State of the Art Review

What do we know about cyber security in small firms?

Joanne Turner
Enterprise Research Centre
Joanne.E.Turner@wbs.ac.uk

SOTA Review No 63: September 2024

Digitalisation – the application of digital technologies and infrastructures – is associated with higher productivity, value added and employment. However, with digitalisation comes a reliance on cyberspace that has brought about new digital threats and risks for firms. Cyberspace has transformed the crime environment for businesses, with some 50 per cent of businesses experiencing a cyber security breach or attack during 2023. Here, in this review, we highlight factors that the literature suggests are related to cyber security breach and attack in firms. In addition, we examine what the literature suggests about the cyber security challenges faced by firms, particularly smaller firms.

Background

Digitalisation across business, the economy and society, i.e., the application of digital technologies and infrastructures (Autio 2017), is well underway. Industry 4.0 has seen the application of new technologies rapidly change the way firms design and curate experiences, manufacture, distribute and service products (Deloitte 2018). In recent years, the digital sector has experienced strong growth, which, since 2015, has been almost three times stronger than that of the total UK economy in real terms. In 2022, the digital sector contributed £158.3 billion to the UK economy and accounted for 1.9 million filled jobs, further illustrating the sector's significance (DCMS 2024; DSIT/DCMS 2024).

Building on the UK Innovation Strategy (BEIS 2022a), the UK Digital Strategy (DCMS 2022) focuses on the role that digital plays in supporting innovation. In 2020, around one fifth of UK business research and development (R&D) was digital R&D (e.g., computer programming and information services, telecommunications, software development) (DCMS 2022). Moreover, evidence suggests that there are performance benefits to be gained for businesses that adopt digital technologies (Awano 2018; ERC 2018). Small and medium-sized enterprises (SMEs)[1] that use two or more business management technologies, for example, have been found to exhibit productivity gains of up to 25 per cent (Awano 2018), and the adoption of digital technologies in micro enterprises has been found to be strongly linked to sales per employee, one measure of productivity (ERC 2018). Industrial digital technology (IDT) (e.g., artificial intelligence (AI), Digital Twins,

[1] i.e., firms with fewer than 250 employees.

Industrial Internet of Things (IIoT)) has the potential to increase manufacturing productivity, add some £455 billion gross value added (GVA), reduce CO_2 emissions by 4.5 per cent and create 175,000 new jobs over a decade (Maier 2017). Furthermore, greater use of digital innovation across the economy provides the UK's digital businesses with larger markets, continued growth and success (Awano 2018). The UK's economic future, jobs, wage levels, prosperity, national security, cost of living, productivity, and ability to compete globally are all reliant on continued and growing success in digital technology (DCMS 2022).

With digitalisation comes an increased reliance on cyberspace, i.e., the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices (Cabinet Office 2022). Cyberspace is open space – open to innovation and the free flow of ideas, information and expression, 'feeding the flow of innovation and productivity'.[2] However, as well as bringing about new opportunities for firms, cyberspace has brought about new digital threats and risks. Key data and systems on which firms rely can become compromised or damaged in ways that are hard to detect or defend against. As a result, services may be disrupted, files or network access might be lost, and software may be corrupted, hindering firm performance and impacting businesses both socially and economically (Kaplan, Sharma and Weinberg 2011). Moreover, cyberspace has transformed the crime environment for businesses. Despite fraud being the most common crime in the UK, costing almost £7 billion a year, incidents of small business cybercrime have more than tripled in recent years (FSB 2023). From January 2021 to January 2023, 37 per cent of small businesses experienced fraud, whereas 72 per cent of small businesses experienced cybercrime.

Cybercrime is crime committed through the use of information and communication technology (ICT) devices, where the devices are both the tool for committing the crime and the target of the crime (Cabinet Office 2022). This includes complicated technical attacks on computers, networks and mobile devices, or using computers and the internet to commit traditional crimes like harassment, bullying and fraud (Love Business Hate Fraud 2022). In 2024, The Cyber Security Breaches Survey (DSIT 2024) found that 50 per cent of businesses experienced a cyber security breach or attack during the previous twelve months. Furthermore, some two-fifths (44 per cent) of these businesses were victims of cybercrime,[3] i.e., 22 per cent of all businesses. In addition, the survey identified that 3 per cent of businesses were victims of fraud as a result of this cybercrime. Across all organisations, medium and large businesses were significantly more likely to experience a cybercrime than smaller firms. However, this may indicate underreporting in smaller organisations as they may have less sophisticated cyber security monitoring in place (DSIT 2024).

As digital threats and risks are an unavoidable by-product of digitalisation and the advancement of new technology, cyber security breaches and attacks and their effect on firms have become important in the strategic management field of study. Here, in this review, we examine what the evidence suggests about firms' vulnerabilities to cyber security breach and attack, and the cyber security challenges faced by smaller firms.

[2] Cabinet Office (2011). The UK Cyber Security Strategy, p.7.

[3] Not all cyber security breaches and attacks constitute a crime under the Computer Misuse Act 1990 and the Home Office Counting Rules. For example, some attempted attacks will not have penetrated an organisation's cyber defences and some, such as online impersonation, would be beyond the scope of the Computer Misuse Act. (CSBS 2024).

Overview of evidence

Much of the previous cyber security literature is quantitative in nature, utilising firm-level survey data. Some research focuses on factors that the literature has identified as being related to cyber security breach and attack in firms, i.e., vulnerability factors, while other studies examine firms' cyber security challenges, particularly in relation to smaller firms. A summary of this research is shown in the Appendix.

