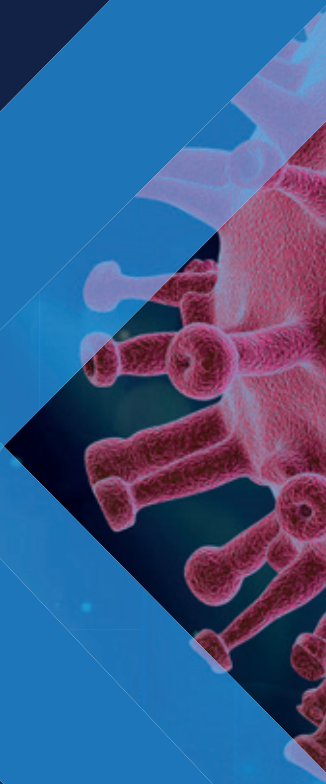
DigitalXRAID
CYBER SECURITY EXPERTS

The Impact of COVID-19 on Cyber Security in the UK



The Impact of Covid-19 on UK Businesses

The 2020 pandemic has seen a huge global impact on businesses, along with effecting the lives of millions of people. Here in the UK, 11% of businesses are currently at risk of insolvency and 48% of businesses reported turnover below their previous expectations[1]. The pandemic has placed a huge strain on our economy, affecting businesses up and down the country. The cybersecurity industry has seen a large increase in attacks since the beginning of the outbreak and with 27% of employees now working remotely, the opportunity for cyber criminals to access sensitive information has become easier than ever[2].

400%

The increase in scams over the month of March, making COVID-19 the largest-ever security threat[3]. (ReedSmith)

60%

The increase in visits to popular hacker websites and forums between March and May[4]. (cybernews)

18m

The daily malware and phishing emails related to Coronavirus that Google blocked in April alone[5]. (Google)

With the rise of online shopping during lockdown and in the lead up to Christmas, 58% of UK consumers say they're shopping more online than they did before Covid-19[6]. Data is being exchanged at astounding rates, giving cyber criminals ample opportunity to attack. The main industries that have suffered attacks or breaches are eCommerce, Financial Services, Healthcare and Education[7].

25% **report an increase in fraudulent emails, phishing attempts and spam to their corporate email since the start of the COVID-19 crisis[8].** (Deliotte)

47% **of employees cited distraction as the reason for falling for a phishing scam while working from home[9].** (Tessian)

1. Office for National Statistics; Coronavirus and the economic impacts on the UK. 2. Office for National Statistics; Coronavirus (COVID-19) roundup: Economy, business and jobs; 24th September 2019. 3. Reed Smith; Coronavirus is now possibly the largest-ever security threat. 4. Cybernews.com; Data suggests unprecedented interest in hacking and cybercrime during pandemic. 5. Google; Protecting businesses against cyber threats during COVID-19 and beyond 6. Econsultancy.com; Coronavirus impact on marketing, ecommerce & advertising. 7. PWC; Why has there been an increase in cyber security incidents during COVID-19? 8. Deliotte: Cybercrime - the risks of working from home; 2020. 9. Tessian; How Hybrid-Remote Working Will Affect Cybersecurity.

The Growing Threat of Cybercrime

It's a fact that since the first cases of coronavirus were reported back in January, cybercrime has been on the rise. Cyber criminals are always looking for new and inventive ways to exploit weaknesses in our security, and the pandemic has presented a number of unexpected opportunities.

Working From Home

Thousands of employees have been forced to work from home as a result of Covid-19. This has made businesses more susceptible to cyber-attacks, with criminals targeting remote workers with inadequate security.

Influx of New Cyber Criminals

Covid-19 has had a crippling effect on the global economy, with millions losing their jobs as a result of the pandemic. This has had an unfortunate knock-on effect, as more and more people turn to cybercrime as a way to make money.

Delays in Detection and Response

With businesses attempting to save money and streamline operations, security has taken a hit. Budget cuts and redundancies have made it harder for organisations to detect malicious activities and respond accordingly.

What has caused this increase in cyber attacks?

- Organised crime groups see this as an opportunity to target organisations
- Opportunistic criminals will see quickly set up remote working practices as a vulnerability for organisations
- Increased online spending means more personal credit card details online

CYBERCRIME: THE THREAT TO YOUR BUSINESS

Malware

Malware is malicious software that allows hackers to gain access or cause damage to your network. It's notoriously difficult to detect, and devices are often infected without the user noticing. Malware attacks are becoming more sophisticated every year and remain one of the biggest threats to our privacy and security.

19

A small business is successfully hacked in the UK every 19 seconds[1].

Source: Hiscox

£652k

is the average cost of a successful ransomware attack on UK businesses[2].

Source: Sophos

Ransomware

Ransomware is a form of malware deployed by criminals to extort money. Using sophisticated hacking techniques, cybercriminals circumvent security and plant the ransomware on your computer, encrypting files so you are unable to access them. The attacker will then demand a fee (usually payable in Bitcoin) for a decryption key.

DDoS Attacks

A distributed denial-of-service (DDoS) attack is one of the most common and potentially damaging weapons in a hacker's armoury. By overwhelming a device or a network with traffic, a DDoS attack can disrupt normal service and effectively disable your website.

65,000 attempts to hack small and medium-sized enterprises (SMEs) occur in the UK every day[3].

