Small Bus Econ (2025) 64:1493–1514
https://doi.org/10.1007/s11187-024-00946-8

RESEARCH ARTICLE

Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya

Godsway Korku Tetteh · Chuks Otioma

Accepted: 13 June 2024 / Published online: 5 July 2024

Abstract Most scholarly work has focused on the positive effects of digitalisation in Sub-Saharan Africa without accounting for the associated risks and mitigation measures at the firm level. Using the 2016 Enterprise ICT Survey of Kenya which provides a rich source of information on the use of ICT among firms, we examine the effect of cybersecurity breach on labour productivity and show how this effect is moderated by cyber risk mitigation capabilities at the firm level. We find that cybersecurity breach reduces labour productivity at the firm level. We also find that upskilling mitigates the negative effect of cybersecurity breach on labour productivity especially for Small and Medium-sized Enterprises. The results further suggest that while Information Technology Policy and Information Technology Security capabilities can enable firms to improve labour productivity, these measures are not sufficient to offset the adverse effect of cybersecurity breach on labour productivity. Together the results imply that upskilling is an effective cyber risk mitigation measure against cybersecurity breaches at the firm level and therefore should be an integral part of the overarching IT governance strategy of firms.

Plain English Summary Cyberattack decreases labour productivity, but upskilling can mitigate this effect. Using the 2016 Enterprise ICT Survey of Kenya we find that cyberattack reduces labour productivity at the firm level. However, upskilling enables firms to mitigate the negative effect of cyberattack on labour productivity. We also find that Information Technology Policy and Information Technology Security improve labour productivity, but these measures are not sufficient to offset the negative effect of cyberattack. Overall, the evidence suggests that upskilling is an effective cyber risk mitigation measure against cyberattack especially among Small and Medium-sized Enterprises. Therefore, upskilling in the form of (re)training should be encouraged among firms to build the capacity of employees against cyberattack.

Keywords Cyberattack · Cybersecurity · Upskilling · Labour productivity

JEL Classification G33 · L25 · L26 · M15 · O32 · O33

G. Tetteh (✉)
University of Strathclyde, Glasgow, UK
e-mail: tetteh@merit.unu.edu; godsway.tetteh@strath.ac.uk

G. Tetteh · C. Otioma
UNU-MERIT, Maastricht University, Maastricht, The Netherlands
e-mail: otioma@merit.unu.edu; Chuks.Otioma@glasgow.ac.uk

C. Otioma
Adam Smith Business School, University of Glasgow, Glasgow, UK

1 Introduction

Advances in digital technologies afford firms unprecedented capabilities to manage data, coordinate supply chain activities and improve overall business functions. The increasing digital resources enable firms to develop innovative platform-based business models, products and markets (Acs et al., 2021; Bouwman et al., 2018; Nambisan et al., 2019), increase operational efficiency and improve performance (Bharadwaj, 2000; Brynjolfsson & Hitt, 2000; Cainelli et al., 2006; Castiglione & Infante, 2014; Vu et al., 2020).

However, the increasing volume of information and interconnectivity of business processes, activities, and actors come with the risks of cybersecurity breaches. A cybersecurity breach occurs when the confidentiality, availability and integrity of data and related infrastructure are compromised (Acquisti et al., 2006; Tchernykh et al., 2019). The richness of digital data, which in turn can provide access to critical and sensitive resources in firms, makes it attractive to cyber intruders and attackers. Unintentional mishandling of data and related IT resources by internal users such as staff members, or insider abuse, in connivance with external actors, can cause severe cybersecurity breaches (Alraja et al., 2023; Apolinário et al., 2023; D'Arcy et al., 2009; Vance et al., 2013; Warkentin & Willison, 2009). An attack on any vulnerable node in the IT system or digital platform can spread through the networks and cause infrastructure and operational disruptions (Kher et al., 2021; Moore, 2010).

The intensifying risks and effects mean that firms have had to invest in, develop and implement cybersecurity programmes, as part of their overarching IT governance strategy (Eloff & Solms, 2000; Gordon et al., 2015; Hasan et al., 2021; Phillips & Tanner, 2019). While technical defence and/or adaptation to cybersecurity threats, in the form of software solutions for detection, authentication, repair and recovery of compromised data and related resources, are critical to organisations, effective cybersecurity programmes require a broader IT policy framework, practices, leadership and coordination (Chang, 2013; Shaikh & Siponen, 2023; Velasco et al., 2018; Weill & Ross, 2004).

A growing body of literature attempts to unravel the effect of cybersecurity breaches on reputation damage, adverse stock market reaction and sales revenue (Arcuri et al., 2018; Campbell et al., 2003; Cavusoglu et al., 2004; Kamiya et al., 2021) with limited empirical evidence on the productivity effect of cybersecurity breaches (for example, Makridis & Dean, 2018; Sonnenreich et al., 2005). Makridis and Dean (2018), for example, investigate the productivity effect of cybersecurity breaches on publicly traded (large) firms. This study provides little or no scope for understanding cybersecurity incidents and impacts among Small and Medium-sized Enterprises (SMEs) in a developing country context. Also, to the best of our knowledge, previous studies do not account for the extent to which cybersecurity mitigation capabilities of firms can moderate the effect of cybersecurity breaches on labour productivity. Understanding the impact of cybersecurity measures is important as it provides guidance to firms on cybersecurity investment policy and decision-making (Gordon et al., 2016). Therefore, our study seeks to provide answers to the following research questions: What is the effect of cybersecurity breach on labour productivity? Do cyber risk mitigation capabilities matter in the relationship between cybersecurity breach and labour productivity?

To estimate our results, we use the 2016 Enterprise ICT Survey of Kenya which provides a rich source of information on the use of ICTs among firms. As part of our empirical strategy, we first compute risk mitigation capabilities using Principal Component Analysis. Second, we estimate the results using Ordinary Least Squares regression and account for endogeneity using simultaneous equation approach. We find that cybersecurity breach reduces labour productivity at the firm level. We also find that upskilling enables firms to mitigate the negative effect of cybersecurity breach on labour productivity, especially for SMEs. The results further suggest that while IT policy and IT security capabilities can enable firms to improve labour productivity, these measures are not sufficient to offset the adverse effect of cybersecurity breach on labour productivity. Together, the results imply that upskilling is an effective cyber risk mitigation measure against cybersecurity breaches at the firm level.

This study contributes to the literature on digitalisation and entrepreneurship in the context of a developing country. We account for the role of technical and non-technical cyber risk mitigation capabilities in firms. In this way, we align our work with the broader thinking about cybersecurity programmes, as part of a firm's overarching IT governance. Our focus on productivity allows a close investigation into the role

of firm capabilities in the form of skills and related security programmes which themselves drive productivity, as well as mitigate the effect of cyberattacks, for example, through learning and awareness. This paper also contributes to understanding the firm-level effect of cyberattacks and mitigating capabilities in a Sub-Saharan African (SSA) context, where the digital revolution is taking place amidst the challenges of commitment to cybersecurity governance (International Telecommunication Union, 2021). A rich amount of work in SSA has focused on the positive effects of digital capabilities on firm innovation and performance, with limited empirical insights into the business risks of digitalisation (for example, Gaglio et al., 2022; Islam et al., 2018; Masenyetse & Manamathela, 2023; Muzi et al., 2023).

