TWC
IT SOLUTIONS

UK Cybersecurity Report 2022

Introduction

Every organisation, regardless of size, is exposed to a cyber attack due to the critical amount of client information they hold. Malicious attackers continue exploiting such databases as people and organisations rely on internet-connected devices.

Businesses need to be highly vigilant about the consequences of different threats, including ransomware attacks, data breaches and phishing email attacks spreading across the UK. According to the Department for Digital, Culture, Media & Sport, four out of ten firms (39%) had experienced cyber security breaches or attacks in 2021.

The UK Cybersecurity Report 2022 analyses the UK cyber landscape with a particular focus on the most hazardous cyber attacks that businesses encountered since 2006.

Table of Contents

The alarming increase in business-related cyberattacks has no doubt been caused by poor security management within hybrid working environments, as companies still struggle to deal with the fallout of the pandemic and the extra financial burden this places upon them. Prevention is always better than the cure when it comes to mitigating the impact of business cyberattacks - raising awareness amongst employees and conducting regular cybersecurity training should never be underestimated as part of a successful defence strategy.

Paolo Sartori

Chief Executive Officer

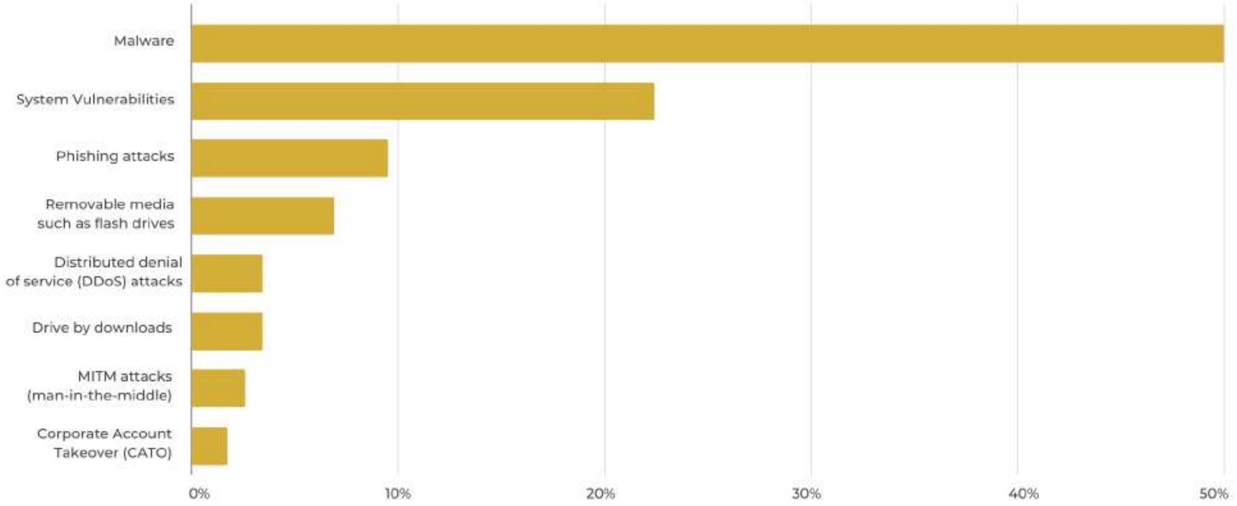
TWC IT Solutions

- CHAPTER 1 -

Key findings of the UK Cybersecurity Report 2022

Key Finding #1

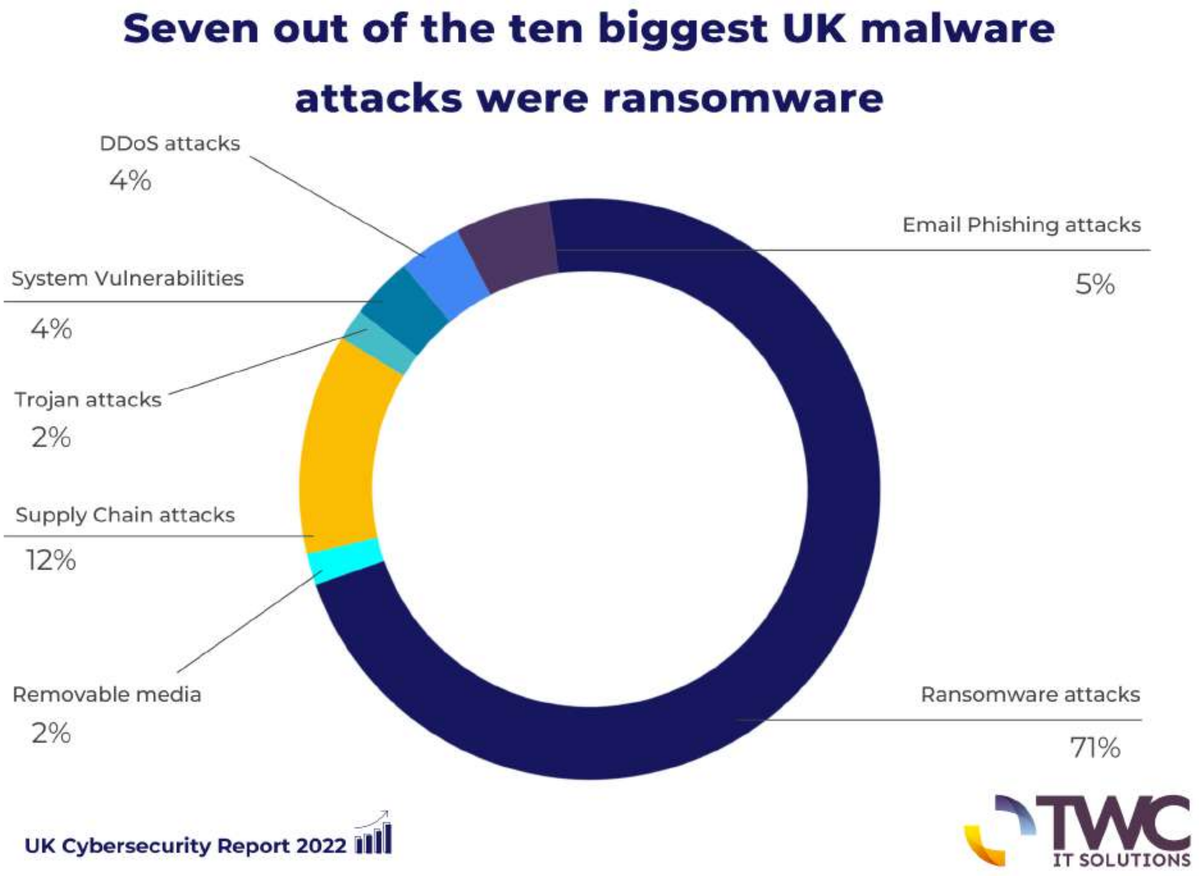
Malware, system vulnerabilities & phishing attacks are the top three threats in the UK



