Policy Brief

Cybercrime and Cyber Threats in the UK

DISSEMINATION LEVEL PUBLIC

PARTNER

PSNI

AUTHOR

PSNI

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

1. Cybercrime and Cyber Threats in the UK[1]

Cybercrime in the United Kingdom (UK) has become an increasingly pressing issue in recent years, with domestic and international actors posing a significant threat to the country's security and economy. This report will examine the various forms of cybercrime in the UK, including both domestic and international threats, and will discuss the impact of the COVID-19 pandemic on these trends.

Domestic cybercrime in the UK is primarily perpetrated by individual actors or small groups, who engage in activities such as hacking, identity theft, and online fraud. Four in ten businesses and a quarter of charities report having any kind of cyber security breach or attack in 2021. Larger businesses are more likely to identify breaches or attacks than smaller ones. This year's statistics show a particularly stark gap between micro and small firms on one hand, and medium and large ones on the other.

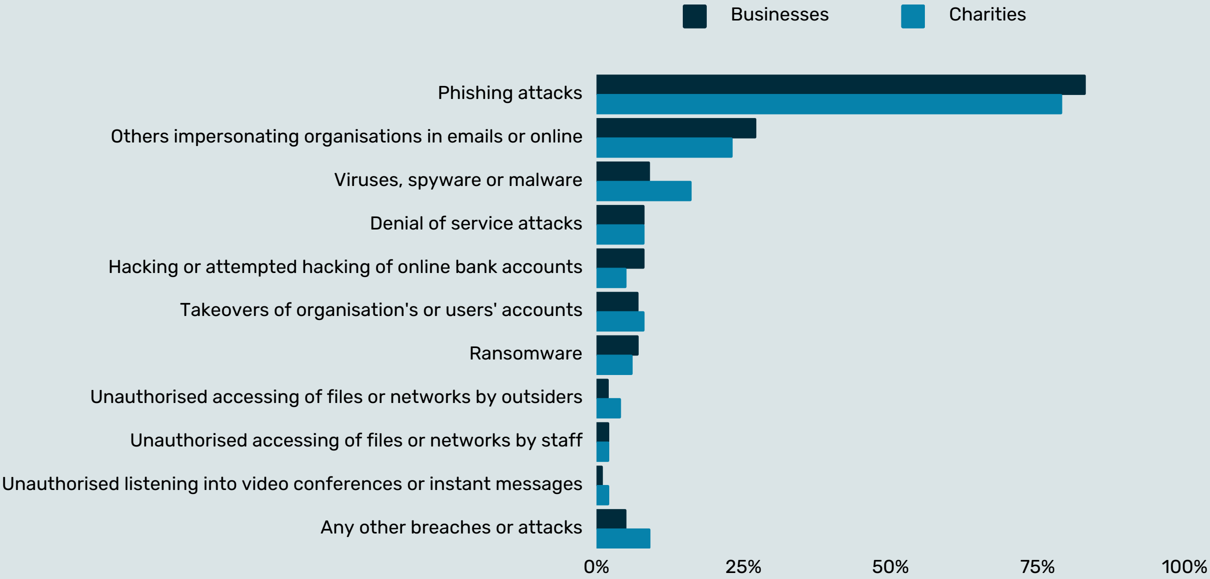

Figure 1: Cyber security breaches and attacks in the UK on businesses and charities[2]

2. Cybercrime and cyber threats emanating from domestic actors

According to the National Cyber Security Centre (NCSC), the most common form of domestic cybercrime in the UK is "phishing," in which criminals use fake emails or websites to trick victims into revealing sensitive information. In 2019, the NCSC reported that it had prevented over 1,200 phishing attacks from successfully reaching their intended targets.