African countries face constraints in the organisational infrastructure and capacity development required for cybersecurity. For example, only 13.6% of African countries have appropriate incentives for cybersecurity development, compared with 65% of European countries (ITU, 2021). This means that African countries lag behind in deploying such instruments as tax incentives, integration of cybersecurity standards into contracts and encouragement of private sector actors to prioritise cybersecurity in their business strategies and operations. The case of Kenya is of special relevance considering that it is an important part of the African digital economy, where digitalisation has transformed business across sectors, especially ICT, financial services and Business Process Outsourcing (Graham & Mann, 2013; Islam & Muzi, 2022; UNCTAD, 2022). However, businesses face cybersecurity threats as the implementation of ICT infrastructure and applications prioritises efficiency and convenience over cybersecurity in Kenya (The Government of Kenya, 2022). In the second quarter of 2023 alone, the National Kenya Computer Incident Response Team – Coordination Centre detected around 139.8 million cyber threat attempts in the form of malware, denial of service and system vulnerabilities (National KE-CIRT/CC, 2023). In the face of cyber threats, Kenya requires stronger efforts in the dimensions of organisational support and capacity development for cybersecurity such as national agencies' implementation of cybersecurity strategies and awareness campaigns, as well as education, training and development of cybersecurity-focused industries (ITU, 2021).

The broader institutional challenges limit the development and implementation of cybersecurity programmes in firms, albeit with unique implications for SMEs. While SMEs leverage the adoption of basic digital technologies in driving business operations and productivity, they are increasingly constrained as such technologies become sophisticated (Kergroach, 2021). The capabilities to make sense of the increasing volume of data powered by digital advances in business processes and govern cybersecurity threats tend to be skewed in favour of a few (large) companies and countries (ITU/UNDP, 2023). For example, small firms face difficulty in upskilling across their workforce in ways that encompass ICT and non-ICT teams (Pedota et al., 2023). Cybersecurity programmes require advanced digital capabilities, for example, the skills to manage devices, personal and institutional data, and maintain privacy (Audrin et al., 2024), as well as the requisite organisational coordination. Given these resource requirements, SMEs face a unique challenge in developing and implementing cybersecurity programmes. This makes them more vulnerable to cybersecurity threats in the same environment as large firms (Raineri & Resig, 2020; Selznick & Lamacchia, 2018; Wang et al., 2024). Despite the importance of cybersecurity for SMEs, research on the impact of cybersecurity breaches and mitigation capabilities has given less attention to SMEs, especially in developing countries (Alharbi et al., 2021).

While we do not compare the analysis of the case country (and by extension SSA countries) with others, our study points to the importance of this underexplored context for extending existing knowledge of cybersecurity breaches and firm performance beyond western industrialised economies. Our paper provides unique insights into the role of upskilling as a critical mechanism through which firms, including SMEs, can deal with the effect of cyberattacks on labour productivity amidst constraining internal resources and institutional environments.

The rest of the paper is structured as follows. The next Section reviews the literature. Section 3 presents the data and key variables. Section 4 provides the estimation strategy. Section 5 presents the results, while Sect. 6 discusses the results with the main conclusion.

2 Related literature

2.1 The nature and productivity effect of cybersecurity breaches

Cybersecurity is the method, line of actions and practices that organisations and/or states follow to protect the confidentiality, integrity and availability of data and assets in the cyber space (Schatz et al., 2017). It takes the form of policies and guidelines, technologies and training that enable an entity to develop capabilities to protect its IT assets, networks and operations, including interaction with external users in the cyber environment. Confidentiality means that access to digital content is reserved for authorised individuals. Integrity ensures that the content can only be modified upon due authorisation, and in line with the stated terms. Availability ensures that authorised users have access to the platform and content when needed, as defined in enabling rights to access and use.

A cybersecurity breach may be an attack aimed to disrupt the platform and activities of the target individual or firm and/or a similar malicious cyber incident aimed to gain unauthorised access to content and commit fraud (Al-Saleh et al., 2015; Lee, 2021). Cybersecurity breaches entail more than the intent to commit fraud. For example, cyberattacks are also in the form of offensive and malicious operations that use ICTs to generate significant losses of confidentiality, integrity and availability of personal devices, computer systems and networks, often with the intent to degrade, disrupt and damage a computer system and its infrastructure (Finnemore & Hollis, 2020).

Cybersecurity incidents take the form of unauthorised access to data, devices, a computer system or network, malware (malicious programme or software aimed to damage or weaken the function of the software, device or computer network) and denial-of-service (ICT-enabled malicious lock out of an authorised user), as well as phishing and other incidents whose nature are not immediately known to the developers of the authorised IT asset (Al-Saleh et al., 2015; Sulaiman et al., 2022).

Cybersecurity breaches have adverse effects on firm operations, sales, revenues, stock market value and reputation (Arcuri et al., 2018; Campbell et al., 2003; Hasan et al., 2021; Huang et al., 2019; Lee, 2021). Cybersecurity incidents deplete firm resources, raise the cost of doing business and contribute to underperformance. The financial, IT and human resources that drive firm productivity constitute the resources that are disrupted and lost in cybersecurity breaches, which means that the breached firm risks decreased productive resources. The financial strength of the firm is constrained as cyber risks result in credit downgrade and higher costs of borrowing or loss of stock market value of the breached firm (Huang et al., 2023; Kamiya et al., 2021). Operational shocks mean that the affected firm commits human and material resources to detect, monitor and recover breached resources, leading to productivity loss, as these resources are unavailable for productive activities (Cavusoglu et al., 2004; Lee & Choi, 2021).

Makridis and Dean (2018), for example, examine the effect of data breaches on firm-level productivity using data from the Privacy Rights Clearinghouse (PRC) and the US Department of Health and Human Services (HHS) databases. The study finds that a 10 per cent increase in data breaches is associated with a 0.2 per cent reduction in productivity at the firm level. However, this result is not robust to different specifications and datasets. The study shows skewness in the distribution of observed data breaches and heterogeneity across sectors and between public and private firms.

Kamiya et al. (2021) develop and test a theoretical model on the impact of cyberattacks on targeted firms. The study reveals that cyberattacks resulting in the loss of personal financial information can lead to a significant loss of shareholder wealth compared to attacks without the loss of personal financial information. The study further suggests that the loss of shareholder wealth is driven by reputation costs. Thus, firms that record high drops in sales growth also experience a higher loss in shareholder wealth. Firms that experience cyberattacks also tend to invest more in risk management. The study finds similar results among competitor firms.

Tripathi and Mukhopadhyay (2020) investigate the effect of data privacy breach on firm performance using an event study methodology. The study shows a negative relationship between data privacy breach and the market value of firms. This effect is more pronounced among smaller firms than large firms. Similarly, Morse et al. (2011) employ the event study method to examine the impact of data security breach on the behaviour of the stock market. The evidence

points to negative stock price returns following a data breach. The study further shows that the source of data breach matters in the relationship between data breach and the stock market.

2.2 Cybersecurity risk mitigation and firm productivity

When faced with cybersecurity risk, firms tend to ignore, accept, transfer or mitigate the risk (Tsiakis & Stephanides, 2005). Taking action to reduce the impact of the risk is seen as the most likely option when the effect of the cyber breaches is expected to be high such that the cost of mitigation is lower than the cost of a successful cyber incident (Cavusoglu et al., 2004; Kamiya et al., 2021). The rising waves of cyber incidents mean that organisations must develop cybersecurity programmes as part of IT governance strategy. Cybersecurity governance entails programmes that define and promote the protection of an organisation's data, systems and networks, as well as the coordination of people and processes to ensure that its IT assets are protected from cyberattacks (Hasan et al., 2021). This means that IT security governance goes beyond traditional defence strategies that focus on technical detection and response to cyber incidents.

The technical defence strategy aims to identify risk, monitor and respond to cyber incidents. This involves the software or hardware application deployed to identify malicious activities and practices in a device or network and the information it hosts (Hasan et al., 2021). Firewalls, antivirus, data encryption and authentication are major technical defence solutions that enable detection, protection, recovery and continuous monitoring of intrusion in cyber systems (Sulaiman et al., 2022).