Vulnerability factors

- **Business strategy**

Evidence suggests that a firm's business strategy is a determinant of cyber security breach likelihood. Based on organisational theory, Li and Walton (2023) compare an innovation strategy with an efficiency strategy, and find that those firms that focus on innovation are more likely to have weaker, decentralised control systems, multiple technologies, and greater risk than firms with an efficiency-focused strategy. Following Miles et al. (1978), an innovation-focused firm is likened to a 'prospector' firm, seeking to identify and exploit new products and market opportunities, whereas an efficiency-focused firm is likened to a 'defender' firm. Li and Walton (2023) suggest that a prospector firm's focus on technological flexibility makes it more likely to invest in cyber security than other firms, reducing breach risk. A defender, however, could be a more attractive target for attackers than other firms due to organisational stability and profitability, increasing breach risk. Conversely, a prospector firm's lack of lengthy technological commitments and decentralised control systems can promote organisational instability (Miles et al. 1978), potentially increasing breach risk. Similarly, defender firms could have greater capabilities of defending against breach attempts, reducing the likelihood of a successful breach. Quantitative analysis undertaken by Li and Walton (2023) suggests that, overall, prospector strategy firms face a greater breach likelihood than other firms.

- **Employee characteristics**

The literature suggests that employee traits – both cognitive and personality – play a part in shaping firms' cyber security breach risk. An employee's risk-taking propensity, cognitive (inhibitory) control, and social cognition contributes towards a firm's cyber security breach susceptibility. Moreover, personality traits such as extroversion and agreeableness can affect employees' motivation to participate in security awareness training. These traits interact in complex ways to determine employee vulnerability (Boritz et al. 2022). Aspects of passive engagement, misdirected attention and engaging in risky cyber security behaviours all have the potential to increase organisational susceptibility to security flaws. Individuals who are quick to react or fail to think carefully about their decisions, for example, are less engaged in good cyber security behaviours (Hadlington 2018). Furthermore, research suggests that impulsive individuals are attracted to entrepreneurship, and are more likely to act despite uncertainty (Wiklund and Patzelt 2018). Therefore, entrepreneurial start-ups – typically micro or small firms – may be inherently more vulnerable to cyber security breach or attack. In terms of employee attitudes towards cyber security, Hadlington (2018) suggests that in larger firms, there can be a sense of devolved responsibility in terms of employees' cyber security responsibilities within an organisation, aligning with the viewpoint that individuals who believe they are protected by technical interventions provided by their host organisation engage in more risky cyber security behaviours. However, individuals employed by smaller organisations may not be made aware of the risks of engaging in dubious cyber security practices, which may be the result of differences in budget and organisational polices across firms of

different sizes. Moreover, Hadlington (2018) finds that as the age of an employee increases, attitudes towards cyber security improve. The personality trait of conscientiousness is suggested as a reason for this as it tends to increase with a person's age, and is associated with the propensity to follow rules and norms set by society, delayed gratification, and the ability to control impulses.

- **Firm characteristics**

Previous research identifies several firm characteristics that determine cyber security breach vulnerability. First, firm size is identified as being important. Smaller firms are susceptible to the same threats as larger organisations; however, larger firms have a larger attack surface with more susceptible employees and attackable devices, increasing firm vulnerabilities. There is a significant degree of heterogeneity in the level of digitalisation across firms. This spectrum ranges from firms at the forefront of digital technology integration, incorporating advanced elements like robotics, cloud computing, and smart devices, to firms in the early stages of adopting Industry 4.0 technologies. Research suggests that the extent of digitalisation is related to the information technology (IT) security issues experienced, i.e., there is an intricate interplay between cyber security concerns and the level of digital maturity achieved by firms (Arroyabe et al. 2024). Given the positive correlation between the number of integrated online services within an organisation and firm size (de Arroyabe and de Arroyabe 2023), it is unsurprising that the evidence suggests larger businesses experience more cyber attacks and breaches than smaller companies (Wanamaker 2019; Hawdon et al. 2023), with victimisation rates increasing with the number of employees (Woods and Walter 2022). In particular, small businesses report significantly less incidents of illegal access and cyber extortion (i.e., ransomware) than large businesses. In the case of cyber extortion, medium size businesses also report significantly less incidents than large businesses (Paoli et al. 2018).

Second, firms' vulnerability to cyber breach or attack varies across industrial sectors. Firms in sectors that operate more in the virtual world of cyberspace (e.g., defence, transportation, IT, finance and communications) are most vulnerable to a cyber breach or attack (Hawdon et al. 2023). Related to this is firms' vulnerabilities due to intellectual property (IP) holdings, which are themselves often determined by firms' industrial sectors. Evidence suggests that the importance of trade secrets to the firm has a highly significant, positive effect on the cyber threats encountered (Härting et al. 2023), with criminals targeting a firm's intellectual assets. The cost of trade secret theft is not insignificant. Theft of trade secrets is now estimated to cost businesses between 1-3 per cent of national GDP in developed economies. £280 billion of secret information is reported as being stolen by cyber criminals each year (The Law Society 2024).

Third, a lack of knowledge and understanding about information technology (IT) and cyber security at the firm level can leave organisations open to cyber security breach or attack. Research by Hadlington (2018) suggests that firms, particularly smaller firms, often lack the skills and knowledge needed to implement effective cyber security and deal with any cyber security incidents that arise. In addition, vulnerabilities resulting from firm-level knowledge and understanding constraints can interact with those arising from business strategies, influencing the connection between business strategy and breach likelihood (Li and Walton 2023).

Fourth, a firm manager's perception of the business's vulnerability to and preparedness for cyber breaches play a part in determining cyber security breach likelihood. A study by Hawdon et al. (2023) suggests that firm managers underestimate their businesses' vulnerabilities whilst they overestimate their preparedness, despite some 95 per cent of firms being surveyed having some form

of online presence. Most firms assess the risk for their company of being hit by a targeted attack as being relatively low (Huaman et al. 2021). Experience in and awareness of cyber security breaches increases the level of perceived cyber threats and lowers that of perceived preparedness. In reality, it seems that many firms most likely adopt security measures after suffering a cyber incident and/or being attractive targets for attackers (Gandal et al. 2023). Seemingly, cyber security breach experience and awareness leads to an underestimation of perceived preparedness compared to perceived threat, and therefore, experience in and awareness of cyber security breach raises perceptions of underperformance.

