Approaches to cyber security in small and medium-sized enterprises: Why it needs to change

Received (in revised form): 2nd May, 2023

Simon Newman
Chief Executive Officer, Cyber Resilience Centre for London, UK

Simon Newman is the Chief Executive Officer (CEO) of the Cyber Resilience Centre for London — a not-for-profit organisation owned by the Mayor's Office for Policing and Crime and part of a national network of centres covering England and Wales. As CEO, Simon leads a small team to help small and medium-sized enterprises reduce their vulnerability to common cyber threats by working in partnership with central and local government, industry and academia. During his career, Simon has held a number of senior management positions across the public sector. Prior to his current role, he was Head of Business and Government Engagement at Police Crime Prevention Initiatives, where he was responsible for the Police Digital Security Centre and the Community Safety Accreditation Scheme. Simon has spent much of his career in the public sector including roles at the National Policing Improvement Agency and the Home Office, where he was Programme Director with responsibility for setting up the National Police Air Service. He has also worked overseas as a Strategic Adviser to the Ministry of Interior and Abu Dhabi Police in the United Arab Emirates. In addition to his current role, he is an Associate Trainer for Dods Group Plc and recently became an Honorary Visiting Fellow at City, University of London.

Cyber Resilience Centre for London, City, University of London, Northampton Square, London, EC1V 0HB, UK
E-mail: simon.newman@londoncrc.co.uk

Abstract Over the last decade, the growth in technology has created numerous opportunities for businesses to improve efficiency, develop new products and services and reach new customers. But it has also provided an opportunity for the criminal fraternity to find new, and incredibly lucrative, ways of targeting victims from anywhere in the world. This has led to cybercrime becoming one of the fastest-growing types of crime affecting individuals, businesses and third-sector organisations alike. For example, in England and Wales, official government statistics show the number of cybercrime incidents has risen by 89 per cent in the past year alone. This paper describes the effect cybercrime has on small and medium-sized enterprises (SMEs), in particular those at the smaller end of the spectrum. The paper explains why SMEs are among the most vulnerable to a breach or an attack and what challenges they face against this growing threat. The paper also describes what the UK government is doing to support SMEs specifically.

KEYWORDS: SME, cyber security, phishing, cyber breach, cyberattack, supply chains, cyber resilience

INTRODUCTION

Before we begin, it is important to understand the demographic footprint of businesses in the UK. According to a recent House of Commons report,[1] there were approximately 5.5m businesses registered in 2022 — a rise of 2 million since the year 2000. Further analysis of the data shows,

however, that just over 5.2m (95 per cent) have fewer than nine employees, with 74 per cent having no employees at all. Despite the UK having a reputation as a global centre of commerce, there are just 8,000 larger employers nationwide (ie those with more than 250 employees) (see Table 1).

These small and medium-sized enterprises (SMEs) increasingly rely on technology to carry out their business. The Cyber Breaches Survey,[2] published each year by the Department for Digital, Culture, Media and Sport (DCMS), estimates that 92 per cent of businesses have at least one form of online presence. Whether this means using online banking, having a website with e-commerce capability or using social media to promote their business services or products, they are often the most vulnerable to cybercrime, with four out of ten having suffered at least one attack or breach in the past year. Using the figures from the House of Commons report, that equates to over 2m SMEs who fell victim to cybercrime in the past 12 months (see Figure 1).

Table 1: Business demographics by size (2022)

	No. of businesses	Size
	5.47m	Small (0–49 employees)
	35,900	Medium (50–249)
	7,700	Large (250+)
Total:	**5.5 million**	

Source: Office of National Statistics, UK

Yet despite these figures and the risks these organisations face, we know that there are still too many SMEs who fail to take cyber security seriously. To understand the reasons why, it is important to understand *how* they are vulnerable.