UK Cybersecurity Report 2022

- The results show that **malware (49.14%)**, **system vulnerabilities (22.41%)** and **phishing attacks (9.48%)** are the most frequent cyber attacks from the 200 major UK cyber attacks that were analysed for this paper.
- Based on the cases that were looked at, it was concluded that **not all organisations were able to provide information regarding the cyber attack.**
- Approximately **four out of ten UK businesses disclosed details on the cyber attack**, including the number of accounts impacted and the type of data that was compromised. The organisation might not always be aware of the attack, or they may be concerned about the potential legal consequences when not revealing this information.

Key Finding #2



- Ransomware attacks made up **71%** of the UK malware cases that have been investigated.
- This was followed by **supply chain attacks (12%)** and **email phishing attacks (5%)**, the two most common types of malware attacks.
- **Trojan** assaults, **system vulnerabilities** and **DDoS** attacks made up **10%** of all malware cases.
- The industries that were impacted the most by ransomware attacks were the **services** and the **retail** sector.
- **76.9%** of ransomware attacks targeted **B2C** businesses.

The NHS ransomware attack

What happened

The malware attack against the **NHS** in **August 2022** was one of the UK's worst cyber attacks. The attack on the morning of the 4th of August resulted in significant NHS outages and **Advanced**, a business that makes software for the healthcare industry, was the main target.