The people element is critical to IT defence strategy considering that the activities and interactions of stakeholders with IT assets, as well as among themselves, affect the firm's cybersecurity. This element focuses on internal users such as employees, and their interaction with systems and external users, for example, customers in the value chain (Gani et al., 2023; Lee, 2021). Employees' rights and responsibilities, awareness, motivation, trust, behaviour, experience and skills relevant to cybersecurity play an important role in the handling of an organisation's IT asset, policy and process (Bokhari & Manzoor, 2022; Galinec et al., 2017; Li et al., 2019).

IT security governance is a subset of an organisation's overall IT governance, which lays out the frameworks or rules regarding the rights and accountability in the use of IT assets, with a focus on clarity about the decision on who uses IT, who makes the decision and how activities related to these decisions are to be monitored (Weill & Ross, 2004). The top executives or board have the mandate to guide the formulation and implementation of IT strategy and ensure its alignment with business value (Van Grembergen, 2002). IT governance lays out the structures, processes and relations in the development and implementation of IT-enabled initiatives and the reduction of related risks. The structure entails defining the decision-making responsibility which lies with the executives and committees that lay out the formal guidelines that govern the broader organisational IT operations. The process entails aligning the decision-making and overall IT management strategy with business needs, while the relational aspect of IT governance ensures knowledge sharing, peer learning and coordination between teams (Van Grembergen et al., 2004; Zhen et al., 2021).

The development and implementation of IT governance frameworks can help to reduce IT-related risks and improve operational performance (Bradley et al., 2012). IT risk mitigation programmes and actions can contribute to firms' overall IT governance, which enables internal process improvement, cost reduction and effective service delivery that result in productivity gains (Lunardi et al., 2014). IT security governance promotes best practices that support safe and secure data sharing, collaboration, system integration and reduction in data breaches (Gani et al., 2023). Effective management of cyber incidents can reduce breach-related costs, improve stakeholder confidence, including investors, and ease the mobilisation of productive resources for improved firm performance.

Effective cyber risk mitigation programmes can eliminate or minimise breach-induced downtimes, improve business efficiency and maintain firm productivity (Sonnenreich et al., 2005). Strengthening employees' skills with IT risk reduction solutions, improved security policy awareness among employees, and robust IT security measures will minimise data breaches and vulnerabilities that may result in productivity loss (Alqahtani, 2017; Bokhari & Manzoor, 2022).

While these studies recognise the potential of cybersecurity policies/programmes, empirical work on their role in mitigating the effect of cyberattacks on productivity remains underexplored. For example, Alqahtani (2017) presents a case study of IT security maturity in organisations based on semi-structured interviews with managers. However, it does not address the question of the effect of cyber security practices/systems on firm operations and productivity. Bokhari and Manzoor (2022)'s study on Information Security Management System (ISMS) and firm performance focuses on the role of brand reputation in cyber security breaches. Considering the sophistication of cybersecurity breaches, it is unclear whether and how upskilling (advancement of digital skills in firms, beyond basic IT literacy) mitigates the effect of cyberattacks on productivity, as well as the variability of these links in small and large firms. While cybersecurity measures are broadly encapsulated in IT governance programmes, the question about whether and how IT policy-related elements (written standards/documentation and awareness) and technical applications (anti-intrusion and anti-virus apps) remains unanswered.

The objective of this paper is to understand the effect of cybersecurity breach on labour productivity and the moderating role of cyber risk mitigation capabilities including upskilling, IT policy and IT security. We expect that cyber risk mitigation capability of firms will enable them to mitigate the adverse effect of cybersecurity breach on labour productivity.

3 Data and key variables

This study is based on the 2016 Enterprise ICT Survey of Kenya. This survey provides unique information on access to and use of ICTs such as the Internet, mobile applications, communication applications, online applications, and ICT security and management policies among others at the firm level. The survey was designed to provide firm level data on access to and usage of ICT at the national level in line with UNCTAD manual for the production of statistics. The survey covers all the sections of the ISIC Rev. 4 except under section A (agricultural, forestry, and fishing) where only firms engaged in horticulture were included. The survey adopted a stratified random sampling methodology. In particular, the survey used a representative probability sampling approach to arrive at a nationally representative sample. Firms were selected based on a stratified random sampling methodology. The power allocation method was used to determine the number of firms per stratum. Data collection took place between 23 February 2016 and 6 May 2016 using paper questionnaires. Overall, the survey targeted 4,000 firms, out of which 3,530 firms responded, leading to a response rate of 88.3 per cent.

We use as our dependent variable labour productivity which is computed as turnover divided by the total number of employees (in logs). A similar approach has been adopted by previous studies to measure labour productivity at the firm level (Fu et al., 2018; Motta, 2020). The main independent variables of interest are cybersecurity breach and cyber risk mitigation capability variables. We measure cybersecurity breach using two variables. First, we measure cybersecurity breach with a dummy variable that equals 1 if a firm experienced a virus attack leading to the loss of data, time, or damage to software, and 0 otherwise. Second, we measure cybersecurity breach with a binary variable that equals 1 if a firm experienced an online crime[1] including hacking, phishing, identity theft, website vandalism, computer virus, theft of money and information, and 0 otherwise.

We further take advantage of the richness of the dataset to compute our capability variables using Principal Component Analysis. Following a common practice in the literature (eg. Ndubuisi et al., 2021), we retained components using the 1 eigenvalue cut-off point and employed varimax rotation to simplify the interpretation of the variable loadings. We identified 7 components that correspond to our capability indicators as shown in Table 1. We name the first component upskilling given that it comprises 5 variables that respectively measure if the firm received the following training: technical support for equipment repair and maintenance; technical support for the internal system of the government organization; software development; development of web portals, hosting providers and other information services on

[1] The difference between the virus attack variable and the online crime variable is as follows: The online crime variable accounts for other possible cybersecurity breaches at the firm level including hacking, phishing, identity theft, website vandalism, computer virus, theft of money and information whereas the virus attack variable only account for firms experience of virus attack at the firm level.

Table 1 Capability dimensions using PCA

	Comp 1 Upskilling	Comp 2 IT policy	Comp 3 digital infrastructure	Comp 4 IT security	Comp 5 Mobile commerce	Comp 6 Ecommerce	Comp 7 digital finance
Mobile money	-0.027	-0.059	-0.003	0.018	0.105	0.004	**0.646**
Mobile banking	0.021	0.027	0.001	-0.012	-0.077	-0.002	**0.750**
Computer penetration	-0.007	0.003	**0.706**	0.006	0.002	-0.012	0.001
Internet penetration	0.005	-0.007	**0.704**	-0.005	-0.001	0.010	-0.002
Technical support for equipment repair and maintenance	**0.429**	-0.064	0.004	0.129	0.008	-0.026	-0.040
Technical support for Internal system	**0.415**	0.001	0.023	-0.152	-0.026	0.021	-0.006
Technical support for software development	**0.459**	0.035	-0.021	-0.029	0.021	-0.014	-0.007
Technical support for the development of web portals	**0.444**	0.019	0.022	-0.005	-0.019	0.063	0.047
Technical support for electrical infrastructure or networks	**0.484**	0.008	-0.020	0.034	0.018	-0.040	0.016
Risk detection	0.015	-0.127	0.020	**0.596**	0.004	0.040	-0.051
Authentication and safety	-0.015	0.036	-0.022	**0.626**	-0.001	-0.023	0.034
Data backup	0.011	0.198	0.018	**0.448**	-0.014	-0.021	0.029
Place orders online	-0.005	0.008	-0.005	0.037	-0.013	**0.685**	0.051
Receive orders online	0.001	0.002	0.003	-0.030	0.014	**0.719**	-0.044
Receive orders via mobile phones	0.003	-0.010	0.017	0.009	**0.703**	0.019	-0.020
Place orders via mobile phones	0.001	0.014	-0.016	-0.011	**0.698**	-0.016	0.008
IT Policy	0.014	**0.604**	-0.010	-0.008	0.000	0.034	-0.028
IT security policy	0.003	**0.603**	-0.013	0.030	-0.003	-0.001	-0.020
Aware of CIRT	-0.030	**0.452**	0.039	-0.084	0.023	-0.041	0.065

CIRT is Computer Incident Response Team. PCA connotes Principal Component Analysis

the Internet; and technical support on the electrical infrastructure and networks.