WHY AND HOW SMES ARE VULNERABLE TO CYBERCRIME

One of the main reasons is the use of the term 'cyber', which is often poorly understood by many small businesses. Through our Community Outreach programme at the Cyber Resilience Centre for London, we often hear business owners saying that they get confused by the terminology or cannot understand how it

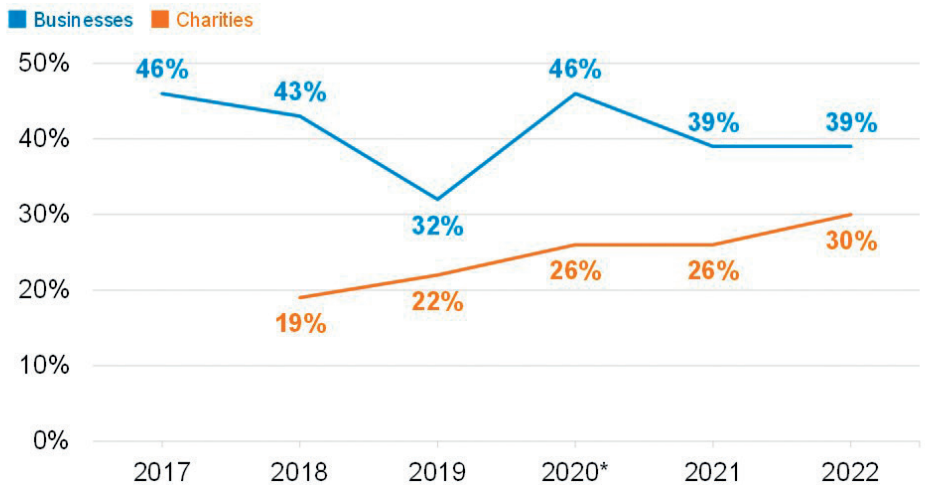

Figure 1: Percentage of SMEs suffering cyberattacks or breaches in 2022[3]
Bases: 1,000+ UK businesses per year; 300+ charities per year
*N.B. the weighting approach for businesses was changed for 2020, although this is expected to have a negligible impact on comparability to previous years. Full details of the change are available in the technical annex.

affects their business in the same way as more traditional forms of crime do. Terms such as 'phishing', 'whaling' and 'DDOS attacks' are still relatively unknown – particularly among micro businesses and sole traders.

We also hear business owners say that it is something their outsourced IT provider deals with, rather than themselves or a specific member of their team. As the Cyber Breaches Survey states, these businesses 'often had a fear of the technicalities of cyber security and a preference to not research and mitigate against the risks they presented. They knew there could be a potentially devastating impact, but were not sure of the specifics of this, and felt it was low probability.'[4]

Another issue concerns the rise and evolution of phishing. In 2022, phishing was the most common and most disruptive form of cyberattack, with 83 per cent[5] of businesses having reported at least one phishing attempt in the past year. As we saw with the global COVID-19 pandemic, cybercriminals were quick to exploit the opportunities it presented during a time of rapid change. This included mimicking official government agencies to entice victims to click on malicious links. We also saw a significant increase in phishing attacks following the invasion of Ukraine by Russia in February 2022, where cybercriminals pretended to be legitimate fundraising organisations collecting donations for those displaced by the conflict. According to the SlashNext State of Phishing Report 2022,[6] there were 255m attacks in 2022 — an increase of 61 per cent on the previous year (see Figure 2).

Figure 2: Percentage of identified types of breaches or attacks in the last 12 months, among the organisations that have identified any breaches or attacks[7]

Perhaps one of the most frustrating issues concerns the way in which SMEs view the data they hold, with many failing to understand its value. Whether this includes customer records, details of suppliers or intellectual property, data is arguably an emerging currency for cybercriminals, who can use it to commit secondary fraud or sell it on to other criminals. The challenge here is that business owners do not understand that this type of information is of any value and, consequently, do not think they will be a target. Yet, as we have seen recently, some fairly sophisticated attacks have been targeted at a number of small businesses, underlining the importance of securing data irrespective of their size.

THE THREAT FROM SUPPLY CHAINS

Arguably the greatest threat SMEs face is through supply chains. The rise in globalisation and demand from consumers means that supply chains are becoming increasingly complex and lengthy. They are naturally an attractive target for cybercriminals as a large proportion of the companies in these supply chains are SMEs. According to ENISA,[8] the European Union's cyber security agency, supply attacks were expected to quadruple between 2020 and 2021.

So, what is behind this increase in supply chain attacks and why are SMEs such a target for cybercriminals? Well, there are two main reasons for this rise. First, over the past few years, larger organisations have invested heavily in their own security posture, making it much more difficult for attackers to be successful. This has led cybercriminals to look for easier and less direct ways of targeting such organisations — ie suppliers. Secondly, SMEs are likely to be suppliers to many other firms and therefore, if an attacker can successfully infect the systems of one SME, it is highly likely that it will infect the systems of other organisations it supplies as well. This was a key feature of the Solar Winds[9] attack in 2020.

