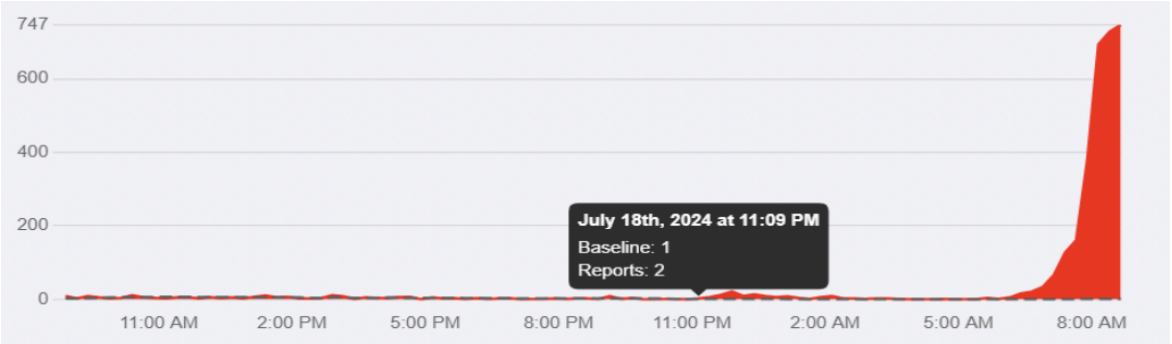
Cybersecurity Attacks: The invisible threat that could change everything

In 2024 there was over 1 billion records compromised by online hackers, 7.78 million cyber-attacks on UK businesses and over 70,000 cases of identity theft to UK residents up and down the country. This barely captures the growing toll that online hacking is taking on the UK economy and its residents. Economists now claim that “oil is no longer worth more than gold, but data now leads the way” signifying the immense worth of data and the serious risks posed if it’s misappropriated. The UK government reported that in 2016 cybercrime’s cost to the economy was £14.8 billion in 2016-2017 yet in 2024 it cost £27 billion. This staggering rise represents an impending threat to national economic stability, it has paralysed business operations, created a tax on growth and crippled public trust.

The disturbing 70% rise in Ransomware attacks is a key contributor in this and should be a critical issue for every citizen. Ransomware attacks are a type of cyberattack where malware or malicious software (software intentionally designed to harm the user or network) is used to encrypt data and render files or whole networks inaccessible. The hacker often demands a ransom, mostly in cryptocurrency, in exchange to restore access. The Cybersecurity and Infrastructure Security Agency reported that the average ransom paid often exceeded $200,000 highlighting both the significant power and potential danger of these attacks. Ransomware attacks frequently impact everyday citizens through ripple effects, such as sharp declines in stock prices and sectoral impacts, highlighting the need for greater public awareness of these threats. These attacks take various forms and while the 2024 Microsoft CrowdStrike attack, which impacted many summer holiday goer’s, was not a direct Ransomware attack, it was driven by the same underlying causes.

The attack stemmed due to the distribution of malicious software targeting CrowdStrike customers, the same cause of most Ransomware attacks. In July 2024, ‘the biggest IT outage’ linked to CrowdStrike and Microsoft disrupted businesses worldwide, by the time the error was identified it had already reached millions of devices internationally. Microsoft reported that 8.5 million devices were hit, exposing the sweeping global influence of CrowdStrike's software. These devices experienced a devastating ‘blue screen of death’ leaving critical sectors like healthcare and finance paralysed as servers were abruptly taken offline.. The graph below depicts the rapid rise of outages reported after the breach.



Building on this, on September 23rd, 2024, CrowdStrike testified in a US house of representatives hearing which signifies the severe and widespread damage that infiltrated every area of the company. The outage resulted in the cancellation of over 10,000 flights around the world, leaving thousands of holiday goers stranded and significantly disrupting holiday plans due to a cybersecurity breach through malicious software. Additionally, CrowdStrike shares plummeted by 11% after the incident. The outage inflicted significant losses, costing Fortune 500 companies an estimated $5.4 billion in revenues and gross profit, with insurance covering only 10-20% of these losses, this compounded the financial impact. While all industries were severely impacted the health care and banking sectors were hit the hardest with estimated losses of $1.94 billion and $1.15 billion. The CrowdStrike breach emphasises the critical need for strong cybersecurity and indicates the plaguing global consequences for the victims of the ever-evolving world of tech.

When considering the victims of advancing cyber technology, the recent NHS Ransomware attack should spring to mind and serve as a reminder that everyday citizens are increasingly affected by and at risk of these cyber threats. In September 2024 the NHS was targeted by a Ransomware attack that encrypted innocent people's patient records and medical services meaning 1,693 procedures were postponed and emergency services were delayed. The government were quickly compelled to act due to the recent surge in Ransomware attacks and their significance on the UK residents and economy. The Cybersecurity and Resilience Bill, hastily released on September 30th, aims to tackle Ransomware attacks and mitigate their severe impacts. It confronted the looming nightmare of these attacks and mandates tighter reporting and response protocols. Additionally, it enhanced requirements for companies to implement strong cybersecurity standards. However, it's not only the government taking steps to curb the dangers of technological hacks, but cybersecurity company Swivel Secure who specialise in advanced authentication to combat these threats. Yet, enhanced technology also means hackers are enhancing their methods to trap unsuspecting victims.

One growing threat is the rise of watering hole attacks, which pose a major online danger to both companies and individuals alike. These attacks involve hackers targeting a specific group by compromising websites the victim is likely to visit and waiting on the site like a predator at a watering hole. The UK was the second most targeted country in the world for cyber-attacks with watering hole attacks contributing to a substantial number of these attacks. With only 31% of UK businesses taking cyber risk assessment in 2024, leaving them more vulnerable than ever of becoming victim to watering hole and Ransomware attacks. This directly impacted the citizens that engage with and trust these businesses as demonstrated by Cutout.Pro's catastrophe. On February 27th, 2024, a CSV file of Cutout.Pro's data was shared on BreachForums. This comprised almost 20 million unique records and was a 5.93GB leak. It included the emails, addresses and names of 19.98 million people, despite cutout initially denying it. The cyberattack triggered an economic decline for the company, with the resulting reputational damage proving nearly irreparable. Its stock value also took a significant hit due to widespread outrage over the security breach. This indicates that cybersecurity breaches are leaving business in financial, reputational and legal fallout.

2024 has revealed that the disruption of these cybersecurity breaches and attacks is increasing, yet efforts to prevent them are on the decline. The rapid advancement of technology and AI is posing a detrimental danger to businesses worldwide and the innocent civilians who trust them with their data and finances. Cybersecurity breaches, if not soon managed, will be an unstoppable threat and all industries should be deeply concerned. While some companies may be deterred from properly implementing correct preventative security measures due to the financial commitment, it is essential to protect your business from these persistent attacks.