The malware attack impacted services like patient referrals, emergency medications, ambulance dispatch, after-hours appointment scheduling and mental health services.

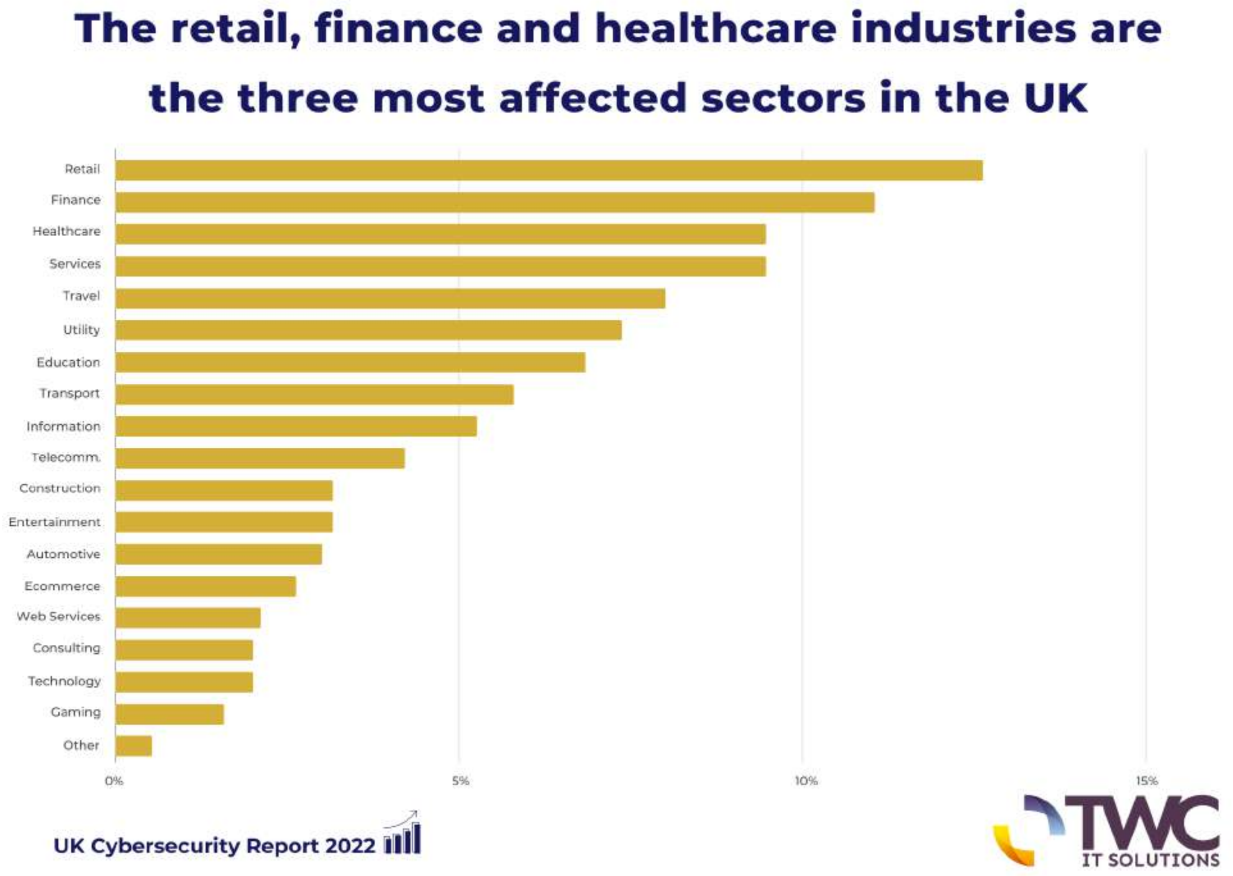
What we learned

No organisation, no matter how large or small, is safe from the constant danger of cybercrime. Hackers are constantly attempting to stay one step ahead of the cybersphere, with many business owners even recruiting a team of cybersecurity experts to build effective protection measures. Regardless of your current network security, third-party providers in the supply chain can also expose a business to cyber attacks.