But another reason supply chain attacks are so commonplace, and devastating, is that reviewing the cyber resilience of suppliers is considered a low priority for most larger companies. Only 13 per cent[10] of larger businesses say that they regularly review the security of their immediate supply chain, with only 7 per cent reviewing their wider supply chain where 'some firms admitted that there tended to be some complacency at board level when considering supplier risks'.[11]

SEEKING ADVICE AND GUIDANCE: THE ABSENCE OF INFORMED CUSTOMERS

SMEs also face a challenge in terms of who they turn to for specialist advice and support. The UK government's Cyber Security Sectoral Analysis Report[12] shows that revenue among cyber companies grew to over £10bn last year, but how do SMEs know which vendor, product or service is right for them if they do not understand their own security posture? We know that many smaller companies are put off by cost, a lack of confidence in being able to have an informed discussion with vendors about their needs and an implicit trust in the cloud. As the Cyber Breaches Survey confirms, however, 'smaller organisations took little proactive action on cyber security, driven by a lack of internal knowledge and competing priorities with their budgets'.[13]

Of course, we cannot ignore macro issues affecting SMEs. Current global events, such as the war in Ukraine, a slowdown in the economy and the rise in energy prices (particularly in the UK), are undoubtedly having an impact on how SMEs view cyber security. At times of crisis, the primary focus of every business is survival, meaning that cyber security falls down the priority list.

THE CYBERCRIME PARADOX: VOLUME OF INCIDENTS VERSUS IMPACT

It goes without saying that the impact of cybercrime can be devastating for some. In the USA, it has been suggested that as many as 60 per cent of small businesses which suffered a cyberattack go out of business within six months — although this figure has been widely disputed by the US National Cyber Security Alliance.[14] The reality is that we simply do not know how many businesses fail due to a cyberattack or breach — whether it was the primary reason for the failure, a contributory factor or completely irrelevant.

What we do know, however, is that in the vast majority of cases, the impact of an attack or breach is negligible. The Cyber Breaches Survey[15] shows that of the 39 per cent of businesses who suffered an attack or breach in the last 12 months, only one in five actually suffered a negative impact. This is particularly true if the incident is caused by 'viruses or ransomware, account takeovers, hacking attempts or other unauthorised access'. Permanent loss of data is even rarer with only 1 per cent of businesses reporting it. Surprisingly, phishing, arguably the most common type of attack, appears to have little impact.

The Cyber Breaches Survey also tells us the time it takes for a business to recover from an incident, with 89 per cent of businesses stating that they fully recover within 24 hours and 70 per cent saying that it took no time at all to recover.[16]

It is a similar picture with the financial impact of cybercrime. Again, the impact seems negligible, with the majority of business surveyed saying that it did not cost them anything at all to recover. This could be due to a lack of understanding about the impact or the ability of the business to calculate the cost, but even taking this into account, few small businesses appear to have suffered catastrophic losses.

For many businesses, therefore, the cost and effort required to implement controls when measured against the impact of an attack or breach means that 'doing nothing' is a risk that many are willing to take and may explain why there is such a low take-up of preventative measures.

THE GROWTH OF CONSUMER PROTECTION: REIMBURSING MONEY LOST TO FRAUD

There is also another factor which may influence behaviour and in particular, encourage greater risk taking when it comes to cyber security: 'no blame reimbursement'. It is estimated that in the UK in 2020, 98 per cent[17] of victims of fraud who suffered financial losses were reimbursed by their banks. This followed the introduction of a voluntary Code of Conduct for the banking sector in 2019 which sought to better protect consumers from advanced push-payment (APP) fraud. An APP fraud is where victims pay in advance for goods or services that they never receive.

The Code means that signatory banks agree to fully reimburse victims of APP fraud unless it can be proven that they were negligent — for example, sharing log-in details of their bank account with others. Earlier this year, the Lending Standards Board, which oversees the voluntary Code, announced an update placing further responsibility on banks[18] which makes it harder for them to avoid paying out.

While the Code is aimed primarily at consumers, some banks are extending this approach to customers with business bank accounts. TSB bank, one of the original signatories to the Code of Conduct, now offers its business customers 'guaranteed fraud protection'[19] of up to £1 million. Others may follow.