Small firm challenges

Various studies examine the challenges firms face in relation to cyber security, with several focusing on smaller firms. Small firms are being increasingly targeted by online threats because they are perceived as being inherently more vulnerable. Attackers believe that small firms require a low effort in order to acquire information due to their financial constraints, low levels of attack prevention and inadequate knowledge (Härting et al. 2023). The lack of resources, experience and awareness in small firms, compared to larger firms, means that they regularly have difficulties in complying with new regulations and deploying security measures in their systems and hardware (Bada and Nurse 2019). In a review article, Chidukwani et al. (2022) highlight the key cyber security challenges small firms face, these include technical, human, organisational, financial and legal challenges. SMEs lack in-house expertise, have tight IT budget constraints, and lack an understanding of how to protect against cyber attacks.

Typically, small business owners and managers have a weak understanding of information systems and security technologies. Moreover, they lack knowledge and expertise in information control measures, risk assessments and the development of security policies (Bada and Nurse 2019). They have limited knowhow on how to secure their organisational information and data from cyber attacks. To maintain an acceptable level of cyber security requires a dedicated budget and a specialist, often a technical person, with knowledge of cyber operations. However, Kappe et al. (2023) find that more than 40 per cent of SMEs do not assign cyber security to anyone in the firm, 58 per cent do not employ anyone to take care of IT, and 35 per cent said they had neither an internal nor external cyber security consultant. The lack of adequately skilled IT experts in the market, nonetheless, may prevent smaller firms from hiring proficient IT security personnel (Hoppe et al. 2021).

In most cases, larger firms have the human and financial resources to put in place cyber security controls. They are likely to have dedicated cyber security employees, with the knowledge and skills required to work with a firm's cyber security strategy. However, IT companies are the main source of information for micro and small businesses. As the IT market is unregulated, this can be problematic for smaller firms. Smaller firms are in danger of receiving incorrect information or adopting inappropriate behaviours, including complacency about cyber threats (Cartwright et al. 2023). Furthermore, IT companies themselves are typically micro or small firms, facing the same risks as micro and small firms more generally. The literature suggests that firms are more likely to access information on cyber security as their number of employees increases. In terms of information access, the least used source of information for smaller firms is the public sector, including government campaigns such as Cyber Essentials (Cartwright et al. 2023). There is evidence to suggest, however, that access to information is beneficial. In

their study on Saudi Arabian SMEs, Alharbi et al. (2021) find that having contact with cyber security authorities statistically reduces the restoration time following a cyber attack, and having an in-house cyber security inspection team and a recovery plan reduces the financial damage of a cyber attack.

An additional challenge for small firms is the motive that lies behind the cyber attack. Small firms are often targeted as a weak link in supply chains in order to attack bigger links of the chain (Härting et al. 2023). Empirical evidence shows that smaller firms are both targeted in their own right and for being part of a supply chain that includes larger companies (Arroyabe et al. 2024).

Cyber security incident reporting is also challenging for some firms. Larger firms, especially those with tech departments and in-house cyber security, tend to report incidents to public authorities, whereas outsourced cyber security management is not associated with public authority reporting (Huaman et al. 2021; Kemp et al. 2023). In addition, some firms are reluctant to report incidents because of the perceived time and financial costs associated with reporting. Others fear fines from regulatory agencies as well as the reputational damage that comes with disclosure. Wanamaker (2019) suggests businesses refrain from reporting incidents to the police because the majority of incidents are resolved internally or through IT consultants, the incident is thought to be too minor to report, or businesses do not think to contact the police. Moreover, the study finds that risk management and formal training are positively related to the reporting of incidents to police (Wanamaker 2019). Kemp et al. (2023) find that firms are more likely to report a cyber security incident if they suffer a negative impact or outcome, or when cyber security is a high priority. They are less likely to report an incident to public authorities, however, if employees use personal devices for work purposes.

Summary and evidence gaps

As well as bringing about new opportunities for firms, the increased reliance on cyberspace that comes with digitalisation has brought about new digital threats and risks. This review highlights factors that the literature identifies as being related to cyber security breach and attack in firms. The factors include: business strategy; employee characteristics; and firm characteristics. In addition to this, the literature uncovers some of the cyber security challenges faced by firms, particularly those faced by smaller firms. These challenges include: lack of financial resources; weak IT infrastructure; lack of cyber security knowledge; and lack of cyber security technical and human experience.

In the UK, there are an estimated 5.5 million micro and small businesses – more than 99 per cent of the total business population (BEIS 2022b). Smaller firms find it more difficult than larger firms to optimally invest in cyber security due to the challenges that they face. Cyber attacks are moving beyond data breaches and privacy concerns to more sophisticated schemes. They are proving to be extremely costly, disrupting entire businesses, industries, supply chains and even nations (Chidukwani et al. 2022). Indeed, experts predict that cybercrime will cost the world $10.5 trillion annually by 2025 (Morgan 2020). There is a pressing policy challenge, therefore, to improve cyber security behaviour in micro and small businesses, with firms more likely to succeed with technology adoption if their leadership and employees are appropriately skilled and supported (DCMS 2022). A cyber security plan, put in place by a firm, may reduce the risk of the firm falling victim to a cyber breach or attack. By ensuring staff, contractors, suppliers and other stakeholders are aware of potential threats to the business and of their own responsibility for improving cyber security, firms can help prevent a cyber attack.