The second component is named IT policy and it includes 3 variables that respectively capture if the firm has an information technology (IT) policy in place, has an IT security policy in place, and is aware of the National Kenya Computer Incident Response Team. The third component is named digital infrastructure and it comprises 2 variables that measure computer and Internet penetration among employees. Component 4 is named IT security and it comprises 3 variables that capture if the firm has up-to-date IT security measures including risk detection (antivirus, antispyware, firewall, spam filter, and intrusion detection system), authentication and safety (authentication software or hardware, and computer password), and regular backup of data. Components 5, 6 and 7 comprise variables that correspond to mobile commerce, electronic commerce, and digital finance, respectively. The naming of each component reflects mainly the variables on which it has high loadings. Following the literature in Sect. 2.2, we use upskilling, IT policy, and IT security indicators as proxies for cyber risk mitigation capabilities at the firm level while the other capability measures are included in the analysis as controls. For ease of interpretation, we normalised the capability variables derived from PCA using the Min–Max method[2] where values lie between 0 and 1. In this case, the capability of firms improves as their capability scores move from 0 to 1. Table 2 presents the descriptive statistics, while the definition of variables are provided in the Appendix.

[2] $Capability_j = \frac{\varphi_j - min_j(\varphi)}{max_j(\varphi) - min_j(\varphi)}$ where φ_j is the actual value of capability derived from PCA, and $min_j(\varphi)$ and $max_j(\varphi)$ are the minimum and maximum values, respectively.

Table 2 Descriptive statistics of main variables

Variable	Obs	Mean	Std. dev	Min	Max
Labour productivity (in logs)	2,520	13.950	1.965	7.075	24.823
Virus Attack	3,482	0.294	0.456	0	1
Online crime	3,300	0.262	0.440	0	1
Upskilling	2,315	0.578	0.346	0	1
IT Policy	2,315	0.350	0.282	0	1
Digital infrastructure	2,315	0.044	0.036	0	1
IT security	2,315	0.804	0.206	0	1
Mobile commerce	2,315	0.735	0.325	0	1
E-commerce	2,315	0.373	0.357	0	1
Digital Finance	2,315	0.539	0.289	0	1
SME	3,409	0.852	0.356	0	1
Regional level cyberattacks	3,529	0 0.294	0.0596	0	1
Sector level cyberattacks	3,529	0.294	0.041	0.143	0.533

4 Estimation strategy

We are interested in understanding the effect of cybersecurity breach on labour productivity and how this effect is conditioned by cyber risk mitigation capabilities of firms. To achieve this objective, we first consider the following baseline model.

$$LogLP_{isr} = \beta_0 + \beta_1 Cyberattack_{isr} + \beta_2 Mitigation\ Capabilties_{isr} + \beta_3 C_{isr} + \delta_s + \lambda_r + \varepsilon_{isr} \quad (1)$$

where $LogLP_{isr}$ denotes labour productivity of firm i operating in sector s and region r. $Cyberattack_{isr}$ connotes cybersecurity breach at the firm level which we measure using two variables (virus attack and online crime). $MitigationCapabilties_{isr}$ is a vector of the various measures of cyber risk mitigation capabilities which include upskilling, IT policy, and IT security. C_{isr} corresponds to a vector of controls. Given that ICT affects firm-level productivity (Grimes et al., 2012; Kılıçaslan et al., 2017), we control for other forms of digital capabilities at the firm level such as digital infrastructure, mobile commerce, E-commerce, and digital finance. Furthermore, we control for firm size with a dummy variable that equals 1 if the firm is an SME, and 0 otherwise. In this case, we define SMEs as firms with less than 100 employees while firms with 100 employees and above are classified as large firms. This approach is similar to the classification employed in the World Bank Enterprise Surveys to define firm size. We also control for sector fixed effects and regional fixed effects which are represented by δ_s and λ_r respectively. β_1 and β_2 are parameters of interest to be estimated, and ε_{is} is the error term.

4.1 Endogeneity concerns

We anticipate that unobserved factors can simultaneously affect cybersecurity breach and labour productivity at the firm level leading to biased estimates of our baseline results. Also, there is the possibility of reverse causality between cybersecurity breach and labour productivity. A possible way out could be to use the lagged values of cybersecurity breach and other independent variables to address reverse causality concerns. However, we are not able to follow this procedure given that the data employed for this study is cross-sectional. While instrumental variable techniques are desirable, finding valid instrumental variables for cross-sectional studies is a challenge. To address endogeneity concerns, however, we adopt a recursive simultaneous equation modelling approach similar to the method proposed by Green (1998) to account for endogeneity as specified in Eqs. 2 and 3.

$$Cyberattack_{isr} = \alpha_0 + \alpha_1 Mitigation\ Capabilties_{isr} + \alpha_2 C_{isr} + Z + \mu_{isr} \quad (2)$$

$$LogLP_{isr} = \gamma_0 + \gamma_1 Cyberattack_{isr} + \gamma_2 Mitigation\ Capabilties_{isr} + \gamma_3 C_{isr} + e_{isr} \quad (3)$$

where α_1, γ_1 and γ_2 are parameters of interest to be estimated. μ_{isr} and e_{isr} are the error terms which are assumed to be jointly normally distributed.

We carried out this estimation using Roodman (2011) conditional mixed-process (CMP) framework which allows for fitting simultaneous equation models. In this case, we jointly estimate the determinants of cybersecurity breach with a probit model (Eq. 2) and the effect of cybersecurity breach on labour productivity using OLS (Eq. 3). Equation 3 is our main equation of interest. To improve identification, we perform exclusion restriction with vector Z which corresponds to two variables measuring exposure to cybersecurity breach. The first variable captures the share of firms that experienced cybersecurity breach at the sector level while the second variable measures the share of firms that experienced cybersecurity breach at the regional level. To qualify as a good instrument vector Z must satisfy the following conditions: The vector Z should have no direct relationship with labour productivity (the outcome variable of interest), but only affect the outcome variable through its effect on cybersecurity breach at the firm level (Angrist et al., 1996). We assume that exposure to cybersecurity breach at the sector and regional levels (Z) can only affect labour productivity through its effect on cybersecurity breach at the firm level. Thus, we expect that firms that are in regions and sectors with a high prevalence of cybersecurity breach will be more susceptible to cyberattacks leading to lower productivity. A similar strategy has been used to compute instrumental variables in previous studies (Acemoglu & Restrepo, 2020; Bloom et al., 2016). We exclude sector and regional fixed effects from Eqs. 2 and 3 given that our Z variables are measured at these levels.

Further, in line with our study objective, we allow for the interaction between our cybersecurity breach variables and risk mitigation variables to capture how these interactions affect labour productivity using Eq. 4 and 5.

$$Cyberattack_{isr} = \alpha_0 + \alpha_1 Mitigation\ Capabilties_{isr} + \alpha_2 C_{isr} + Z + \mu_{isr} \tag{4}$$

$$LogLP_{isr} = \gamma_0 + \gamma_1 Cyberattack_{isr} + \gamma_2 Mitigation\ Capabilties_{isr} + \gamma_3 (Cyberattack_{isr} \times Migitation\ Capabilties_{isr}) + \gamma_4 C_{isr} + e_{isr} \tag{5}$$

where γ_3 of Eq. 4 is the parameter of interest that measures the interaction between cybersecurity breach and cyber risk mitigation capabilities at the firm level.