Cybersecurity Tip

A **Disaster recovery strategy** is strongly advised to be implemented to prevent the risk of losing crucial data following any cyber attack. The best and most economical course of action is to always avoid a potential data loss rather than trying to restore lost data.

Key Finding #3



The retail, finance and healthcare industries are the three most affected sectors in the UK

UK Cybersecurity Report 2022

- The retail industry is the most vulnerable industry to cyber attacks. **12.63%** of the examined UK cyber attacks involved the retail sector. This is not surprising given that the pandemic has dramatically increased online sales and retailer profitability.
- The **finance** and **healthcare** industries are the two other industries often exposed to cyber attacks. **11.05%** of the cases that were examined involved the finance industry and **9.47%** involved healthcare organisations.
- With a rate higher than **5%**, data shows that the **service**, **travel**, **utility**, **education**, **transportation** and **information** sectors have been the most negatively impacted sectors by cyber attacks.

The Works ransomware attack

What happened

The Works, a **retailer**, was the target of a particularly serious **ransomware** attack in the UK in 2022. Ransomware, one of the most common forms of cyber attacks, is believed to have been used by hackers to damage the British discount stationary and book business. The retailer had to **close five of its 526 stores** as a result of the cyber attack. It has also interfered with the company's delivery to its stores and affected its tills.

The retailer claimed that after being notified of the incident, the company immediately took a number of steps. Client **payment information** wasn't accessed, but it has not been determined to what degree any other data may have been impacted. Not to mention the financial damage this ransomware attack has caused to the retailer, which is yet to be confirmed.