>> In December 2020, a UK-based cyber-criminal was sentenced to four years in prison for his role in a ransomware attack that affected over 200 companies worldwide, including several in the UK. The attack, known as the "Ryuk" ransomware, encrypted the victims' files and demanded a ransom payment to restore access.[3]

>> In October 2020, UK police arrested a man for his role in a large-scale phishing scam that targeted individuals and businesses in the UK and other countries. The scam involved sending fraudulent emails that appeared to be from well-known companies, such as Amazon and Netflix, in an attempt to trick victims into giving away personal information and money.[4]

>> In August 2020, a UK-based cyber-criminal pleaded guilty to his role in a cyber-attack that targeted TalkTalk, a major UK telecommunications company. The attack resulted in the theft of personal data belonging to nearly 157,000 customers, including sensitive information such as banking details and addresses.[5]

>> In July 2020, UK police arrested a man for his role in a cyber-attack that targeted a UK-based online gambling company. The attack resulted in the theft of over £1.2 million from the company's bank account.[6]

>> In April 2021, UK police arrested a man for his role in a cyber-attack that targeted companies and individuals during the Covid-19 pandemic. The scam involved sending fraudulent emails that appeared to be from legitimate sources, such as the World Health Organization, and tricking victims into giving away personal information and money.[7]

3. Cybercrime and cyber threats emanating from international actors

In addition to cybercrime emanating from domestic actors, the UK also faces significant cyber threats from international actors. The NCSC has identified a number of foreign countries that are known to have the capability to launch cyber-attacks against the UK, including China, Russia, and North Korea. These countries are believed to have a range of sophisticated cyber capabilities, including the ability to conduct advanced persistent threats (APTs) and to launch Distributed Denial of Service (DDoS) attacks.

>> In 2017, the UK's National Cyber Security Centre (NCSC) and the US Department of Homeland Security reported that the North Korean state-sponsored hacking group known as Lazarus had targeted the UK's media, telecoms and energy sectors with malware attacks. The group was known for stealing money from banks, and using the proceeds to fund the North Korean government.[8]

>> In 2018, the UK's National Cyber Security Centre (NCSC) reported that Russian state-sponsored hacking group APT28 had targeted the UK's political institutions with spear-phishing emails and malware attacks. The group was known for using the stolen data to influence political decisions.[9]

- In 2020, the UK's National Cyber Security Centre (NCSC) reported that the Iranian state-sponsored hacking group known as APT34 had targeted UK-based businesses with spear-phishing emails and malware attacks. The group was known for stealing intellectual property and sensitive business information.[10]

- In 2021, the UK's National Cyber Security Centre (NCSC) and the US Federal Bureau of Investigation reported that a Russian state-sponsored hacking group known as SandWorm had targeted UK-based organizations with spear-phishing emails and malware attacks. The group was known for disrupting critical infrastructure, including power plants and transportation systems.[11]

- In 2021, the UK's National Cyber Security Centre (NCSC) reported that a terrorist group known as ISIS had used social media to spread propaganda and recruitment messages during the COVID-19 pandemic. The group also used encrypted messaging apps to plan and coordinate attacks.[12]

4. Cyber terrorism in the UK

The COVID-19 pandemic has had a significant impact on the cyber terrorism landscape in the UK. According to the UK's National Counter Terrorism Security Office (NaCTSO), "the pandemic has created new opportunities for terrorists to target the UK and its interests" (NaCTSO, 2020).[13]

As a result, many terrorist organizations have shifted their focus to take advantage of the increased opportunities for cybercrime.

The consequences of cyber terrorism in the UK in financial terms can be significant. The cost of cyber terrorism to UK businesses is estimated to be in the billions of pounds, according to a report by the Centre for the Protection of National Infrastructure (CPNI) (CPNI, 2016).[14] Additionally, the cost of cyber terrorism to individuals can include not only financial losses, but also the cost of recovering from a cyber-attack, such as the cost of hiring a professional to restore lost data.

Possible consequences of cyber-attacks by terrorist organizations against the UK include:

- Disruption of critical infrastructure, such as power plants and transportation systems, which could result in loss of life and significant economic damage.