5 Results

5.1 Cybersecurity breach and labour productivity

We present the baseline results in Table 3 followed by the results that account for endogeneity. Except for Table 3, all other results are estimated using simultaneous equation models in line with our estimation strategy as discussed in Sect. 4.

In columns (1) to (3) of Table 3 we report the estimated results when we regress labour productivity on our first measure of cybersecurity breach which equals 1 if a firm has experienced a virus attack. In addition to the full sample results in column (1), we show the results for SMEs on the one hand, and large firms on the other in columns (2) and (3) to understand how results differ by firm size.

The baseline result in column (1) points to a negative and statistically significant relationship between virus attack and labour productivity. This result which is significant at the 1 per cent significance level suggests that virus attack reduces labour productivity by about 35 per cent.[3] In column (2), we find similar results among the subsample of SMEs. The results indicate that virus attack has a significant negative effect on labour productivity among SMEs. Thus, firms that experienced a virus attack record about 33 per cent decline in labour productivity compared with firms without a virus attack. Column (3) further shows that this effect is equally present among large firms leading to about 46 per cent reduction in labour productivity. SMEs and large firms are negatively affected by virus attacks and this effect is higher among large firms compared to SMEs. However, comparing results between SMEs and large firms needs to be treated with caution due to differences in sample size between the two sub-samples.

In columns (4) to (6) we re-estimate our results but, in this case, we regress labour productivity on our second measure of cybersecurity breach that equals 1 if a firm experienced any form of online crime. Thus, we extend the analysis beyond virus attacks to cover other forms of cybersecurity breach

[3] Due to the log transformation of the dependent variable (labour productivity), we exponentiate the coefficient of our independent variable to compute the percentage of the effect size. This applies to all other estimates.

Table 3 Cybersecurity breach and labour productivity: baseline estimates [Dependent variable: Log of labour productivity]

	Virus Attack			Online Crime		
	(1)	(2)	(3)	(4)	(5)	(6)
	Full sample	SME	Large firm	Full Sample	SME	Large firms
Cybersecurity breach (Virus attack)	-0.436***	-0.395***	-0.620***			
	(0.064)	(0.085)	(0.184)			
Cybersecurity breach (Online crime)				-0.311***	-0.302***	-0.243
				(0.067)	(0.072)	(0.194)
Upskilling	0.121	-0.040	1.451***	0.183	-0.010	1.786***
	(0.101)	(0.159)	(0.435)	(0.138)	(0.217)	(0.424)
IT Policy	0.521***	0.517***	0.496	0.520***	0.551***	0.218
	(0.131)	(0.152)	(0.600)	(0.135)	(0.164)	(0.565)
Digital infrastructure	2.465***	2.301***	-0.506	2.851***	2.810***	-1.019
	(0.574)	(0.606)	(6.603)	(0.522)	(0.547)	(7.353)
IT security	0.954***	0.907***	1.773**	0.954***	0.874***	1.711**
	(0.206)	(0.240)	(0.788)	(0.176)	(0.215)	(0.762)
Mobile commerce	0.053	0.035	0.459	0.002	0.011	0.229
	(0.101)	(0.098)	(0.354)	(0.096)	(0.110)	(0.226)
E-commerce	0.094	0.174	0.036	0.111	0.186	0.058
	(0.179)	(0.265)	(0.241)	(0.149)	(0.236)	(0.301)
Digital finance	-0.338	-0.288	-0.684	-0.353	-0.308	-0.728
	(0.224)	(0.171)	(0.582)	(0.253)	(0.186)	(0.668)
SME	-0.055			-0.078		
	(0.128)			(0.162)		
Constant	14.172***	13.672***	11.641***	14.123***	13.188***	11.897***
	(0.331)	(0.671)	(0.927)	(0.349)	(0.261)	(0.837)
Observations	1,712	1,420	292	1,635	1,356	279
R-squared	0.160	0.163	0.337	0.154	0.159	0.351
Sector FE	Yes	Yes	Yes	Yes	Yes	Yes
Location FE	Yes	Yes	Yes	Yes	Yes	Yes

Robust standard errors in parentheses are clustered at the regional (county) level. *** $p<0.01$, ** $p<0.05$.

as indicated in the variable definition section. In line with our estimation strategy, we report the results for the full sample in column (4). The evidence based on the full sample suggests that online crime exposure leads to a reduction in labour productivity among firms by 27 per cent. The results also show a negative and significant relationship between online crime and labour productivity for SMEs. In particular, we find that online crime leads to 26 per cent decline in labour productivity for this category of firms. However, the relationship between online crime and labour productivity is not significant for large firms.

Further, we present the results that account for endogeneity in Table 4 to check for the robustness of our baseline estimations. Panels A and B of Table 4 present the estimates for the cybersecurity breach and labour productivity equations, respectively (Eqs. 2 and 3). The results in Panel A indicate that our Z variables measured at the sector and regional levels significantly predict firm-level cybersecurity breach. This suggests that location in regions or sectors with a high prevalence of cybersecurity breach significantly exposes firms to cyberattacks.

Turning to our main equation of interest, Panel B, we find that cybersecurity breaches proxied by virus attacks and online crime have statistically significant negative effects on labour productivity at the firm level including SMEs and large firms as shown in columns (1) – (6). Overall, the findings suggest that cybersecurity breach is counterproductive to firms.

Table 4 Cybersecurity breach and labour productivity: simultaneous equation estimates [Dependent variable: Log of labour productivity]

	Virus attack			Online crime		
	(1)	(2)	(3)	(4)	(5)	(6)
Panel A	Full sample	SMEs	Large firms	Full Sample	SMEs	Large firms
Regional level cyberattacks (proportion)	2.513***	2.886***	1.605***	1.561***	1.466**	1.995***
	(0.546)	(0.745)	(0.533)	(0.441)	(0.636)	(0.558)
Sector level cyberattacks (proportion)	3.270***	2.636***	5.598***	3.749***	3.441***	5.577***
	(0.693)	(0.696)	(1.113)	(0.919)	(1.013)	(0.995)
Upskilling	0.010	0.004	0.077	0.117	0.112	0.160
	(0.057)	(0.062)	(0.219)	(0.070)	(0.086)	(0.158)
IT Policy	-0.138	-0.185**	0.059	0.125	0.050	0.511**
	(0.097)	(0.094)	(0.264)	(0.148)	(0.142)	(0.214)
Digital infrastructure	-0.476	-0.136	-3.097	0.574	0.889	-2.293
	(0.544)	(0.608)	(2.087)	(0.948)	(0.850)	(2.280)
IT security	0.546***	0.544***	0.561	0.906***	0.922***	1.198***
	(0.162)	(0.167)	(0.382)	(0.121)	(0.139)	(0.284)
Mobile commerce	0.421***	0.424***	0.360**	0.151***	0.154***	0.225
	(0.061)	(0.070)	(0.177)	(0.042)	(0.059)	(0.154)
E-commerce	0.212***	0.262***	-0.005	0.305***	0.289***	0.392**
	(0.048)	(0.042)	(0.163)	(0.052)	(0.054)	(0.177)
Digital finance	0.238***	0.235**	0.378	0.288***	0.295***	0.270
	(0.090)	(0.102)	(0.199)	(0.078)	(0.097)	(0.149)
SME	-0.033			-0.076		
	(0.063)			(0.083)		
_cons	-3.011***	-2.989***	-3.484***	-3.306***	-3.269***	-4.490***
	(0.313)	(0.314)	(0.578)	(0.303)	(0.310)	(0.706)
Panel B						
Dependent variable: Log of labour productivity						
Virus attack	-2.893***	-2.465***	-3.837***			
	(0.299)	(0.490)	(0.442)			
Online Crime				-2.805***	-2.586***	-3.455***
				(0.221)	(0.317)	(0.460)
Upskilling	0.223**	0.121	0.964**	0.366***	0.220	1.344***
	(0.105)	(0.154)	(0.384)	(0.137)	(0.214)	(0.399)
IT Policy	0.459***	0.361**	0.915	0.704***	0.564***	1.379**
	(0.159)	(0.164)	(0.664)	(0.175)	(0.178)	(0.571)
Digital infrastructure	3.912***	3.873***	4.599	5.161***	5.186***	4.033
	(1.005)	(0.913)	(6.107)	(1.495)	(1.215)	(8.670)
IT security	1.393***	1.309***	2.712***	1.558***	1.501***	3.097***
	(0.311)	(0.358)	(0.939)	(0.174)	(0.233)	(0.684)
Mobile commerce	0.530***	0.408***	1.011**	0.187	0.142	0.425
	(0.162)	(0.139)	(0.402)	(0.112)	(0.138)	(0.484)
E-commerce	0.241	0.329	-0.285	0.313**	0.342	0.222
	(0.198)	(0.278)	(0.175)	(0.159)	(0.236)	(0.420)
Digital finance	-0.167	-0.207	-0.123	-0.124	-0.144	-0.142
	(0.200)	(0.164)	(0.633)	(0.235)	(0.173)	(0.785)
SME	0.119			0.033		
	(0.150)			(0.216)		