If banks are reducing, or in some cases eliminating, risk, it becomes harder to motivate business owners to change their behaviour towards the threat from cybercriminals. It may also encourage cybercriminals to specifically target the UK,

knowing that customers rarely bother with implementing security measures because they will almost certainly be reimbursed for any losses.

So, should we even bother investing so much time and effort in trying to change behaviour when the impact is negligible?

OVERCOMING THE CHALLENGES: HOW TO REDUCE VULNERABILITY AMONG SMES

In the previous section, we looked at the threat and the challenges policy makers face when encouraging SMEs to change their behaviour. In this section, we will focus on what SMEs should do to reduce their vulnerability to cybercrime and what part the cyber security industry can play in helping to address these challenges.

From our experience of speaking to thousands of small businesses across London, the first and most important thing to do is to ensure that business owners properly understand the risks they face in a language they understand. This means demystifying the complex terminology we use as professionals in the industry when speaking to them. Business owners generally have a good understanding of risk, and they know how their bottom line may be affected by factors such as the cost of raw materials, rising energy prices or broader economic conditions. They are also incredibly busy people, but taking the time and effort to properly understand cyber risk is still perceived as too difficult and overly time-consuming. That said, we have started to see a shift in focus where much of the messaging is based around everyday language and is now being increasingly targeted at specific sectors to make it far more relatable to individual business owners. Time will tell whether this approach makes a significant difference to vulnerability, but early indications from the engagement we have seen over the past few months through our Community Outreach programme have been positive.

GETTING THE TONE OF MESSAGE RIGHT: MOVING FROM USING FEAR TO FOCUS ON THE POSITIVES

Directly related to this point is the tone of the message. Identifying 'what works' for SMEs is a key priority for many cyber security companies and government organisations trying to make a difference to the way SMEs address their cyber risk. While demystifying the language we use can help, it is no good if we cannot get the messaging right. For example, there is a significant volume of cyber security content available to SMEs from a wide range of sources and in many different formats. Much of it is extremely good. The messaging is not getting through enough, however, as the number of SMEs falling victim to cybercrime has increased over the last few years.

We also know that using 'shock tactics' to illustrate the terrifying impact of a cyberattack does not work either. In many cases, SMEs in particular simply switch off and are less likely to engage in the future. This makes them even more vulnerable. What we need to see in cyber security messaging is a step change in the way we deliver it.

Going back to the previous point about the importance of making the language we use in cyber security relevant and relatable to small business owners, we should focus our efforts on describing the benefits of implementing cyber security control measures. This is not just about reducing organisational vulnerability to cybercrime, but about seeing it as an investment to grow and innovate. Once business owners see how simple measures can deliver tangible benefits from good cyber security hygiene practice, then I am confident that we will see a significant uptake in adoption. The use of case studies can really help here and bring examples to life.

GETTING THE BASICS RIGHT

Another fundamental, yet often overlooked solution is the need to start off by helping

the smallest businesses get the basics right in terms of their cyber security. This is not about outsourcing everything to an external provider, buying an off-the-shelf technical solution or signing up to a subscription service that monitors traffic, but about doing the really simple things that every organisation, irrespective of size, should have in place. Why is this so important? Microsoft's[20] Digital Defence Report shows that 98 per cent of all cyberattacks can be prevented by implementing basic control measures. This means making sure that organisations have a robust password policy in place, implement two-factor or multi-factor verification and set up automatic updates. It also means ensuring data is backed up, access to key systems is restricted to reduce the likelihood of unnecessary data leaks, and staff regularly receive awareness training about the latest threats. Yet too few organisations do this.

CHANGING CULTURE: THE PANACEA TO ADDRESS THE PROBLEMS CAUSED BY CYBERCRIME?

A key part of 'getting the basics right' is how an organisation embeds cyber resilience into its culture. The majority of data breaches within organisations are the result of human actors,[21] so it is essential that security awareness training forms part of a wider cyber security culture (CSC) that concerns 'the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies'.[22] CSC is about making information/cyber security considerations everyone's responsibility and an integral part of an employee's job, habits and conduct. Of course, CSC only works if senior management are bought into it, and it is incorporated directly into organisational goals through monitoring of key performance indicators. Many businesses, however, are starting to recognise the importance of CSC, which suggests a greater understanding of its value in organisational resilience.