Despite an increase in cyber security-related literature during recent years, an evidence gap exists in relation to the understanding of firms' approaches to cyber security risk management. Further research in this area would provide a deeper insight into firms' cyber attack preparedness as well as firms' activities for preparedness. In addition, it would reveal firm managers' perceptions of cyber attack risk, and firm managers' approaches to help improve their cyber security positions. A second evidence gap exists in relation to firms' recovery following a cyber breach or attack. The expensive remediation costs associated with cyber incidents can make it difficult for firms, especially smaller firms, to recover. Cyber insurance is a possible approach here, however, it is not well understood amongst smaller firms.

Sources

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F. and Al-Otaibi, K. (2021). The impact of cyber security practices on cyber-attack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), p.6901.

Arroyabe, M.F., Arranz, C.F., de Arroyabe, I.F. and de Arroyabe, J.C.F. (2024). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. Technological Forecasting and Social Change, 199, p.123051.

Autio, E. (2017). Digitalisation, ecosystems, entrepreneurship and policy. Perspectives into topical issues is society and ways to support political decision making. Government's Analysis, Research and Assessment Activities, Policy Brief, 20, p.2017.

Awano, G. (2018). Information and communication technology intensity and productivity. ONS. https://backup.ons.gov.uk/wp-content/uploads/sites/3/2018/10/Information-and-communication-technology-intensity-and-productivity.pdf

Bada, M. and Nurse, J.R., 2019. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), pp.393-410.

BEIS (2022a). UK innovation survey 2021. Department for Business, Energy & Industrial Strategy. https://www.gov.uk/government/statistics/uk-innovation-survey-2021-report

BEIS (2022b). Business population estimates for the UK and regions 2022: Statistical release. https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html

Boritz, J.E., Ge, C. and Patterson, K. (2022). Factors Affecting Employees' Susceptibility to Cyber-attacks. Journal of Information Systems, 36(3), pp.27-60.

Cabinet Office (2011). The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

Cabinet Office (2022). National Cyber Strategy. Pioneering a cyber future with the whole of the UK. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Cartwright, A., Cartwright, E. and Edun, E.S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131, p.103288.

Chidukwani, A., Zander, S. and Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, pp.85701-85719.

DCMS (2022). UK Digital Strategy. Department for Digital, Culture, Media & Sport https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy

DCMS (2024). Digital Sector Economic Estimates Gross Value Added 2022 (provisional). https://www.gov.uk/government/statistics/dcms-and-digital-sector-gva-2022-provisional/digital-sector-economic-estimates-gross-value-added-2022-provisional#:~:text=the%20digital%20sector-,We%20use%20current%20prices%20to%20report%20current%20sector%20estimates%20and,(measured%20in%20current%20prices).

de Arroyabe, I.F. and de Arroyabe, J.C.F. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterprise Information Systems, 17(3), p.1942997.

Deloitte (2018). Managing Risk in Digital Transformation. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf

DSIT (2024). Cyber Security Breaches Survey 2024. Department for Science, Innovation and Technology. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

DSIT/DCMS (2024). Economic Estimates: Earnings 2023 and Employment October 2022 to September 2023 for the DCMS Sectors and Digital Sector. https://www.gov.uk/government/statistics/economic-estimates-earnings-2023-and-employment-october-2022-to-september-2023-for-the-dcms-sectors-and-digital-sector#:~:text=and%20data%20limitations.-,Headline%20findings%3A,previous%20equivalent%2012%2Dmonth%20period.

ERC (2018). State of Small Business Britain Report 2018. https://www.enterpriseresearch.ac.uk/publications/state-small-business-britain-report-2018/

FSB (2023). Cracking the Case: Uncovering the cost of small business crime. https://www.fsb.org.uk/resource-report/cracking-the-case-uncovering-the-cost-of-small-business-crime.html

Gandal, N., Moore, T., Riordan, M. and Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. Computers & Security, 133, p.103380.

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology, 12(1), pp.269-281.

Härting, R.C., Schulz, G.N., Deffner, D. and Karg, C. (2023). Digital Transformation and Cyber Threats for Small and Medium Sized Enterprises. In KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications pp. 161-170.

Hawdon, J., Parti, K., Dearden, T., Vandecar-Burdin, T., Albanese, J. and Gainey, R. (2023). Cybercrime victimization among Virginia businesses: frequency, vulnerabilities, and consequences of cybervictimization. Criminal Justice Studies, 36(3), pp.269-291.

Hoppe, F., Gatzert, N. and Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. The Journal of Risk Finance, 22(3/4), pp.240-260.

Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A. and Fahl, S. (2021). A {Large-Scale} interview study on information security in and attacks against small and medium-sized enterprises. In 30th USENIX Security Symposium pp. 1235-1252.

Kaplan, J., Sharma, S., and Weinberg, A. (2011). Meeting the Cyber security Challenge. Digit. McKinsey. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Meeting%20the%20cyber security%20challenge/Meeting%20the%20cyber security%20challenge.pdf

Kappe, M., Härting, R.C., Karg, C. and Deffner, D. (2023). Cyber security in SMEs–Drivers of Cybercrime, Insufficient Equipment and Prevention. Procedia Computer Science, 225, pp.3631-3640.

Kemp, S., Buil-Gil, D., Miró-Llinares, F. and Lord, N. (2023). When do businesses report cybercrime? Findings from a UK study. Criminology & Criminal Justice, 23(3), pp.468-489.

Li, T. and Walton, S. (2023). Business Strategy and Cyber security Breaches. Journal of Information Systems, 37(2), pp.51-76.

Love Business Hate Fraud (2022). Preventing cybercrime. How to keep fraud and cybercrime out of your business. https://lovebusiness-hatefraud.org.uk/wp-content/uploads/2022/12/Preventing-Cybercrime-Full-Guide-Dec22.pdf

Maier, J. (2017). Made Smarter Review. UK Industrial Digitalisation Review. https://www.gov.uk/government/publications/made-smarter-review

Miles, R.E., Snow, C.C., Meyer, A.D. and Coleman Jr, H.J., 1978. Organizational strategy, structure, and process. Academy of management review, 3(3), pp.546-562.