Table 4 (continued)

	Virus attack			Online crime		
	(1)	(2)	(3)	(4)	(5)	(6)
_cons	12.996***	13.210***	11.236***	12.793***	12.965***	10.499***
	(0.452)	(0.384)	(0.848)	(0.394)	(0.308)	(0.870)
rho_12	0.677***	0.589***	0.828***	0.680***	0.628***	0.814***
	(0.050)	(0.090)	(0.036)	(0.035)	(0.047)	(0.041)
Wald $\chi 2$	4421.94	1025.70	1576.17	11230.54	2669.74	940.16
Probability > $\chi 2$	0.000	0.000	0.000	0.000	0.000	0.000
No. of observations	2308	1912	396	2208	1829	379

The table reports the coefficient estimates using simultaneous equation models. Robust standard errors in parentheses are clustered at the regional (county) level

** $p < 0.05$, *** $p < 0.01$

The evidence shows that cybersecurity breach can lead to a reduction in productivity at the firm level. This finding is consistent with the literature indicating that cybersecurity breach can affect labour productivity by disrupting operations or business processes including loss of data, revenue, time or damage to software (Arcuri et al., 2018; Campbell et al., 2003; Hasan et al., 2021).

The firm-level cyber risk mitigation capability variables yield interesting results as indicated in Table 4. Our first risk mitigation capability of interest is upskilling which captures on-the-job training in information technology including equipment repair and maintenance, software development, development of web portals, and electrical infrastructure among others. In columns (1) and (4) we find significant positive effects of upskilling on labour productivity for the full sample. We also find a significant positive effect between upskilling and labour productivity among large firms as indicated in columns (3) and (6). However, the results show no significant relationship between upskilling and labour productivity for the SMEs subsample. This is probably because large firms are better placed to invest in upskilling compared with SMEs. In this case, we expect that large firms will benefit more from upskilling than SMEs. Our second risk mitigation capability of interest is IT policy which measures firms' readiness in terms of information technology policy, information technology security policy, and awareness of computer incident response team. We expect that firms with good IT policies will exhibit higher levels of productivity given that such firms will be able to adopt appropriate measures to maximise the gains from information technology while at the same time reducing the potential effect of cybersecurity breaches. The results in Table 4 show a positive and significant relationship between IT policy and labour productivity except in column 3 when we examine the effect of virus attack on labour productivity for large firms. In line with our expectations, the evidence implies that IT policy improves labour productivity at the firm level. Furthermore, we find a positive and significant relationship between our third cyber risk mitigation capability, IT security, and labour productivity for the full sample, SMEs, and large firms. The evidence suggests that IT security capability enhances labour productivity.

Turning to the control variables, the results show a positive and significant relationship between digital infrastructure and labour productivity. The results are significant for the full sample and SMEs sample at 1 per cent significant levels. We expect that digital infrastructure will contribute to improvement in labour productivity given its potential to enhance efficiency and reduce manual completion of tasks which is time-consuming. We also relate labour productivity with mobile commerce, E-commerce, and digital finance. We find that mobile commerce does matter for labour productivity in columns (1) – (3) and E-commerce tends to enhance labour productivity when we proxied cybersecurity breach with online crime in our model (column 4). However, we find no statistically significant relationship between digital finance and labour productivity.

Table 5 Cybersecurity breach and risk mitigation capability interaction (Full Sample) [Dependent variable: Log of labour productivity]

	Virus attack			Online crime		
	(1)	(2)	(3)	(4)	(5)	(6)
Virus attack	-3.199***	-2.819***	-3.048***			
	(0.281)	(0.375)	(0.319)			
Online crime				-3.133***	-2.901***	-2.869***
				(0.181)	(0.143)	(0.232)
Upskilling	0.050	0.226**	0.222**	0.221	0.364***	0.365***
	(0.120)	(0.106)	(0.104)	(0.148)	(0.136)	(0.137)
IT Policy	0.447***	0.534***	0.458***	0.694***	0.622**	0.703***
	(0.156)	(0.158)	(0.158)	(0.174)	(0.255)	(0.176)
IT security	1.423***	1.382***	1.352***	1.598***	1.569***	1.548***
	(0.312)	(0.316)	(0.389)	(0.165)	(0.166)	(0.208)
Virus attack X Upskilling	0.495***					
	(0.151)					
Virus attack X IT Policy		-0.215				
		(0.282)				
Virus attack X IT security			0.187			
			(0.406)			
Online crime X Upskilling				0.500***		
				(0.171)		
Online crime X IT Policy					0.253	
					(0.367)	
Online crime X IT security						0.075
						(0.393)
_cons	13.080***	12.977***	13.030***	12.844***	12.803***	12.801***
	(0.467)	(0.444)	(0.509)	(0.399)	(0.403)	(0.414)
rho_12	0.681***	0.824***	0.678***	0.685***	0.681***	0.680***
	(0.049)	(0.093)	(0.050)	(0.031)	(0.034)	(0.034)
Wald $\chi 2$	5421.32	4614.74	4474.26	10,888.70	11,381.92	13,634.71
Probability > $\chi 2$	0.000	0.000	0.000	0.000	0.000	0.000
No. of observations	2308	2308	2308	2208	2208	2208

The table reports the coefficient estimates using simultaneous equation models but only the equation of interest is reported. Robust standard errors in parentheses are clustered at the regional (county) level. The estimation includes all controls as in the baseline

** $p<0.05$, *** $p<0.01$

5.2 Cyber risk mitigation capabilities, cybersecurity breach, and labour productivity

Table 5 reports the estimates for the interaction between cybersecurity breach and risk mitigation capabilities using the full sample. We estimate the results using Eqs. 4 and 5 but to save space we only report the equation of interest that captures the interactions (Eq. 5). Column (1) provides the estimates for the interaction between our first measure of cybersecurity breach, virus attack, and upskilling. The coefficient associated with the interaction term is positive and statistically significant at the 1 per cent significance level. This evidence implies that upskilling can enable firms to mitigate the negative effect of cybersecurity breach on labour productivity. We also report the results of the interaction between IT policy and virus attack in column 2. As evident in Table 5, the coefficient associated with the interaction term is not statistically significant. The evidence suggests that IT policy is not enough to offset the negative effect of cybersecurity breach at the firm level. Similarly, in column (3) we find no significant interaction effect for virus attack and IT security. In columns (4)—(6), we report the results for the interaction analyses where the independent variable is online crime, our second measure of a cybersecurity breach. Following the same estimation procedure, we find that the interaction between online crime and

upskilling is positive and statistically significant at the 1 per cent significance level. We find no significant interaction effect between online crime and other cyber risk mitigation capability measures.