- Theft of sensitive information, such as government and military secrets, which could be used to plan and carry out further attacks.

- Spread of propaganda and disinformation, which could be used to influence public opinion and create chaos and confusion.

- Disruption of communication and information systems, which could make it difficult for emergency responders and other key personnel to coordinate their efforts during a crisis.

5. Criminal opportunities in the context of the Covid-19 pandemic

The COVID-19 pandemic has had a significant impact on cybercrime in the United Kingdom, with criminals taking advantage of the increased online activity to launch cyber-attacks.

- An increase in phishing and malware attacks related to COVID-19. According to the National Cyber Security Centre (NCSC), there has been a significant increase in the number of phishing emails and messages that purport to be from trusted organizations, such as the World Health Organization (WHO) or the NHS, but are actually designed to trick victims into revealing sensitive information or downloading malware. For example, in May 2020, the NCSC issued an alert about a phishing campaign that used the WHO logo to trick victims into revealing their personal information.

- An increase in ransomware attacks. Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key. In April 2020, the NCSC reported that a number of UK organizations had been targeted by a ransomware attack that used a strain of malware called "NetWalker." According to the NCSC, the attackers had demanded a ransom of $3 million from the victims.

- An increase in attacks on remote working systems and devices. As more people have been working from home, criminals have been able to take advantage of the increased use of remote working systems and devices to launch attacks. For example, in April 2020, the NCSC reported that a number of UK organizations had been targeted by a cyber-attack campaign that used a strain of malware called "DoublePulsar." The attackers had used this malware to gain unauthorized access to the victims' systems, and had then used it to install other malware.

- An increase in attacks on financial systems. According to the NCSC, cyber criminals have been exploiting the increased use of digital financial services during the pandemic to launch attacks. For example, in June 2020, the NCSC reported that a number of UK banks had been targeted by a cyber-attack campaign that used a strain of malware called "Dridex." The attackers had used this malware to gain unauthorized access to the victims' systems and to steal financial information.[15]

6. Technology to counter cyber threats

The UK National Cyber Security Centre is spearheading research and analysis to find new ways to secure the UK's digital systems.

The aim of the NCSC's research programme is to manage long-term critical risks, and to strengthen the security of the critical systems that the UK relies upon. This includes defence and intelligence networks, national infrastructure, and the technologies used throughout homes and schools.[16]

The NCSC works with academia and industry partners to share expertise across cutting-edge technologies such as artificial intelligence and quantum computing.

Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today's 'classical', computers. A quantum computer – theoretically – could break some types of cryptography currently used to protect classified systems.[17]

The UK has designed its first 'quantum-safe' cryptographic algorithms, designed to be resilient to such attacks.

Work continues with the Alan Turing Institute (the national institute for data science and artificial intelligence) to explore whether machine learning can be used to detect certain types of cyber-attack. The research built on the capabilities of 'Logging Made Easy', a tool that helps organisations set up a basic end-to-end monitoring of their IT estate. This research has improved our understanding of how we can use artificial intelligence to detect malicious activity.[18]

7. Tackling the increasing challenge of cyber threats in the future

UK agencies have taken steps to counter these growing threats. Significant investment in our intelligence capabilities has increased our understanding of the threat and enabled us to conduct more effective covert counter campaigns.

We have developed an integrated law enforcement response to cybercrime, led by the National Crime Agency (NCA) and dedicated cyber teams within regional organised crime units and local police forces across England, Wales, Northern Ireland and Scotland. This has enhanced our operational and investigative edge over cyber criminals and other adversaries.

We have invested significantly in our offensive cyber capabilities, first through the National Offensive Cyber Programme, and more recently through the establishment of the National Cyber Force (NCF). The NCF draws together personnel from the Government Communications Headquarters (GCHQ), the Ministry of Defence (MOD), the Secret Intelligence Service (SIS, also known as MI6) and the Defence Science and Technology Laboratory.[19]

In coordination with our allies, we have also sought to raise the cost of state-sponsored hostile activity in cyberspace by attributing attacks and imposing consequences on those responsible.