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cyber security. Technology in society, 58, p.101122.

Paoli, L., Visschers, J. and Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 70, pp.397-420.

The Law Society (2024). Keeping trade secrets: the big questions. https://www.lawsociety.org.uk/topics/in-house/keeping-trade-secrets-the-big-questions#:~:text=As%20business%20information%20is%20more,national%20GDP%20in%20developed%20economies.

Wanamaker, K.A. (2019). Profile of Canadian businesses who report cybercrime to police. The 2017 Canadian Survey of Cyber Security and Cybercrime. Research Report. Public Safety Canada.

Wiklund, J., Yu, W. and Patzelt, H. (2018). Impulsivity and entrepreneurial action. Academy of Management Perspectives, 32(3), pp.379-403.

Woods, D.W. and Walter, L. (2022). Reviewing estimates of cybercrime victimisation and cyber risk likelihood. In 2022 IEEE European Symposium on Security and Privacy Workshops. pp. 150-162.

About the author

Joanne Turner is a Research Fellow at Enterprise Research Centre. Her research examines the productivity and growth returns to R&D, the links between intellectual property protection and innovation, and the role of local, regional and broader eco-system factors in supporting innovation and growth. She can be contacted at Joanne.E.Turner@wbs.ac.uk

Appendix: Literature surrounding firms' cyber security vulnerability factors and challenges

Study	Aims	Data and methods	Key findings
Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F. and Al-Otaibi, K. (2021). The impact of cyber security practices on cyber-attack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), p.6901.	The study measures the impact of cyber security practices in SMEs following a cyber security attack, as well as the relationship between cyber security practices and the level of harm that results from cyber security attacks.	Quantitative study using data for 282 Saudi Arabian SMEs during December 2020 to March 2021. Multiple regression is used to examine the effectiveness of twelve cyber security practices, in terms of financial damage, loss of sensitive data, and restoration time.	The results indicate that an in-firm inspection team, a recovery plan, and firm contact with cyber security authorities lower a firm's restoration time following a cyber security breach or attack. SMEs that have an inspection team and a recovery plan will likely suffer less financial damage. There is a negative relationship between cyber security awareness in the firm and the loss of sensitive data. Professionals' salaries have a negative effect on the loss of data in firms (a positive relationship between economic incentives and improved levels of cyber security).
Arroyabe, M.F., Arranz, C.F., de Arroyabe, I.F. and de Arroyabe, J.C.F. (2024). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. Technological Forecasting and Social Change, 199, p.123051.	The study examines how IT security issues affect the digital transformation of manufacturing SMEs. In addition, the study asks how IT security challenges influence the level of digitalisation in manufacturing SMEs.	Quantitative study using data for 3184 manufacturing SMEs from the Flash Eurobarometer No. 486 database from Eurostat (European Union).	There is a significant degree of heterogeneity in the level of digitalisation across firms. This spectrum ranges from firms at the forefront of digital technology integration, incorporating advanced elements like robotics, cloud computing, and smart devices, to firms in the early stages of adopting Industry 4.0 technologies. The extent of digitalisation is related to the IT security issues in manufacturing SMEs, i.e., there is an intricate interplay between cyber security concerns and the level of digital maturity achieved by firms.
Boritz, J.E., Ge, C. and Patterson, K. (2022). Factors Affecting Employees' Susceptibility to Cyber-attacks. Journal of Information Systems, 36(3), pp.27-60.	The study examines employee behaviour in a cyber security context. It examines factors associated with employees' susceptibility to phishing attacks in a professional services firm and a financial services firm.	Quantitative study (probit regression analysis) using data obtained from a Qualtrics personality test, administered to employees who have been successfully phished and employees who have not been successfully phished in exercises administered by their employers (208 responses from a Canadian professional services firm and 186 responses from a Canadian bank). Trust, suspicion, and professional scepticism as well as risk-taking propensity, cognitive (inhibitory) control, and social cognition are measured as well as several demographic and work-context variables.	Employees' susceptibility to phishing attacks is influenced by a combination of scepticism, trust, risk-taking behaviour, cognitive control, and social cognition, with these traits interacting in complex ways to determine vulnerability. Bank employees are more susceptible to being phished than professional services firm employees, but bank employees with professional certificates are less susceptible to phishing attacks than other bank employees. Individuals with self-reported responsibility for cyber security demonstrate lower susceptibility to phishing attacks, highlighting the importance of promoting a culture of accountability within organisations to enhance cyber security measures.
Cartwright, A., Cartwright, E. and Edun, E.S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies.	The study examines the potential role IT companies play in passing on information to firms regarding cyber security best practice.	Quantitative study using the UK Cyber Security Breaches Survey, 2018-2021. Businesses are asked where, if anywhere, in the last twelve months, they have sought information, advice or guidance on the cyber	IT companies are the main source of information for micro and small businesses, across all sectors, although some sectors are more likely to access information than others. Micro and small firms require advice and guidance on how to identify 'good' IT companies. Support is also required for IT companies, who themselves are typically micro