5.3 Cyber risk mitigation capabilities, cybersecurity breach, and labour productivity (SMEs vs large firms)

We further explore the interaction between digital capabilities and cybersecurity breach among SMEs and large firms. Table 6 presents the results of the interplay between cybersecurity breach and digital capability variables in relation to labour productivity for SMEs. The estimates for the virus attack variable are reported in columns (1) to (3), whereas the results for the online crime variable are presented in columns (4) to (6). The results in column (1) indicate a positive and significant interaction effect between virus attack and upskilling. The evidence implies that upskilling among SMEs has the potential to offset the negative effect of virus attacks on labour productivity. We find no significant interaction effect between virus attack and IT policy on the one hand, and IT security on the other hand. We find

Table 6 Cybersecurity breach and risk mitigation capability interaction (SMEs) [Dependent variable: Log of labour productivity]

	Virus attack			Online crime		
	(1)	(2)	(3)	(4)	(5)	(6)
Virus attack	-2.912***	-2.429***	-2.518***			
	(0.470)	(0.516)	(0.376)			
Online crime				-2.989***	-2.658***	-2.565***
				(0.315)	(0.231)	(0.319)
Upskilling	-0.131	0.123	0.121	0.048	0.219	0.221
	(0.173)	(0.155)	(0.153)	(0.241)	(0.213)	(0.214)
IT Policy	0.348**	0.403***	0.361**	0.556***	0.494	0.564***
	(0.160)	(0.124)	(0.164)	(0.178)	(0.256)	(0.180)
IT security	1.360***	1.304***	1.295***	1.550***	1.509***	1.505***
	(0.358)	(0.358)	(0.468)	(0.226)	(0.221)	(0.279)
Virus attack X Upskilling	0.736***					
	(0.196)					
Virus attack X IT Policy		-0.129				
		(0.313)				
Virus attack X IT security			0.065			
			(0.563)			
Online crime X Upskilling				0.623***		
				(0.192)		
Online crime X IT Policy					0.228	
					(0.438)	
Online crime X IT security						-0.024
						(0.506)
_cons	13.322***	13.200***	13.222***	13.026***	12.979***	12.962***
	(0.388)	(0.387)	(0.474)	(0.306)	(0.325)	(0.343)
rho_12	0.599***	0.590***	0.590***	0.638***	0.629***	0.628***
	(0.084)	(0.090)	(0.089)	(0.042)	(0.047)	(0.046)
Wald $\chi 2$	1123.02	1017.88	1068.02	2621.09	2715.58	3183.10
Probability > $\chi 2$	0.000	0.000	0.000	0.000	0.000	0.000
No. of observations	1912	1912	1912	1829	1829	1829

The table reports the coefficient estimates using simultaneous equation models but only the equation of interest is reported. Robust standard errors in parentheses are clustered at the regional (county) level. The estimation includes all controls as in the baseline

** $p < 0.05$, *** $p < 0.01$

a similar effect in column (4). Thus, we find that, for the SME sample, the interaction term associated with online crime and upskilling is negative and statistically significant at the 1 per cent significance level.

Table 7 reports the results when we estimate the interaction between cyber risk mitigation capabilities and cybersecurity breach for large firms. For the large firm subsample, we find that the coefficient associated with the interaction between virus attack and upskilling is negative and statistically significant. However, we find no significant interaction effect between online crime and other measures of cyber risk mitigation capabilities. We interpret the results of the large firms with caution due to the small sample size.

To further test for the robustness of our results, we estimate all interactions together and the results are presented in Table 8. We find that the effects of the interaction between cybersecurity breach variables and upskilling remain robust for the full and SME samples as shown in columns (1)-(6) while IT security capability tends to matter for large firms (column 3). Overall, the evidence suggests that upskilling can help firms mitigate the negative effect of cybersecurity breach on labour productivity.

Table 7 Cybersecurity breach and risk mitigation capability interaction (large firms) [Dependent variable: Log of labour productivity]

	Virus attack			Online crime		
	(1)	(2)	(3)	(4)	(5)	(6)
Virus attack	-2.910***	-3.481***	-5.986***			
	(0.750)	(0.405)	(0.975)			
Online crime				-2.760***	-3.252***	-2.768**
				(0.940)	(0.953)	(1.357)
Upskilling	1.507***	0.983***	0.916**	1.691***	1.351***	1.342***
	(0.471)	(0.380)	(0.391)	(0.545)	(0.405)	(0.395)
IT Policy	0.959	1.169	0.838	1.380**	1.502***	1.395**
	(0.684)	(0.699)	(0.688)	(0.578)	(0.430)	(0.574)
IT security	2.874***	2.766***	2.105**	3.086***	3.107***	3.243***
	(0.932)	(0.928)	(1.052)	(0.684)	(0.674)	(0.741)
Virus attack X Upskilling	-1.295**					
	(0.625)					
Virus attack X IT Policy		-0.639				
		(0.400)				
Virus attack X IT security			2.356			
			(1.322)			
Online crime X Upskilling				-0.924		
				(0.788)		
Online crime X IT Policy					-0.348	
					(0.981)	
Online crime X IT security						-0.756
						(1.357)
_cons	10.674***	11.012***	11.836***	10.224***	10.425***	10.357***
	(0.874)	(0.805)	(0.787)	(0.906)	(1.013)	(1.022)
rho_12	0.829***	0.824***	0.834***	0.811***	0.811***	0.813***
	(0.035)	(0.037)	(0.034)	(0.041)	(0.045)	(0.042)
Wald $\chi 2$	3836.66	1627.78	1673.05	2983.51	1411.34	1434.78
Probability > $\chi 2$	0.000	0.000	0.000	0.000	0.000	0.000
No. of observations	396	396	396	379	379	379

The table reports the coefficient estimates using simultaneous equation models but only the equation of interest is reported. Robust standard errors in parentheses are clustered at the regional (county) level. The estimation includes all controls as in the baseline** $p<0.05$, *** $p<0.01$

Table 8 Cybersecurity breach and risk mitigation capabilities (estimating all interactions together) [Dependent variable: Log of labour productivity]

	Virus attack			Online crime		
	Full sample	SMEs	Large firms	Full Sample	SMEs	Large firms
	(1)	(2)	(3)	(4)	(5)	(6)
Virus attack	-3.146***	-2.669***	-5.339***			
	(0.311)	(0.363)	(1.107)			
Online crime				-2.963***	-2.705***	-2.122
				(0.241)	(0.350)	(1.568)
Upskilling	0.020	-0.161	1.449***	0.220	0.041	1.686***
	(0.127)	(0.190)	(0.505)	(0.165)	(0.259)	(0.501)
IT Policy	0.599***	0.466***	1.043	0.657**	0.530**	1.400***
	(0.170)	(0.134)	(0.763)	(0.258)	(0.256)	(0.458)
IT security	1.398***	1.407***	2.165**	1.638***	1.608***	3.221***
	(0.414)	(0.490)	(1.003)	(0.189)	(0.267)	(0.729)
Virus attack X Upskilling	0.592***	0.840***	-1.265			
	(0.195)	(0.237)	(0.703)			
Virus attack X IT Policy	-0.439	-0.361	-0.451			
	(0.353)	(0.332)	(0.606)			
Virus attack X IT security	0.047	-0.253	2.900**			
	(0.474)	(0.638)	(1.298)			
Online crime X Upskilling				0.500***	0.651***	-0.915
				(0.193)	(0.226)	(0.671)
Online crime X IT Policy				0.128	0.104	-0.014
				(0.378)	(0.433)	(0.857)
Online crime X IT security				-0.253	-0.394	-0.700
				(0.349)	(0.493)	(1.270)
_cons	13.065***	13.262***	11.266***	12.820***	12.988***	10.092***
	(0.517)	(0.472)	(0.761)	(0.409)	(0.342)	(1.085)
rho_12	0.681***	0.602***	0.836***	0.685***	0.636***	0.810***
	(0.048)	(0.083)	(0.031)	(0.031)	(0.043)	(0.045)
Wald $\chi 2$	5379.44	1231.42	6307.28	14,381.48	3315.90	3173.67
Probability > $\chi 2$	0.000	0.000	0.000	0.000	0.000	0.000
No. of observations	2308	1912	396	2208	1829	379

