Business Recovery and Growth Board

28 October 2021

Cybercrime affecting businesses in South Yorkshire

Is the paper exempt from the press and public?	No
Purpose of this report:	Discussion
Is this a Key Decision?	No
Has it been included on the Forward Plan?	Not a Key Decision

Director Approving Submission of the Report:
Helen Kemp, Director of Business and Skills

Report Author(s):
Muz Mumtaz
muz.mumtaz@southyorkshire-ca.gov.uk

Executive Summary

Cybercrime has increased significantly in the UK, in the past 18 months, during the various national lockdowns imposed, as a result of the COVID-19 pandemic, and now accounts for 50% of all fraud committed (according to PWC's Global Crime Survey).

The South Yorkshire region has also experienced a significant increase in cybercrime, particularly targeted at local businesses, with just under 40% of firms reporting such attacks, with an estimated loss in revenue exceeding £68 million (from actual incidents reported). However, with almost 72% of attacks not reported (according to the Department for Digital, Culture and Media), the true cost of cybercrime affecting the South Yorkshire economy could be as high as £243 million per year.

The nature of online fraud, both regionally and nationally, has mainly been in the form of either ransomware attacks (servers/systems hacked with data stolen) or phishing (email hacks that encourage recipients to click a link).

Business support interventions which help businesses protect themselves against cybercrime have traditionally been delivered via modules/webinars on cybercrime in the South Yorkshire

region. However, with the advancement of technology, cybercriminals have become even more sophisticated in their methods of targeting and defrauding local businesses.

Hence, this paper sets out the context for cybercrime trends/activity in South Yorkshire affecting businesses and provides a number of options/interventions to support local businesses protect themselves.

What does this mean for businesses, people and places in South Yorkshire?

Cybercrime targeted at local businesses in South Yorkshire has resulted in many businesses being unable to operate. Cybercriminals typically attack the online presence of local firms affecting their business processes and operations. Unless business owners and employees are made more aware of the methods and technologies to protect their business operations, more revenue will be lost to cybercriminals in the region, with business failures also rising.

Recommendations

Consideration by any other Board, Committee, Assurance or Advisory Panel
None

---

1. Background

1.1 Businesses across all sectors of the economy in the South Yorkshire region have invested heavily in developing their digital/online presence, over the past several years, in order to remain competitive and to realise growth, by providing their customers with alternative channels to access/purchase their products or services.

This trend accelerated over the past 18 months, as a result of the national lockdowns imposed by government, due to COVID-19, which meant that businesses needed to rapidly pivot towards digital platforms/channels in order to continue to trade, due to the closure of business premises.

1.2 Also, with many offices and shops closing, many business owners and their employees have been running their businesses remotely/from home, during the pandemic.

Hence the digital resilience of businesses has never been so critical to the local economy, which relates to the ability of business owners to not only protect their business operations from online attacks but also to develop plans for recovery, if they suffer from a cyber attack.

1.3 Unfortunately, cybercriminals have been increasingly active across the UK and in the South Yorkshire region, taking advantage by exploiting the vulnerabilities evident in the digital channels operated by businesses, reflecting in a rise in online fraud, over the period.

2. Key Issues

2.1 According to research commissioned by the Department for Digital, Culture, Media and Sport (DCMS), almost 40% of the businesses experienced some sort of the

cybercrime in 2021, which equates to over 7,500 businesses in the South Yorkshire region. Larger firms were worse affected (65%).

2.2 The average cost of an attack to an SME was estimated to be around £8,460, with larger firms losing as much as £13,400. Aggregated across the regional economy, this amounts to over £68 million in lost revenue for businesses per year. However, this is only the tip of the iceberg, since as much as 72% of cybercrime goes unreported by business owners due to a number of reasons including the risk of reputational damage.

2.3 The most common types of cybercrime include:

- Ransomware – data stolen by hackers through malware etc with owners asked to pay a ransom to release data or prevent its publication.
- Phishing – with almost 80% of firms reporting this type of attack, which comes in the form of an email with links to fake websites.
- Home working – exploiting vulnerabilities including outdated anti-virus software or older operating systems (which no longer receive updates)
- Wider online fraud – including Denial of Service (DoS) attacks which flood a server with data/traffic causing a network to crash.

2.4 With many business owners and staff working remotely/at home due to the pandemic, fewer firms have been able to administer cyber security measures including security monitoring tools etc. Also, only a third of businesses have been using VPNs (encrypted data communications) when working from home.

In addition, upgrading hardware and software systems to improve resilience became more challenging during the pandemic, logistically, with employees and managers working from home.

2.5 Many local organisations are engaged in supporting local businesses to protect themselves from cybercrime, including through raising awareness to offering technology solutions. Organisations that can offer businesses advice and support on protecting themselves against future cyber threats include:

- South Yorkshire police and the Regional Cyber Crime Unit
- The National Cyber Security Centre
- Private IT support providers and suppliers
- Chambers of Commerce (see below)
- The Yorkshire Cyber Security Cluster – helping businesses/organisations to build stronger standards of cyber security. The cluster are developing an online directory of local cyber security firms that can assist local firms.
- The North East Business Resilience Centre, which specialises in cyber security programmes for small firms.