Computers & Security, 131, p.103288.		security threats faced by their organisation. In addition, focus groups and interviews are carried out with thirteen experts on cyber security for micro and small businesses in the UK to explore the role IT companies play in the UK market, and how their role could be supported.	and small businesses, that lack expertise on cyber security. The IT market is unregulated, and there is a danger that IT companies could spread the wrong information or promote the adoption of inappropriate behaviours, including complacency about cyber threats. The least used source of information is the public sector, including government campaigns such as Cyber Essentials. As the number of employees increases, firms are more likely to access information on cyber security, and more likely to access information from an IT/cyber company.
Chidukwani, A., Zander, S. and Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, pp.85701-85719.	The study identifies the key challenges SMEs face in implementing cyber security.	Literature review of recent research on cyber security in SMEs.	SMEs fail to implement adequate cyber security strategies, and as a result can be easy targets for cyber attackers. Reasons include: SMEs face technical, human, organisational, financial and legal challenges. They lack in-house expertise, have tight IT budget constraints, and lack an understanding of how to protect against cyber attacks. Older SME owners and those with negative attitudes towards technology are less likely to implement adequate cyber security strategies. SMEs underestimate risk, lack skills and knowledge, lack resources, lack perseverance, and are unable to keep up with technology advancement.
de Arroyabe, I.F. and de Arroyabe, J.C.F. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterprise Information Systems, 17(3), p.1942997.	This study examines how different types of cyber breach affect SMEs (in terms of severity, e.g., disruption time, cost etc.).	Quantitative study using the UK Cyber Security Breaches Survey, 2016-2017. Survey includes different types of breach, the frequency of these breaches, the severity of the breaches (most disruptive breach, time until breach was identified, cost of cyber security breaches), and the impact of the breaches (in financial, management and economic terms, also considering the responsibility that the firm has to its environment). Statistical analysis to estimate a causal analysis model of the effect of breaches in SMEs.	Results show a positive correlation between the number of integrated online services within an organisation and firm size. Breaches have an effect on SMEs in economic, financial and management terms. Attacks that attempt to take down a firm's website or online services yield the largest disruption cost. Unauthorised use of computers, networks or servers by staff, even if accidental, yield the greatest disruption time. As dependence on online services increases, SME managers increase their interest in and concern about cyber security. The most common impact of an incident on SMEs is the implementation of new measures to prevent further attacks, i.e., attempts by management to protect themselves against future attacks.
Gandal, N., Moore, T., Riordan, M. and Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. Computers & Security, 133, p.103380.	The study examines whether cyber security precautions taken by firms affect the likelihood that a cyber incident will occur.	Quantitative study using firm-level data from an ICT and cyber security survey undertaken in 2020–2021 by the Israeli National Cyber Directorate (INCD) and Central Bureau of Statistics (CBS). The survey includes private sector businesses with more than 10 employees, detailed questions about the types of security controls adopted by firms, and whether the firm	Without instrumenting for precautions: The coefficient on the security precautions is positive and statistically significant. Many firms most likely adopted the security measures after suffering a cyber incident and/or were attractive targets for attackers. Instrumenting for precautions: The coefficient on security precautions is negative and statistically significant. Employing more security precautions reduces the probability of suffering a cyber incident.

		has experienced a cyber security attack, as well as questions about Internet use, e-commerce, and other firm characteristics. Regression analysis using the occurrence of a cyber incident as the dependent variable and the number of security precautions, firm and industry characteristics as independent variables.	Using six easy to implement (basic) cyber security precautions as the security variable leaves the results qualitatively unchanged. For large firms with significant revenues, using e-commerce and cloud services (the riskiest firms), adopting all six basic security precautions reduces the probability of experiencing a cyber incident from 80 per cent to 42 per cent. This shows that the six basic security measures make a difference. Moreover, adopting even more controls also has a positive impact.
Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology, 12(1), pp.269-281.	The study explores if the frequency of employee engagement in risky cyber security behaviour is linked to organisational factors (e.g., firm age), the employee's attitudes towards cyber security and cybercrime, and the employee's age.	2016 online questionnaire through Qualtrics Online Sampling. Dataset includes 515 UK participants. Quantitative analysis using ANOVA tests.	The study finds a significant negative correlation between attitudes towards cyber security and engaging in risky cyber security behaviours, indicating that individuals with more negative attitudes are more likely to exhibit risky behaviours. Individuals in the higher age bracket demonstrate a more positive attitude towards cyber security. Significant differences are observed for both risky cyber security behaviours and attitudes towards cyber security in relation to firm size.
Härting, R.C., Schulz, G.N., Deffner, D. and Karg, C. (2023). Digital Transformation and Cyber Threats for Small and Medium Sized Enterprises. In KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications (pp. 161-170.	The study identifies the determinants of cyber threats in SMEs.	Quantitative study based on a systematic literature review and a questionnaire. Hypotheses are developed from the literature review, and in relation to these hypotheses, a questionnaire is used to collect data for 104 SMEs in Germany between May 2021 and March 2022 (importance of trade secrets to the firm, firm security risks, security prevention in the firm, and the motive for crime). Structural equation modelling is undertaken using a multivariate analysis.	The importance of trade secrets to the firm has a highly significant, positive effect on the cyber threats to SMEs. Security risks have an insignificant, but positive effect on the cyber threats to SMEs. Motives for crime has an insignificant, negative effect on the cyber threats to SMEs. Prevention (training and education etc.) has a highly significant effect on the cyber threats to SMEs.
Hawdon, J., Parti, K., Dearden, T., Vandecar-Burdin, T., Albanese, J. and Gainey, R. (2023). Cybercrime victimization among Virginia businesses: frequency, vulnerabilities, and consequences of cybervictimization. Criminal Justice Studies, 36(3), pp.269-291.	The study examines the extent to which firms perceive their vulnerabilities, the extent to which firms engage in behaviours that can potentially make them vulnerable, the policies and practices firms have in place to reduce vulnerability, and their experiences with victimisation.	Quantitative study using data from 428 US (Virginia) firms. Firms of all sizes and sectors are included. The survey used follows the format of the UK Cyber Security Breaches Survey (2020). The survey asked about business demographics, vulnerabilities, actual preparedness or controls in place, cybercrime attacks and breaches, harms and costs, actual preparedness, perceived preparedness to cyber attacks.	16 per cent of businesses thought that US businesses (in general) were very prepared for an attack in contrast to 30 per cent saying that their own business was very prepared. 87 per cent said that cyber security is a high or very high priority for their business. Cyber security importance varies by sector. Over 90 per cent of the firms in defence, transportation, IT, finance, communications, and real estate said cyber security is a high or very high priority for their company. Conversely, 80 per cent of the firms in consumer discretionary, 63.6 per cent of the firms in materials, and 79.1 per cent of those in 'other' sectors reported that cyber security is of high importance. 78.9 per cent said employees in their firm use personally owned devices to carry out regular work activities, and another 3.1 per cent did not know if this was the case (providing possible avenues for cybercriminals). Only 58.8 per cent of the surveyed businesses provide regular cyber security training to their employees, and approximately 20 per cent of