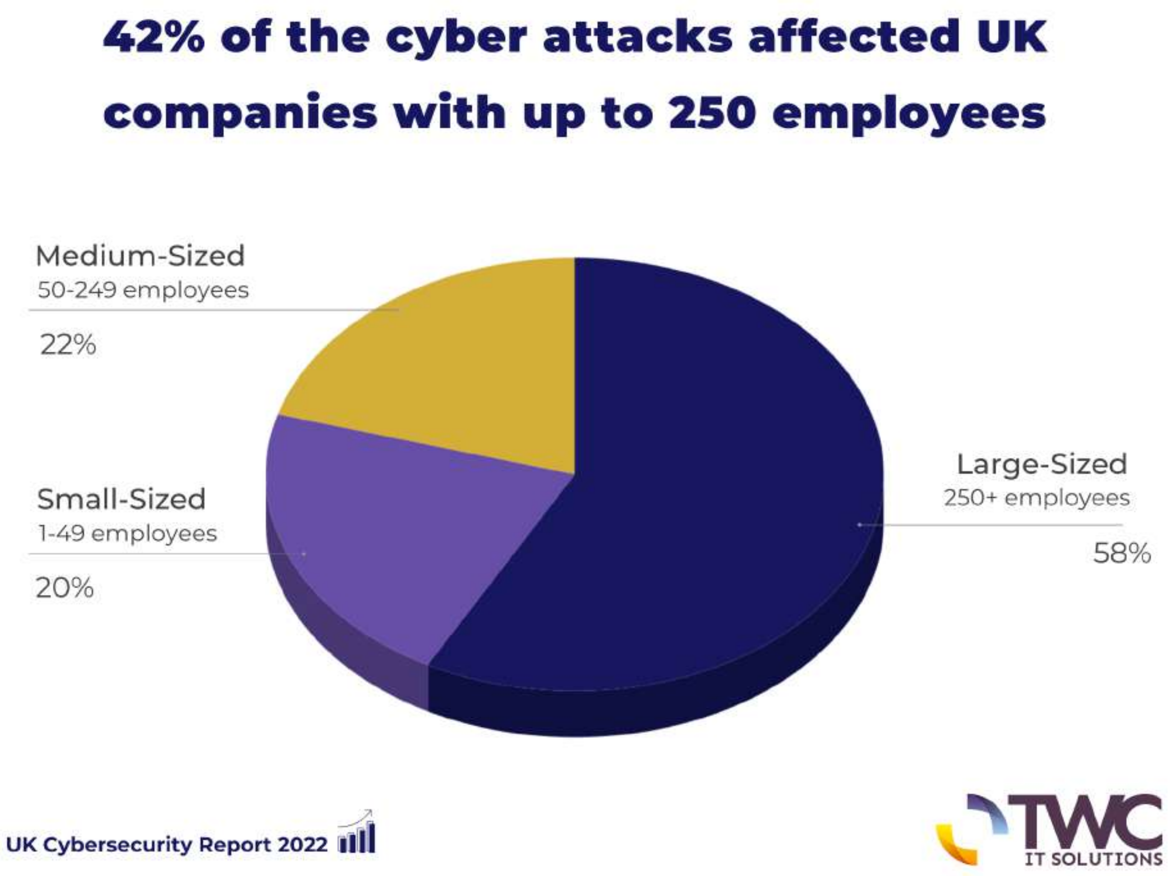
What we learned

From 'The Works' ransomware attack, we can conclude that **no system is secure against cyber attacks**. Hackers compromised The Works, even though it appears to have solid protection in place.

Cybersecurity Tip

Using reliable **Cybersecurity services** will help you identify issues and solve them before they get out of control.

Key Finding #4



42% of the cyber attacks affected UK companies with up to 250 employees

UK Cybersecurity Report 2022

- **Large** companies were affected **58%** of the time compared to small and medium-sized businesses.
- **Small** and **medium-sized** businesses experienced almost the **same** amount of cyberattacks as larger businesses.
- Given that the examined cases are the most significant cyber attacks in the UK over the last 15 years, the fact that **22%** of the total attacks occurred against **small businesses** can lead to the conclusion that no business is truly safe from cybercrime.

The EasyJet data breach

What happened

The British airline EasyJet's computer systems were the target of a cyber attack in January 2020, which was made public in May 2020. A total of **nine million** people were impacted, and 2,208 people had their credit card information stolen. During the course of their investigation into the incident, EasyJet informed the Information Commissioner's Office.

Due to an increase in phishing attacks during the Covid-19 pandemic, EasyJet released the facts even though it wasn't required to warn passengers whose basic booking details were compromised.