CSC may also include compliance with relevant standards and compliance with appropriate cyber security accreditations. For most small to medium businesses in the UK, this means the government's flagship Cyber Essentials scheme,[23] which was launched in 2014 and designed around five key controls. Since its introduction, many public sector organisations (as well as some larger companies) are now insisting on Cyber Essentials as the minimum standard of security for their suppliers, which has led to a sharp rise in the number of certificates issued over the past few years.

But despite this, take-up is still low among those who are most vulnerable to cybercrime. SMEs are reluctant to invest in measures they do not understand or fail to see the value in and in many cases, Cyber Essentials adoption is driven by necessity — perhaps as a requirement as part of a supplier contract as opposed to an active interest in achieving compliance.

Leadership and accountability in how cyber security is manged within an organisation is another important element that can help make a difference to vulnerability from common threats. For sole traders and micro businesses, this responsibility usually rests with the owner, among many other responsibilities, but for larger SMEs which may have a board of directors, identifying or nominating a board member with specific responsibility around cyber security should be a priority. According to the Cyber Breaches Survey, however, only 34 per cent of businesses have a board member with specific responsibility for cyber security — and the trend is going down.[24]

Finally, most businesses will have some form of business continuity plan in place to deal with certain types of incidents, such as power outages or flooding. These plans help the business deal with the incident and

ensure that it can get back up and running as quickly as possible. It therefore makes sense to adopt exactly the same approach to cyber threats, especially if the SME suffers a breach or an attack — particularly where they may be unable to access key systems. Encouragingly, there has been a significant increase in the number of businesses in the UK which have a dedicated incident response plan in place (93 per cent in 2021 from 66 per cent in 2020).[25] This increase may have been driven by the pandemic and the sudden change to remote working which prompted many organisations to review their security posture.

Of course, having a plan in place is one thing, but it is absolutely no good if it just sits on a shelf gathering dust. Reviewing plans and exercising them regularly can help identify gaps and allow them to be adjusted for changes in the threat landscape.

LEARNING THE LESSONS: HOW TO IMPROVE THE CYBER RESILIENCE OF SMBS

Looking further ahead in terms of the levers available to government, what lessons can the UK learn from how other countries have attempted to tackle the problem SMEs face from cybercrime and what is the likelihood of these measures being effective in the current climate?

Several countries have recognised the cyber threat facing SMEs and have developed a range of initiatives which seek to educate SMEs about the importance of good cyber security. The European Union Agency for Cybersecurity, ENISA[26] has been at the forefront of this, producing several guides and toolkits for SMEs across member states.

At the heart of these initiatives is partnership. Cyber cuts across every sector and it can often be difficult to identify a single agency or government department to lead the response against the threat. Instead, it is often dealt with by a multitude of government agencies and arms length bodies. To give an example of how this manifests itself in the UK, cyber policy is primarily the responsibility of the DCMS. Yet, the Home Office, HM Treasury and the Department of Business, Energy and Industrial Strategy (BEIS) also have a significant interest, not to mention the intelligence services, Ministry of Defence and of course, the National Cyber Security Centre (NCSC), part of the government's Communications Service. That is why the development of National Strategies to prioritise activities and bring together relevant agencies is so important to tackling the threat faced by SMEs. The UK recently launched its new National Cyber Strategy[27] which seeks to do exactly that and identifies the cyber resilience of SMEs as a key pillar.

THE POWER OF LEGISLATION: IS IT TIME TO MANDATE MINIMUM STANDARDS IN CYBER?

Another route that some countries have taken is to look at introducing legislation that stipulates minimum cyber security standards for businesses — such as the UKs flagship Cyber Essentials scheme. While most governments are generally reluctant to impose additional bureaucracy on businesses, the scale of the threat to SMEs and the limited success of existing initiatives to reduce the number of victims significantly, may encourage some administrations to rethink their approach to legislation. In November 2022, the UK government announced plans[28] to boost cyber laws in order to reduce the disruption caused by attacks. Although aimed primarily at outsourced IT providers (many of whom are SMEs themselves) the proposed legislation enables the government to create additional laws in the future to address threats to supply chains.

Should we now consider making Cyber Essentials mandatory for all SMEs? Arguably, it would create challenges for business owners, but it would clearly demonstrate a firm commitment from the UK government to tackle cyber risk.