8. Conclusions

In conclusion, cybercrime in the United Kingdom is a significant and growing problem. The country is facing a range of cyber threats from both domestic and international actors, including individual criminals, terrorist groups, and state-sponsored hackers. The COVID-19 pandemic has also exacerbated these challenges, leading to an increase in cyber-attacks and a shortage of cybersecurity professionals.

It is essential that the UK continues to invest in cybersecurity measures and to work closely with international partners to combat cybercrime.

References

1. This Policy Brief was prepared by the Police Service of Northern Ireland (PSNI), International Programmes Office, as part of T10.5.
2. Home Office (2021), Cyber Security Breaches survey, at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/.
3. BBC. (2020, December 14), Ransomware: UK man sentenced for role in cyber-attack. Retrieved from https://www.bbc.com/news/technology-55276797.
4. National Cyber Security Centre (2020, October 13), UK police arrest man for role in large-scale phishing scam. Retrieved from https://www.ncsc.gov.uk/news/uk-police-arrest-man-role-large-scale-phishing-scamBBC. (2020, August 18). TalkTalk data breach: Man admits role in cyber-attack. Retrieved from https://www.bbc.com/news/technology-53597226.
5. BBC. (2020, August 18). TalkTalk data breach: Man admits role in cyber-attack. Retrieved from https://www.bbc.com/news/technology-53597226.
6. National Cyber Security Centre. (2020, July 14). UK police arrest man for role in cyber-attack on online gambling company. Retrieved from https://www.ncsc.gov.uk/news/uk-police-arrest-man-role-cyber-attack-online-gambling-company.
7. National Cyber Security Centre. (2021, April 7). UK police arrest man for role in COVID-19 themed scam. Retrieved from https://www.ncsc.gov.uk/news/uk-police-arrest-man-role-covid-19-themed-scam.
8. NCSC. (2017, October 13). WannaCry: How the attack unfolded. Retrieved from https://www.ncsc.gov.uk/news/wannacry-how-attack-unfolded.
9. NCSC. (2018, February 13). Russian cyber threat: UK and US government issue joint statement. Retrieved from https://www.ncsc.gov.uk/news/russian-cyber-threat-uk-and-us-government-issue-joint-statement.
10. NCSC. (2020, November 10). Iranian cyber threat: UK government issues statement. Retrieved from https://www.ncsc.gov.uk/news/iranian-cyber-threat-uk-government-issues-statement.
11. NCSC. (2021, January 13). Russian cyber threat: UK government issues statement. Retrieved from https://www.ncsc.gov.uk/news/russian-cyber-threat-uk-government-issues-statement.
12. NCSC. (2021, January 13). Terrorist use of the internet: UK government issues statement. Retrieved from https://www.ncsc.gov.uk/news/terrorist-use-internet-uk-government-issues-statement.
13. NaCTSO. (2020). COVID-19: Counter terrorism advice for businesses. Retrieved from https://www.gov.uk/government/publications/covid-19-counter-terrorism-advice-for-businesses.
14. CPNI. (2016). Cyber security: Protecting national infrastructure. Retrieved from https://www.cpni.gov.uk/documents/publications/cyber-security-protecting-national-infrastructure.
15. National Cyber Security Centre. (2020). Cyber Threats during COVID-19.
16. NCSC mission statement. Retrieved from https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
17. NCSC. (2020). https://www.ncsc.gov.uk/whitepaper/preparing-for-the-quantum-safety-cryptography.
18. NCSC. (2022) Introducing Scanning Made Easy. Trial project to aid public sector, cyber security professionals and organisation to detect system vulnerabilities. https://www.ncsc.gov.uk/blog-post/introducing-scanning-made-easy
19. NCSC mission statement. Retrieved from https://www.ncsc.gov.uk/section/about-ncsc/what-we-do