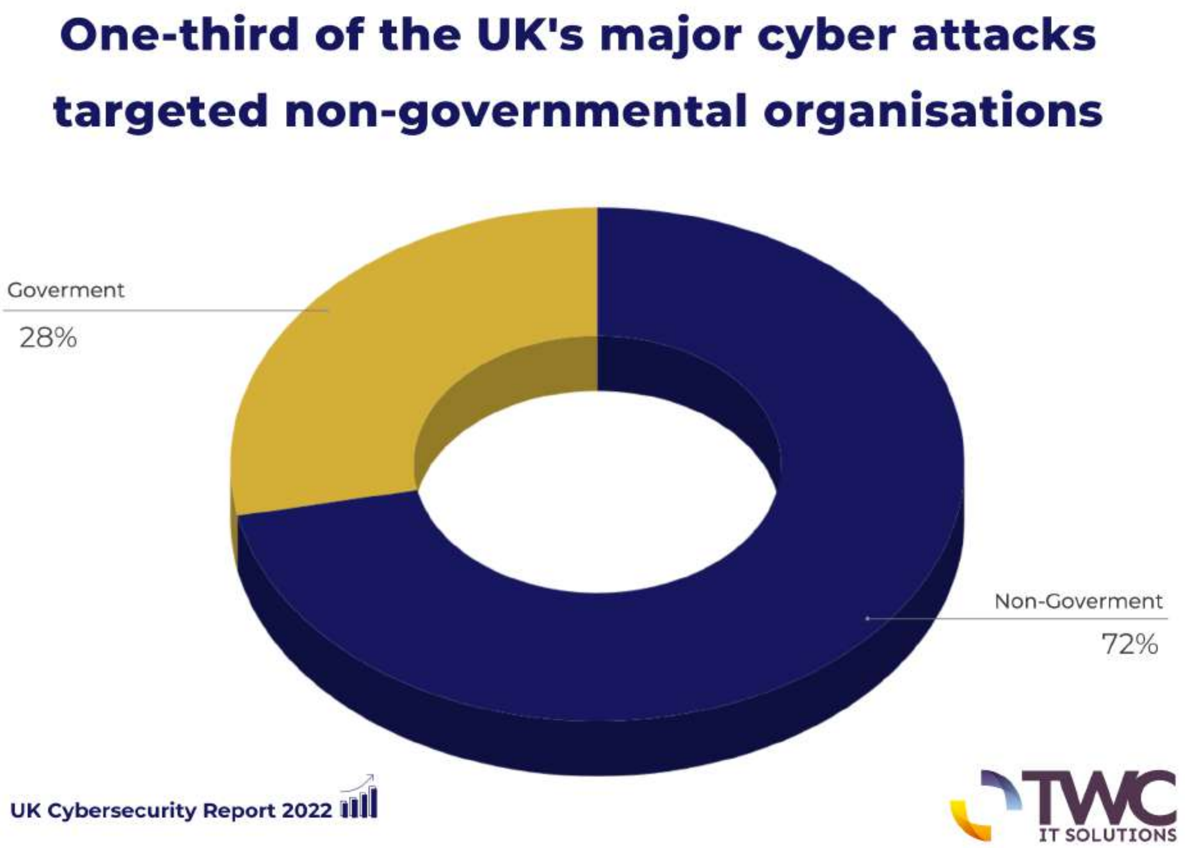
What we learned

The first airline targeted by cybercriminals was not EasyJet, and it certainly won't be the last. The travel industry is the fifth most vulnerable to cyber attacks. What is notable **how quickly EasyJet responded** and informed their passengers. Any organisation, regardless of size, is vulnerable to cybercriminals.

Cybersecurity Tip

To minimise the possibility of losing essential data in the event of a cyber attack, businesses are encouraged to implement a solid **disaster recovery strategy**.

Key Finding #5



One-third of the UK's major cyber attacks targeted non-governmental organisations

UK Cybersecurity Report 2022

- Almost **three out of ten** major cyber attacks targeted **governmental** organisations.
- The majority of non-government cyber attacks **(60.7%)** targeted **large corporations**.
- The **retail** sector was the most vulnerable to non-governmental cyber attacks.
- **Finance** and **travel** were the industries affected the most, followed by retail.
- Only **9.8%** of cyber attacks against non-governmental organisations were carried out by individuals **inside** the organisation.
- **Passive** cyber attacks accounted for **71.3%** of non-government cyber attacks.

The WannaCry attack against NHS

What happened

The **NHS** was impacted by one of the biggest ransomware attacks in **2017**, known as **WannaCry**. The attack has significantly impacted the NHS systems.

The primary characteristic of this attack is that it only affected computers that were still running the March security update from Microsoft. The WannaCry ransomware attack, which **lasted a few hours**, is believed to have affected **more than 300,000 computers in 150 countries**. Due to the lack of examples of people receiving their data after paying the ransom and that huge revenue would promote more of these efforts, experts promptly recommended impacted users against doing so. A total of **327 payments** worth **£106251.79** have been sent as of June 14, 2017, when the attack had subsided.