MANDATORY REPORTING?

Closely related to the potential for proscribed minimum standards is the need for mandatory reporting of incidents. It is estimated by the Office for National Statistics[29] that only 3–5 per cent of cyber incidents are reported to the relevant authorities. There are a number of reasons as to why reporting rates are so low among SMEs. It may be because they do not consider the incident sufficiently serious enough to report it, or, it may be because the police are way down their list of people to contact in the event of an attack or breach. In some cases, it may be because the SME is not aware that they have been a victim of a cyberattack. Whatever the reason, under-reporting poses a huge problem for policymakers. The less they understand about the problem, the less effective the response.

So, is mandatory reporting a way forward? The US recently introduced the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA),[30] signed into law in March 2022, which will 'require critical infrastructure companies, including financial services, to report cybersecurity incidents, such as ransomware attacks, to the Cybersecurity and Infrastructure Security Agency (CISA)'. Australia[31] has taken a similar path. While these laws are aimed primarily at critical national infrastructure, it seems somewhat inevitable that it is only a matter of time before law makers start to consider extending these rules further.

BOARD DIRECTORS PERSONALLY LIABLE FOR CYBER BREACHES

An issue that we see too commonly among Directors of SMBs is a lack of understanding of their exposure to cyber risk. One (somewhat controversial) idea to address this is to make Board Directors personally liable for major attacks or breaches. The recent case in the USA against Uber's former Chief Security Officer,[32] who was convicted of criminal obstruction for failing to report a cyber breach to the relevant authorities, demonstrates an increasing toughness from regulators. While there were underlying factors behind the conviction, UK regulators will be following events across the pond carefully. Although cases like these are less likely against the owners of SMEs, it does not take too much of a leap in imagination to see something like this catching SMEs out.

CONCLUSION: STRIKING THE RIGHT BALANCE BETWEEN EDUCATION AND GOVERNMENT INTERVENTION

In conclusion, the threat to SMBs continues to grow, with very limited success in making an impact. Cyber threat will evolve, but businesses are still falling victim to common attacks that in the majority of cases can be addressed by getting the basics right. Similarly, the importance of getting the messaging right should not be underestimated, nor should the role larger companies (particularly those in supply chains) must play in helping their SME customers improve their cyber resilience.

In this paper, I have looked at the role of partnerships and the importance of joined up working across government and specifically, considered the levers that governments can press in relation to legislation. I have also commented on the work that is being done internationally to support SMEs.

The UK is not alone in the threat it faces and is putting significant money and effort into addressing the problem, but we also need to get better at targeting those hard-to-reach SMEs who typically do not engage with government, yet are arguably the most vulnerable when it comes to cyber risk. In a world where technology is becoming increasingly impossible to escape, let us not forget that it is not just about risk, but that there are some incredible opportunities for businesses to take advantage of. Effective cyber resilience has to be at the heart of this.

Summary of key issues and recommendations

Issue	Recommendation
Terminology and language	• Simplify the language used in cyber messaging to ensure better understanding • Ensure messaging is relatable to specific industry sectors and not overly generic • Better use of positive language as opposed to scare tactics in cyber messaging • Reward positive behaviour and good practice
Phishing	• Encourage more regular security awareness training for all staff (including Directors) • Ensure business continuity plan in place and regularly reviewed and exercised
Understanding the value of data	• Ongoing training for businesses to help them understand the value of data they hold
Supply chain resilience	• Ensure regular review of first and second tier supply chain to identify potential threats • For larger companies, work with SMBs in supply chains as more of a partnership to help reduce risk
Lack of informed customer	• Better education and guidance for SMBs to help them understand what their managed service provider (MSP) can and cannot provide
Getting the basics right	• Produce positive 'success' stories that are industry specific to make them relevant to SMBs

