc. dataset are becoming more frequent, with a 47% average increase in recorded cases from 2014 to 2023 and a sharp 150% rise between 2022 and 2023. This trend suggests either a growing prevalence of cyber crime, improved reporting, or both. While our current estimates provide an initial understanding, replicating this analysis in future years with a larger sample will help deepen our understanding of the evolving threat landscape and its broader economic impact. This will be essential for developing more effective strategies to mitigate risks and strengthen cyber security, particularly for businesses most vulnerable to these threats.

References

Aina, O., Adenuga, Y., BABATUNDE Kamaldeen, I., 2023. The Role Of Cybersecurity In Contemporary Technology: Evaluating The Effects Of Cyber- Attack On Progress In Modern Science.

Bielig, A., 2015. Intellectual property and economic development in Germany: empirical evidence for 1999–2009. Eur. J. Law Econ. 39, 607–622.

Cabinet Office, 2011. The cost of cyber crime.

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market*. J. Comput. Secur. 11, 431–448.

Cartwright, A., Cartwright, E., Edun, E.S., 2023. Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Comput. Secur. 131, 103288.

Check Point, 2024. Cyber Security Report 2024.

Ciuriak, D., Ptashkina, M., 2021. Quantifying Trade Secret Theft: Policy Implications.

Cloudflare, 2024. Shielding the Future: United Kingdom Cyber Threat Landscape.

Curti, F., Macchiavelli, M., Mihov, A., Pisciotta, K., 2023. Corporate Espionage and Innovation: Evidence from the Theft of Trade Secrets.

Deloitte, 2016. The hidden costs of an IP breach.

Department for Business and Trade, 2024. Business population estimates for the UK and regions 2024: statistical release.

DSIT, 2024. Cyber security breaches survey 2024.

Du, S., Gwebu, K., Wang, J., Yu, K., 2024. Differential Market Reaction to Data Security Breaches: A Screening Perspective. Commun. Assoc. Inf. Syst. 54, 376–401.

Ettredge, M., Guo, F., Li, Y., 2018. Trade secrets and cyber security breaches. J. Account. Public Policy, Special Issue on Cybersecurity and Accounting 37, 564–585.

EUIPO, 2021. Intellectual property rights and firm performance in the European Union.

F12.net, 2024. The Invisible Cyber Threat: Combating Intellectual Property Theft in Business.

Fang, L.H., Lerner, J., Wu, C., 2017. Intellectual Property Rights Protection, Ownership, and Innovation: Evidence from China. Rev. Financ. Stud. 30, 2446–2477.

Gmeiner, R., 2019. Innovation, Theft, and Market Structure. Atl. Econ. J. 47, 243–260.

IBM, 2024. IBM Security X-Force Threat Intelligence Index 2024.

Intellectual Property Office, 2023. From public research spend to innovation: the role of registered IP.

Intellectual Property Office, 2021. The economic and innovation impacts of trade secrets.

Intellectual Property Office, 2017. Hidden Value: A study of the UK IP valuation market.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R.M., 2018. What is the Impact of Successful Cyberattacks on Target Firms? National Bureau of Economic Research Working Paper 24409.

Neves, P.C., Afonso, O., Silva, D., Sochirca, E., 2021. The link between intellectual property rights, innovation, and growth: A meta-analysis. Econ. Model. 97, 196–209.

Palmer, K., 2021. The Aggregate Impact of Cybercrime on Economic and Geostrategic Security, in: Cybercrime in Action an International Approach to Cybercrime. Nobel Akademik Yayıncılık.

Priyandita, G., Hogeveen, B., Stevens, B., 2022. State-sponsored economic cyber-espionage for commercial purposes: tackling an invisible but persistent risk to prosperity.

Proofpoint, 2024. 2024 State of the Phish.

Proofpoint, n.d. What Is Intellectual Property Theft?

Qian, Y., 2008. Impacts of Entry by Counterfeiters.

Reuters, 2024. Britain plans to simplify reporting rules for small businesses. Reuters.

Searle, N., 2011. Status Signaling and Conspicuous Consumption: The Demand for Counterfeit Status Goods Literature Review.

Searle, N., Vivian, A., 2021. Surprisingly Small: The Effect of Trade Secret Breaches on Firm Performance. 2021 Workshop on the Economics of Information Security (WEIS).

Shevchenko, P.V., Jang, J., Malavasi, M., Peters, G.W., Sofronov, G., Trück, S., 2023. The nature of losses from cyber-related events: risk categories and business sectors. J. Cybersecurity 9, tyac016.

TERAMIND, 2024. 5 Examples of IP Theft & How To Prevent IP Theft.

The IP Press, 2025. Cybersecurity and Intellectual Property: Safeguarding Digital Resources in the Age of Cyber Threats. IP Press.

The Times, 2024. Britain exposes North Korea’s global push to hack nuclear secrets.

The UK Government, n.d. Prepare annual accounts for a private limited company.

Tran, D., 2018. The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack.

Williams, H.L., 2017. How do patents affect research investments? Annu. Rev. Econ. 9, 441–469.

WPI Strategy, 2023. The business of cyber security - Protecting SMEs in the changing world of work.

Yang, C.-H., Huang, Y.-J., 2009. Do Intellectual Property Rights Matter to Taiwan’s Exports? A Dynamic Panel Approach. Pac. Econ. Rev. 14, 555–578.

+44 20 8133 3192 43 Tanner Street, SE1 3PL, London, UK
+30 21 2104 7902 Ifigenias 9, 14231, Athens, GR

LinkedIn company/alma-economics
almaeconomics

alma economics