Source: Hiscox

Phishing

Phishing is a cyber-attack often used to steal user data, including login credentials and payment information. It happens when an attacker, impersonates a trusted entity to trick the user in to opening an email, text message or instant message. If the user clicks on the malicious link, it opens the doors for cyber criminals to install malware, conduct a ransomware attack or start to expose sensitive information.

50%

of cyber-attacks in the UK involve phishing[4].

Source: Symantec

1, 3. Hiscox; UK small businesses targeted with 65,000 attempted cyber-attacks per day. 2. Sophos; Around 65,000 attempts to hack small and medium-sized enterprises (SMEs) occur in the UK every day; Paying ransom can double attack recovery costs. 4. Symantec; 2019 Internet Security Threat Report.

COUNTING THE COST: THE EFFECT OF A CYBER ATTACK ON YOUR BUSINESS

With cybercrime on the rise, it's more important than ever to take steps to protect your business against attacks. A security breach could have disastrous effects for your organisation, costing you thousands of pounds in revenue, exposing sensitive information and damaging the credibility of your brand.

46% of UK businesses + **26%** of UK charities reported a cyber security breach or cyber-attack in the last 12 months[1].

Among those businesses that fell victim to an attack... **1 in 5** ...lost money or data and two in five experienced disruption or loss of revenue[2].

Source: gov.uk

£3m

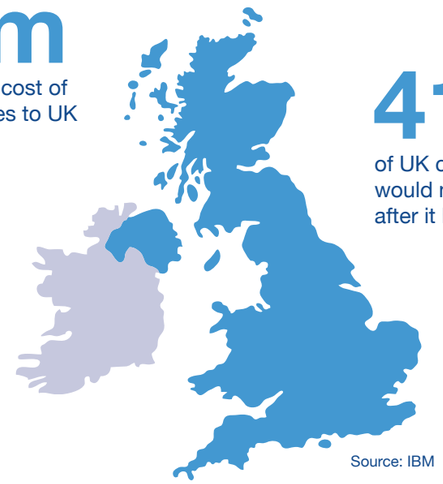
The average cost of Data breaches to UK businesses[3].

41%

of UK consumers say they would not return to a company after it had suffered a breach[5].

33%

of UK organisations say they lost customers following a data breach[4].



Source: IBM

1, 2. Gov.uk; Cyber Security Breaches Survey; 2020. 3, 4, 5. IBM; How much would a data breach cost your company?

HOW TO PROTECT YOUR BUSINESS

COVID-19 is a business critical issue, and paired with a cyber-attack during this time, it could have dire consequences for a business. To be protected, organisations are needed to remain vigilant and put practices in to place to protect their data and infrastructure. It is advised that instead of responding to cyber-attacks, organisations need to be monitoring networks for threats and risks. It is no longer enough to have basic fire walls in place, if organisations don't want to be victim to a expensive, and reputation-damaging breach, they should be looking in to how to best protect their digital assets and infrastructure.

To protect your organisation with round the clock monitoring, Security Operations Centre's are a cut above the rest. With 24/7 365 monitoring, assessing and reporting, there will never be an undetected breach that could put the organisation in jeopardy.

HOW DOES A SECURITY OPERATIONS CENTRE PROTECT MY BUSINESS?

The service includes intrusion detection, threat mining, SIEM and log management, dark web monitoring, file integrity monitoring, end point detection and response and continuous vulnerability monitoring.

With round-the-clock monitoring and real-time analysis, our specialist SOC team can prevent network violations and threats to your security.

SOC analysts interpret the results of vulnerability scans and provide expert advice and guidance.

WHAT ARE THE BENEFITS OF HAVING A SECURITY OPERATIONS CENTRE?

24/7 365 PROTECTION

We protect your business whilst you sleep, so no matter where you are, you know your business is protected.

DETAILED MONTHLY REPORTS

Providing a complete breakdown of your security, allowing you to make internal changes if required.

REAL-TIME SECURITY VIEW

Having a real time view allows us to identify and respond to threats in the moment.

TAILORED SERVICE

We work with you to identify the best solutions for your business and provide a service that you can count on.

ROUND THE CLOCK SUPPORT

Whether it be 3pm or 3am, if you need us, we're there.

COMPLETE PEACE OF MIND

You can relax, knowing you have the best protection in place for your business.

DigitalXRAID

CYBER SECURITY EXPERTS

At DigitalXRAID, we specialise in providing cutting-edge, market-leading cyber security solutions. We're experts in our field and our skills and experience are backed up by our extensive awards and certifications.

Cyber Security Awards

WINNER
START-UP OF THE YEAR

CIR Risk Management 10th ANNIVERSARY AWARDS 2019 shortlisted

FINALIST
CYBER SECURITY SERVICE OF THE YEAR

Doncaster Business Awards

WINNER
SME OF THE YEAR

Doncaster Business Awards 2019

WINNER
SME OF THE YEAR

Cyber Security Awards

RUNNER UP
CONSULTING PRACTICE OF THE YEAR

WINNER
PRESTIGE AWARDS

ISO 27001 CERTIFIED

ISO 9001 CERTIFIED

CYBER ESSENTIALS PLUS

IASME Consortium

CREST

CHECK
IT Health Check Service

Suite 9A Cavendish Court
South Parade, Doncaster
DN1 2DJ
UK

32 Cubitt Street
London
WC1X 0LR
UK

12 Tithebarn Street
Liverpool
L2 2DT
UK

01302 639 470 0207 183 3795 0151 329 0431

info@digitalxraid.com digitalxraid.com