References

1. Hutton, G. (December 2022), 'Business statistics', House of Commons, available at https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf (accessed 2nd May, 2023).
2. Department for Digital, Culture, Media & Sport (DCMS) (July 2022), 'Cyber Security Breaches Survey (2022)', Gov.UK, available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#overview (accessed 2nd May, 2023).
3. *Ibid*.
4. *Ibid*.
5. *Ibid*., Ch. 5.
6. SlashNext, 'The State of Phishing 2022', available at https://www.slashnext.com/the-state-of-phishing-2022/ (accessed 2nd May, 2023).
7. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above.
8. European Union Agency for Cybersecurity (ENISA) (July 2021), 'Threat Landscape for Supply Chain Attacks', available at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (accessed 2nd May, 2023).
9. Oladimeji, S. and Kerner, M. (June 2022), 'SolarWinds hack explained: Everything you need to know', TechTarget, available at https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (accessed 2nd May, 2023).
10. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above, Ch. 4.
11. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above.
12. Department for Digital, Culture, Media & Sport (DCMS) (February 2022), 'Cyber security sectoral analysis (2022)', Gov.UK, available at https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022/cyber-security-sectoral-analysis-2022#profile-of-the-uk-cyber-security-sector (accessed 2nd May, 2023).
13. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above.
14. National Cybersecurity Alliance (May 2022), 'Statement Regarding Incorrect Small Business Statistic', available at https://staysafeonline.org/news-press/press-release/national-cyber-security-alliance-statement-regarding-incorrect-small-business-statistic/#:~:text=Washington%2C%20D.C.%20%E2%80%93%20The%20National%20Cyber,cannot%20verify%20its%20original%20source (accessed 2nd May, 2023).
15. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above, Ch. 5.
16. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above.
17. Murray, A. (September 2020), 'Have you been the victim of fraud? Here's our ultimate guide to getting your money back and the rules that can help you', This is Money, available at https://www.thisismoney.co.uk/money/news/article-8710235/Been-victim-fraud-Heres-guide-getting-money-back.html (accessed 2nd May, 2023).
18. Shaw, V. (February 2023), 'Banks receiving scam payments to take more responsibility

under code update', *The Independent*, available at https://www.independent.co.uk/money/banks-receiving-scam-payments-to-take-more-responsibility-under-code-update-b2278295.html (accessed 2nd May, 2023).
19. TSB, 'TSB Fraud Refund Guarantee', available at https://www.tsb.co.uk/Fraud-Prevention-Centre/Fraud-Refund-Guarantee/ (accessed 2nd May, 2023).
20. Microsoft (2022), 'Microsoft Digital Defense Report 2022', available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us (accessed 2nd May, 2023).
21. Ponemon Institute (January 2012), 'The human factor in data protection', available at https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf (accessed 2nd May, 2023).
22. European Union Agency for Cybersecurity (ENISA) (2017), 'Cyber Security Culture in Organisations', available at https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (accessed 2nd May, 2023).
23. National Cyber Security Centre (NCSC), 'About Cyber Essentials', available at https://www.ncsc.gov.uk/cyberessentials/overview (accessed 2nd May, 2023).
24. Department for Digital, Culture, Media & Sport (DCMS), ref. 2 above.
25. *Ibid.*, Ch. 6.
26. European Union Agency for Cybersecurity (ENISA), 'SME Cybersecurity', available at https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity (accessed 2nd May, 2023).
27. Cabinet Office (December 2022), 'National Cyber Strategy 2022 (HTML)', Gov.UK, available at https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (accessed 2nd May, 2023).
28. Department for Digital, Culture, Media & Sport (DCMS) and Lopez, J. MP (November 2022), 'Cyber laws updated to boost UK's resilience against online attacks', Gov.UK, available at https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks (accessed 2nd May, 2023).
29. Office for National Statistics (ONS), 'Nature of fraud and computer misuse in England and Wales: Year ending March 2022', available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 (accessed 2nd May, 2023).
30. Bailey, T., Greis, J., Watters, M. and Welle, J. (June 2022), 'Cybersecurity legislation: Preparing for increased reporting and transparency', McKinsey & Co., available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency (accessed 2nd May, 2023).
31. Ashurst (July 2022), 'Mandatory cyber incident reporting now live for Australia's critical infrastructure', available at https://www.ashurst.com/en/news-and-insights/legal-updates/mandatory-cyber-incident-reporting-now-live-for-australias-critical-infrastructure/ (accessed 2nd May, 2023).
32. *The Guardian* (October 2022), 'Former Uber security chief found guilty of concealing data breach', available at https://www.theguardian.com/technology/2022/oct/05/uber-joe-sullivan-former-security-chief-guilty-data-breach#:~:text=A%20San%20Francisco%20jury%20has,2016%20cybersecurity%20incident%20to%20authorities (accessed 2nd May, 2023).