- Other professionals, trade bodies, or peer networks.

The South Yorkshire Chambers of Commerce ran a Cyber security event on October 14th for its members called "How to avoid losing your entire business in 30 seconds" which included the following items on the agenda, delivered by several partner organisations:

- **Latest cyber security insights** from South Yorkshire businesses Steve Hughes, Policy Points
- **Cybercrime - The threat for businesses** - Eliza-May Austin, th4ts3curity.company
- **Perspectives from The National Cyber Security Centre (NCSC)** A representative from NCSC
- **Business Reliance and Support Resources** - Danielle Lee, South Yorkshire Police and Steve Leach, North East Business Resilience Centre (NEBRC)

2.6 The event above was prompted by the Chamber's quarterly business survey which indicated the need for greater support to help businesses protect themselves. The survey was carried over the summer of 2021 and included a sample of 572 firms.

Key findings from the survey on cybercrime included:

- 10% of respondents were not confident they could protect themselves from a cyber-attack, whilst 53% were confident that they could.
- 85% of respondents thought that cyber security was a high priority for their business.
- Online training courses on cybercrime were felt to be the most useful way for improving understanding about the issue for 46% of respondents, followed by IT providers (27%). 26% of firms indicated that either the National Cyber Security Centre website or regular newsletters would help keep them informed and protected.

The Mayoral Combined Authority have asked for the addition of 3 questions on cybercrime in the next Chamber survey, taking place between October and December 2021, with results expected in the new year.

3. Options Considered and Recommended Proposal

3.1 **Option 1**
Deliver a Cybersecurity Summit/event, involving local/regional partners, to an audience of local businesses, from all sectors. The event could either be an online event, which is more scale-able or a series of local events held in each local authority area of the region.

3.2 This option would be resource intensive for the MCA, requiring at least one officer's dedicated time to organise the event, marketing and promotion + managing invitations and partners/suppliers to attend.

3.3 **Option 1 Risks and Mitigations**

- Low or poor attendance at the Summit/event – the risk is low and can be mitigated by affective marketing to clients.
- Insufficient resource in the MCA to manage one or several local physical events. The risk is medium as the MCA have struggled with resources to date.

3.4 **Option 2**

Promote future cybersecurity events organised by partners organisations only, through our monthly e-newsletter and social media platforms, referring enquirers to partners including the Chamber of Commerce or the Yorkshire Cybersecurity cluster who may organise events in the near future, partnered by the MCA.

3.5 **Option 2 Risks and Mitigations**

This option is seen as relatively low risk, in terms of probability or impact as this is a referral only intervention.

The only risk would be for the exclusion of non-members of the Chamber of Commerce. However, this could be mitigated by agreeing invitations with the Chamber in advance and supporting the costs for delivering such events.

3.6 **Option 3**

Development of a cyber security programme delivered by a specialist agency, such as the North East Business Resilience centre (NEBRC), which can provide bespoke advice to business and access to a wide range of online resources including webinars and tool on cybersecurity.

3.7 The NEBRC delivered a similar programme for West Yorkshire, at a cost of £100,000 in 2020. The programme assisted 174 businesses over a 6 month period, bespoke advice and support.

The programme includes student placements – (many of which are sourced from Sheffield University). It also provides links to organisations that can offer discounted training on Cyber Essentials (£300 per organisation).

3.8 **Option 3 Risks and Mitigations**

The risks with this option include the limited number of SMEs supported with the programme. However, this could be mitigated by determining the demand for such support and to commission a programme to meet the scale of demand.

3.9 **Recommended Option**

No recommendation is provided, as this is a discussion paper and the Board will need to determine their priorities and the resources (if any) they would wish to dedicate to tackling this issue.

4. Consultation on Proposal

4.1 All internal teams in MCA have been consulted on this paper.

5. Timetable and Accountability for Implementing this Decision

5.1 This is a discussion paper for the October Board – any timetable for implementation may follow the Board meeting.

6. Financial and Procurement Implications and Advice

6.1 There is currently no budget for a cybersecurity event / programme (option 3) or for marketing, promotional and event hire costs (option 2). Funding would therefore need to be found from within existing budgets or a budget change request submitted for consideration.

7. Legal Implications and Advice

7.1 The options fall within the Authority's functions relating to Economic Development and Regeneration of the Combined Authority area.

8. Human Resources Implications and Advice

8.1 None currently – as Board will need to determine if any course of action is preferred.

9. Equality and Diversity Implications and Advice

9.1 None/not applicable at this time.

10. Climate Change Implications and Advice

10.1 None/not applicable at this time.

11. Information and Communication Technology Implications and Advice

11.1 None/not applicable at this time.

12. Communications and Marketing Implications and Advice

12.1 None/not applicable at this time.

List of Appendices Included
None

Background Papers
None