			firms update their senior management about cyber security only once a year or less. Fewer than expected firms follow recommended safety measures. Less than two-thirds of firms took basic cyber security precautions, but even fewer took additional steps to avoid attacks. Of the 386 firms that were victimised, 19.7 per cent did not report the crime to anyone. 62.9 per cent said the breach had a 'moderate' or 'major' effect.
Hoppe, F., Gatzert, N. and Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. The Journal of Risk Finance, 22(3/4), pp.240-260.	The study examines the current state of SMEs' cyber risk management practices, identifying any major challenges.	Market insights (based on the various steps of the risk management process) are collated from 37 recent industry surveys.	Two major challenges, common across countries, are identified. First, deficiencies in risk culture (e.g., knowledge gaps, a lack of risk awareness, and overconfidence) that prevents SMEs from establishing a sound context for risk management and that causes deficiencies along all cyber risk management process steps. Second, a severe lack of adequately skilled IT experts in the market, preventing firms from hiring IT security personnel (scarce resources in the IT labour market leading to a lack of skilled personnel).
Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A. and Fahl, S. (2021). A {Large-Scale} interview study on information security in and attacks against small and medium-sized enterprises. In 30th USENIX Security Symposium pp. 1235-1252.	This study identifies how employees perceive cyber attack risk, what security measures SMEs use, to what extent they are used, what cyber attacks have been detected in the last twelve months and their frequency, how firm characteristics and the security measures used by firms are related to reported incidents, and what the victimisation factors are.	Quantitative study incorporating computer assisted telephone interviews (CATI) with 5000 German SME representatives (August 2018 to January 2019), followed by logistic/linear regression analysis.	Most firms assess the risk for their company of being hit by a targeted attack as relatively low, compared to the risk of being hit by a mass attack. In general, smaller firms reported a lower perceived risk of being attacked than larger firms. Basic technical security measures are widely used. However, industry sector, number of employees, company age and the use of external information security expertise are correlated with the number of security measures used – firm size correlating with all types of security measure. Firms in the finance and energy sector are most likely to employ organisational security measures. Firm characteristics map to the reporting of security incidents more than reported technical security measures map to reporting. Larger firms, especially those with tech departments reported more incidents. Findings suggest that the industry sector correlates with the reporting of security incidents. Findings suggest SMEs are security aware, but awareness has not yet spread to all staff, leaving SMEs open to phishing, insider attacks and advanced persistent threats.
Kappe, M., Härting, R.C., Karg, C. and Deffner, D. (2023). Cyber security in SMEs–Drivers of Cybercrime, Insufficient Equipment and Prevention. Procedia Computer Science, 225, pp.3631-3640.	The study identifies factors linked with cyber threats in SMEs. In addition, the study identifies current equipment and know-how regarding cyber security in SMEs, and asks what assistance from third parties (external) do SMEs need in order to better protect themselves against cyber threats.	Qualitative and quantitative analysis of German (East Württemberg and Heilbronn-Franken) SMEs. Qualitative data collection – semi-structured interviews and content analysis conducted using grounded theory. Quantitative analysis using an online survey developed from the interviews. A structural equation model is evaluated.	The motives for crime and the lack of prevention have a significant positive effect on cybercrime as a threat for SMEs. Over 40 per cent of SMEs did not assign cyber security to anyone in the firm. 58 per cent of firms did not employ anyone to take care of IT. In addition, 35 per cent said they had neither an internal nor external cyber security consultant. Just under 20 per cent of firms said they had already been the victim of a cyber attack. 94 per cent of respondents said they have a firewall and are using up-to-date antivirus software. 32 per cent use 2-factor authentication. Only 30 per cent of SMEs reported having an emergency plan in place to respond to IT security incidents. 44 per cent