What we learned

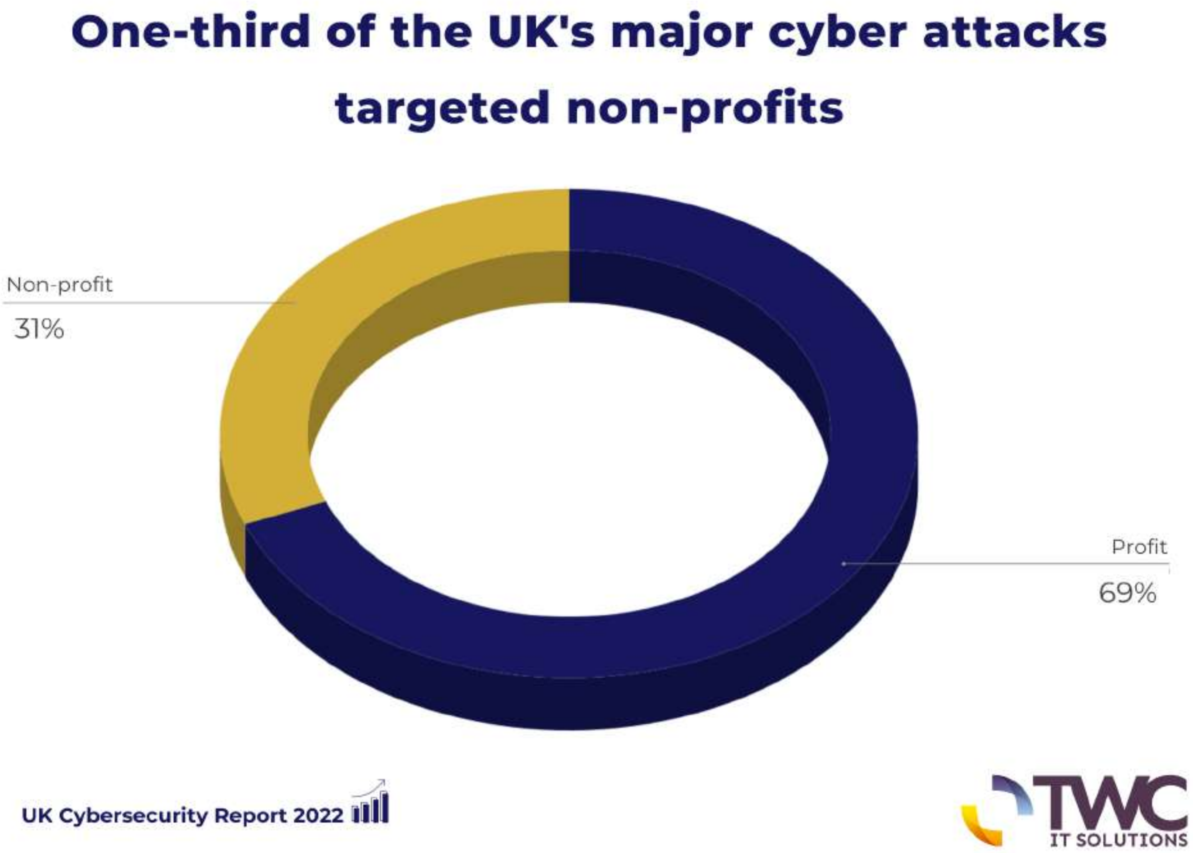
Regarding the types of businesses impacted, WannaCry made **no exceptions**, targeting two major organisations, FedEx and the NHS.

Cybercriminals **don't discriminate** when it comes to their victims; they can be individuals, large or small organisations, governmental or non-governmental organisations.

Cybersecurity Tip

Always **keep up with the latest developments** in **Cybersecurity**.

Key Finding #6


One-third of the UK's major cyber attacks targeted non-profits

UK Cybersecurity Report 2022

- Almost **seven out of ten** major cyber attacks targeted profit-seeking organisations.
- In **20%** of the cases of cyber attacks against non-profit organisations, an **insider** was responsible for the attack.
- **Passive** cyber attacks made up **62.7%** of all non-profit cyber attacks.
- **Malware** is the most common type of cyber attack **(52.9%)** against charitable institutions.
- Concerning cyber attacks targeting voluntary organisations, **education** and **healthcare** were among the most severely impacted sectors.
- **Malware (49.3%)**, **system vulnerabilities (28%)** and **phishing (10.7%)** were the most frequent types of cyber attacks targeting profit-seeking organisations.

Oxford University lab studying Covid-19 targeted by ransomware

What happened

It is believed that the attack on Oxford's Division of Structural Biology took place in the middle of February. Although it is well known that the hackers have been demonstrating access to several systems, including **devices used to process biological samples**, Oxford University is officially classifying it as an isolated incident.

However, the study on the coronavirus could be at risk of theft in the event of a lab breach. If hackers were able to manipulate the flow of liquids or other elements of the purifying system, there is also the risk of research being damaged.

The **National Cyber Security Centre (NCSC)** was notified immediately by the Oxford University lab to launch an investigation into the cybersecurity incident.

