Butterworth Spengler
Insurance Brokers

0151 494 4400
cyber@butterworthspengler.co.uk

Cyber Crime UK Facts

CYBER

FEB. 2022

Cyber security breaches and attacks are a serious threat to all businesses and charities. Data indicates the frequency is undiminished and phishing attacks remains the most common threat.

THE FACTS

Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%).

Among the 39 per cent of businesses and 26 per cent of charities that identify breaches or attacks, one in five (21% and 18% respectively) end up losing money, data or other assets.

One-third of businesses (35%) and four in ten charities (40%) report being negatively impacted regardless, for example because they require new postbreach measures, have staff time diverted or suffer wider business disruption. Source: Official Statistics Cyber Security Breaches Survey 2021

Cyber attacks can have a large financial and psychological impact on victims. In one ransomware attack alone, a company lost €60 million in revenue.

The most reported way to directly extort funds from a victim is through ransomware attacks, where criminals encrypt data and then demand a ransom to decrypt it. Criminals have continued to move towards targeting businesses over individuals.

The use of phishing emails containing malicious content remains the most commonly observed method to deliver malware. The past year has seen a change in the content of phishing emails, with fewer malicious attachments and more links to malicious websites, at a ratio of over five to one.

Data remains the key commodity for cyber criminals, and there are several ways to exploit it for financial gain. As such, it is common for a victim network to be subjected to different methods of monetising an initial infection.

The UK financial data most coveted by cyber criminals continues to be CVV data, the security code on cards that is requested as part of online transactions. Criminals increasingly 'scrape' this data from website payment pages. The scale of CVV scraping has increased in the past year. In one instance, 962 e-commerce sites were compromised within 24 hours.

Business Email Compromise is one of the fastest growing threats, especially for small businesses. Criminals imitate an employee or a common supplier of a company – usually requesting payment of an invoice – by using compromised credentials to seem credible. Source: NCA – National Strategic Assessment of Serious & Organised Crime

UK CYBER CRIME LAW

Cyber crime is a crime and is illegal. Within the UK we have strict laws regarding computer crimes in comparison to other countries. Any crime that involves fraud is covered by the current UK Fraud Legislation, most recently by the Fraud Act of 2006. In addition cyber crime is additionally covered under the Computer Misuse Act of 1990. The unfortunate truth is that cyber crime and cyber criminals are very rarely caught and even more rarely are they prosecuted. Less than 1% of computer hacking offences resulted in prosecution in 2019, of the 17,600 offences recorded in the UK, only 57 were tried under the computer misuse act. The numbers signify a 12% drop in convictions compared to 65 successful prosecutions the year before.

THE REALITY

The average cyber incident / claim costs Small to Medium Enterprises between £60,000 and £115,000 for large businesses it is in the region of £600,000 to £1,100,000.

1.5 million organisations fell victim to cyber crime in 2019, which equates to 25% of all UK businesses.

Less than 10% of businesses in the UK purchase Cyber, Data and Crime Insurance.

Phishing and malware were the most common tools for cyber crime, the larger the organisation, the more likely they were to fall victim.

Among small businesses phishing attacks were successful 29% of the time and malware 20% of the time. However, in large businesses these numbers rose to 38% and 31%.

Source: IT Governance

THE MOST COMMON FORMS OF CYBER ATTACK

Phishing - when you receive an email that purports to be from a bank, your employer, your manager asking for passwords or personal information.

File Hijacking - where a hacker accesses your computer and files, locking you out, a ransom is then demanded to return your files, which are normally corrupted.

Webcam Managing - your webcam is taken over and your key strokes are recorded or record a video of you to blackmail you or learn personal information about you.

Screenshot - where a hacker takes screenshots of your display, obtaining passwords or personal information.

Keylogging - recording keystrokes to gain access to passwords.

Ad clicking - where you are encouraged to click on a link by email or website, which activates malware or requests personal information.

Hacking - where access is gained to business files or servers and information is obtained.

DDoS (Distributed Denial of Service) Attack - this type of attack takes advantage of the specific capacity limits that apply to any network resources, such as the infrastructure that supports a company's website. A DDoS attack will send multiple requests to the attacked web resource, with the aim of exceeding the website's capacity and prevent the website from functioning correctly.

0151 494 4400
cyber@butterworthspengler.co.uk
20-24 Faraday Road, Wavertree Technology Park, Liverpool, L13 1EH

Opening Hours
Monday - Friday
9am - 5pm

BIBA