			have no emergency plan. The rest do not know or are in the process of creating one. 40 per cent of SMEs make employees aware of cyber security once a year, 37 per cent monthly and 7 per cent weekly. 17 per cent of SMEs said they do this on a one-time basis. 95 per cent regularly back up their data. 55 per cent of these use external data carriers for this purpose. 25 per cent use cloud services and 13 per cent use a mirrored server.
Kemp, S., Buil-Gil, D., Miró-Llinares, F. and Lord, N. (2023). When do businesses report cybercrime? Findings from a UK study. Criminology & Criminal Justice, 23(3), pp.468-489.	This study explores factors associated with firms' cybercrime reporting. The study asks if firm characteristics (e.g., size, sector, digital activity) are associated with cybercrime reporting, whether the attitudes of businesses towards cyber security and the cyber security practices instituted by businesses are associated with cybercrime reporting, and if the characteristics of the cybercrime event are associated with reporting.	Quantitative study using the UK Cyber Security Breaches Survey, 2018-2020. Study investigates the likelihood of reporting to anyone outside the organisation, and the likelihood of reporting to public authorities. Binary logistic regression models are used. In addition, the odds ratio of all independent variables is estimated, which is an indicator of the likelihood that the outcome under study (i.e., cybercrime reporting) occurs in one group (e.g., companies with cyber security insurance) relative to the odds of the reference group (e.g., no insurance).	Firm size and sector, in most cases, show no association with reporting cybercrime to someone outside the organisation. However, administrative and financial service companies may be less likely to report cybercrime victimisation to public authorities than other business sectors. Firms in which staff use personal devices for work are less likely to report cybercrime victimisation to public authorities, while this association is not significant in the models of reporting to anyone outside the organisation. There is a positive association between suffering a negative impact/outcome from victimisation and the likelihood of reporting. The type of cybercrime suffered is a strong predictor of the likelihood of reporting. The likelihood of reporting increases when cyber security incidents generate negative impacts and when the company places a high priority on cyber security. Having outsourced cyber security management is associated with reporting to anyone outside the organisation but not to public authorities, whereas in-house cyber security teams seem more inclined to report to public authorities.
Li, T. and Walton, S. (2023). Business Strategy and Cyber security Breaches. Journal of Information Systems, 37(2), pp.51-76.	The study examines the relationship between firms' business strategy and cyber security breach likelihood, providing insights into how strategic choices can impact cyber security outcomes.	Quantitative study estimating the probability of cyber security breach. Data includes 34,308 US firm-level observations (2005 to 2019) on reported breaches, taken from Privacy Rights Clearinghouse and Audit Analytics, and financial and auditing information, taken from Compustat, Audit Analytics and BoardEx.	Firms with an innovative (prospector) strategy may be more susceptible to cyber security breaches than firms with an efficiency-focused strategy due to weaker control systems, multiple technologies, and higher risk levels. IT understanding at the executive or firm level can influence the connection between business strategy and breach likelihood.
Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cyber security. Technology in society, 58, p.101122.	The study identifies factors that influence perceived threats to or perceived preparedness for cyber security, and, in addition, identifies factors that influence the gap between perceived threats to and perceived preparedness for cyber security.	Quantitative study using 2016 US cyber security survey data from the Pew Research Centre. First, ordered logistic regression analysis is used to investigate the significant determinants of perceived threat and preparedness. Second, multinomial logistic regression analysis is used to investigate determinants of the gap between perceived threat and preparedness.	Personal experience in and awareness of cyber security breaches increases the level of perceived cyber threats, but reduces that of perceived preparedness. Confidence in organisational cyber security capacity, social trust, and liberalism exhibits the opposite effect on these two outcomes. Cyber security breach experience and awareness leads to an underestimation of perceived preparedness compared to perceived threat. In other words, experience in and awareness of cyber security breach raises perceptions of underperformance. Results show that the effects of these determinants differ with the type of gap. The determinants of perceived overperformance (good preparedness relative to low threat) and perceived underperformance (poor preparedness relative to high threat) are

			significantly different from those for perceived fair performance (matching levels of threat and preparedness).
Paoli, L., Visschers, J. and Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 70, pp.397-420.	The study develops and tests a conceptual framework to define and operationalise cybercrime affecting businesses, and assesses its impact, harms and costs on businesses.	2016 Belgium web-based survey of high-level representatives of 310 businesses. Sectors include: technology, chemical and life sciences, and commerce and services. Firm sizes include: Small, medium, large. Descriptive analysis undertaken on all variables, and a MANOVA (i.e., multivariate analysis of variance) with the incidences of victimisation for each type of cybercrime.	The MANOVA analysis reveals significant differences across firm size in the incidences of illegal access and data/system interference. In particular, small businesses report significantly less incidents of illegal access and cyber extortion (i.e., ransomware) than large businesses. In the case of cyber extortion, medium size businesses also report significantly less incidents than large businesses.
Wanamaker, K.A. (2019). Profile of Canadian businesses who report cybercrime to police. The 2017 Canadian Survey of Cyber Security and Cybercrime.	The study identifies reasons why businesses do not report cyber-related crimes, factors that may increase the likelihood of reporting a cyber incident, and the profiles of businesses that report cyber incidents.	Quantitative study using 2017 Canadian Survey of Cyber Security and Cybercrime. The survey includes data for 10,794 Canadian businesses with 10 or more employees across all sectors (except government and public administration). The survey covers business characteristics, the cyber security measures in place, the risk management arrangements that are in place, business resilience (e.g., cyber security risks and/or threats that are considered most detrimental to a business), cost to prevent or detect cyber security incident(s), information about cyber security incident(s) (e.g., how businesses were impacted by cyber security incidents), the reporting of cyber security incident(s), and the cost of recovering from cyber security incident(s).	20 per cent of businesses experienced a cyber incident, with larger firms experiencing more cyber incidents than smaller firms; however, very few businesses report incident(s) to police. Risk management and formal training are positively related to the reporting of incidents to police. Results suggest a need to increase awareness of the frequency of cybercrime, as well as the availability of formal training options on cyber-related issues. They also underscore the importance of having enhanced cyber security protocols in place.
Woods, D.W. and Walter, L. (2022). Reviewing estimates of cybercrime victimisation and cyber risk likelihood. In 2022 IEEE European Symposium on Security and Privacy Workshops. pp. 150-162.	This study examines cybercrime victimisation and cyber risk likelihood, aiming to provide a bridge between the academic fields of criminology and cyber security.	Literature review of existing quantitative evidence.	Firms face greater victimisation rates than individuals, which increases with the number of employees. Global surveys reveal a consistent relative ranking of countries in ransomware victimisation. UK firms suffer comparatively lower likelihood of ransomware incident compared to Belgium, Germany and the US. Victimisation varies across different cybercrimes. Rates are much higher when unsuccessful attacks are also counted, such as when an entity receives a fraudulent email without responding, or when a malware infection is re-mediated without any loss.

Other SOTA Reviews are available on the ERC web site www.enterpriseresearch.ac.uk. The views expressed in this review represent those of the authors and are not necessarily those of the ERC or its funders.

Published by Enterprise Research Centre (ERC)