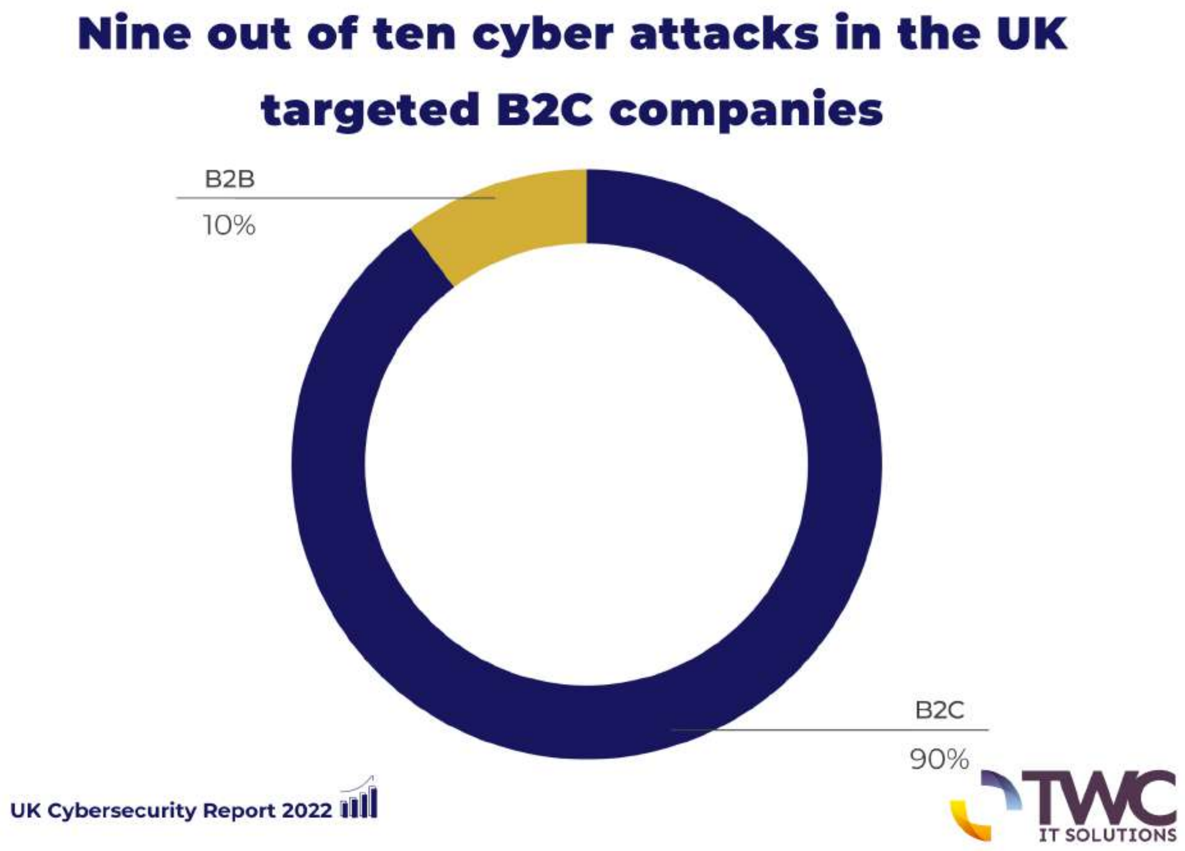
What we learned

This incident highlights how vulnerable every institution is to cyber attacks. They are not always tied to the quantity of sensitive information a business/organisation handles. However, in the case of sensitive information found in the Oxford University lab researching Covid-19, it can be concluded that it's crucial to take preventative measures to safeguard data.

Cybersecurity Tip

Always **keep up with the latest developments** in **Cybersecurity**.

Key Finding #7



Nine out of ten cyber attacks in the UK targeted B2C companies

UK Cybersecurity Report 2022

- An **outside** source was responsible for **90%** of the cyber attacks on B2C business.
- **25.9%** of the cyber attacks targeting **B2C** organisations were **active**.
- Cyber attacks caused significant disturbance on B2C companies in the **retail, finance and travel** sectors.
- **61%** of the attacks involving B2C companies targeted large corporations.
- **Malware** cyber attacks were the most common for B2C companies, accounting for **45.2%** of all cyber attacks.
- The **financial** sector was primarily impacted by cyber attacks among B2B companies **(35.7%)**, with other industries being affected at roughly the same rate.