The table reports the coefficient estimates using simultaneous equation models but only the equation of interest is reported. Robust standard errors in parentheses are clustered at the regional (county) level. The estimation includes all controls as in the baseline

** $p<0.05$, *** $p<0.01$

6 Discussion and conclusion

In this study, we are interested in the effect of cybersecurity breach on labour productivity and how this effect is moderated by cyber risk mitigation capabilities at the firm level. We find that cybersecurity breach reduces labour productivity at the firm level. The evidence demonstrates that firms' exposure to cybersecurity breach or cyberattack is counterproductive. This finding is consistent with the growing body of literature on cybersecurity breach and firm performance (Kamiya et al., 2021; Makridis & Dean, 2018; Tripathi & Mukhopadhyay, 2020). This evidence shows the negative consequences of digital technologies which have received limited attention in the literature. The findings imply that without the appropriate measures, cybersecurity breach can erode the growth potential of firms through a reduction in labour productivity.

We find evidence that upskilling initiatives in firms significantly mitigate the effect of cyberattacks on labour productivity. This means that (re)training employees helps to improve performance in the changing and risky digital business environment. Our result agrees with Hasan et al.'s (2021) findings that IT infrastructure and skills improve firms' readiness for cybersecurity challenges. Such IT capabilities are reflected in the attraction of IT professionals and competence building to prepare firms for business operations and superior performance in the digital economy. Cybersecurity entails capabilities to manage passwords, use email and the Internet, as well as the ability to handle sensitive data and devices (Alqahtani, 2017), which require training to build employees' confidence in the use of IT resources, particularly with respect to cybersecurity (Siponen et al., 2014).

We show that while IT Policy and IT Security capabilities improve labour productivity, these measures are not sufficient to offset the negative effect of cybersecurity breach on labour productivity. Thus, our results do not support that technical IT security programmes, such as anti-malware software, intrusion detection and firewall solutions, significantly offset the effect of cyberattacks on labour productivity. While this does not mean that technical security capabilities are unimportant, it does point to the potential role of individual behaviour in the effectiveness of cybersecurity programmes, including the implementation of (non-technical) IT security policy which we have also found to have no significant mitigating effect on labour productivity loss. Alraja et al. (2023) point to the importance of employer behaviour in the effectiveness of IT security policy in firms. Employees are more likely to support a thorough implementation of IT security policy initiatives in firms when they are aware of the consequences of data misuse and attacks. Having technical and policy frameworks on cybersecurity in place can be ineffective if clear mechanisms, including sanctions and rewards, for not following through with guidelines are not enforced (D'Arcy et al., 2009; Siponen et al., 2014; Vance et al., 2013, 2020), as well as taking into account individual motivation and peer effect among employees (Li et al., 2019). Poor coordination between IT teams, on the one hand, and between IT teams and other authorised users, on the other hand, can contribute to ineffective cyber security policies (Alqahtani, 2017). We recognise that behavioural aspects can play a significant role in explaining the ineffectiveness of technical and policy support for IT security in firms.

The interactions between internal (firm) IT security policy and the external (region and/or country) regulatory environment matter. This resonates with the view that the extent to which the government supports businesses by entrenching and promoting deterrence, standard setting, detection, incident management and remediation contributes to the effectiveness of cybersecurity programmes in firms (Renaud et al., 2018). While Kenya has cybersecurity policies in place, poor coordination and the low level of public awareness mean that vulnerability to cybersecurity risks remains high (The Government of Kenya, 2022). IT security policies in firms are more likely to be ineffective if there is poor coordination of actors and weak enforcement of regulatory requirements targeted at entities that are expected to be custodians of data and related IT infrastructure.

Overall, our findings support upskilling as an effective cyber risk mitigation measure against cyberattacks at the firm level. This implies that firms should make training and retraining of employees an essential component of their overarching IT governance strategy.

Our study is not without limitations. While we highlight the moderating role of cyber risk mitigation capabilities of firms in the relationship between cybersecurity breach and labour productivity, we acknowledge that our risk mitigation capabilities are not exhaustive. For example, our study does not cover other firm-level capabilities such as managerial capability due to data limitations. However, future research may explore how other firm-level capabilities and practices, including individual and peer behaviour, can moderate the effect of cyberattacks on firm performance. This will require sourcing more data on variables that capture diverse firm-level capabilities and practices relevant to cybersecurity risk mitigation. We also see an opportunity for further research on the role of upskilling in the cybersecurity programmes of SMEs. This paper provides evidence that upskilling is a critical factor that helps SMEs offset the effect of cyberattacks on labour productivity in Kenya. This is unique in the sense that sophisticated digital skills in SMEs are often viewed as a constraining factor both as part of cybersecurity capabilities and as a driver of firm productivity. It holds promise for exploring further research questions around what drives SMEs to upskill and how this process is conducted, including how they channel meagre resources and organise for upskilling as part of cybersecurity programmes in an institutionally constrained environment.

Appendix

Table 9 Definition of variables used in the analysis

Variable	Definition
Labour productivity (in logs)	Turnover per worker in logs
Virus Attack	1 if the firm experienced an attack by a virus or similar
Online crime	1 if the firm experienced online crime
Upskilling	An index measuring upskilling at the firm level (scale of 0–1)
IT Policy	An index measuring IT policy at the firm level (scale of 0–1)
Digital infrastructure	An index measuring digital infrastructure at the firm level (scale of 0–1)
IT security	An index measuring IT security at the firm level (scale of 0–1)
Mobile commerce	An index measuring mobile commerce at the firm level (scale of 0–1)
Ecommerce	An index measuring Ecommerce at the firm level (scale of 0–1)
Digital Finance	An index measuring digital finance at the firm level (scale of 0–1)
SME	1 if the firms is a small and medium-sized enterprise
Regional level cyberattacks	Share of firms in region that experienced cybersecurity breach
Sector level cyberattacks	Share of firms in a sector that experienced cybersecurity breach

Table 10 Definition of variables used for the Principal Component Analysis

Variables	Definition
Mobile money	1 if the firm use mobile money platforms before the survey
Mobile banking	1 if the firm used mobile banking before the survey
Computer penetration	Proportion of employees who use computers
Internet penetration	Proportion of employees who use the Internet
Technical support for equipment repair and maintenance	1 if the firm received training for equipment repair and maintenance before the survey
Technical support for Internal system	1 if the firm received training in internal system of the government organization before the survey
Technical support for software development	1 if the firm received training in software development before the survey
Technical support for the development of web portals	1 if the firm received training in the development of web portals and other information services on the Internet before the survey
Technical support for electrical infrastructure or networks	1 if the firm received training in electrical infrastructure or networks before the survey
Risk detection	1 if the firm has Antivirus, Antispyware, Firewall, Spam filter, and Intrusion detection system in place
Authentication and safety	1 if the firm has authentication software or hardware, computer password and Secured communication system
Data backup	1 if the firm has a regular back of data
Place orders online	1 if the firm placed orders online
Receive orders online	I if the firm received orders online
Receive orders via mobile phones	I if the firm received orders via mobile phones
Place orders via mobile phones	I if the firm placed orders via mobile phones
IT Policy	1 if the firm has an IT policy in place
IT security policy	1 if the firm has an IT security policy in place
Aware of CIRT	1 if the firm is aware of the National Kenya Computer Incident Response Team

The year before the survey is 2015

Acknowledgements We are grateful to the Kenya National Bureau of Statistics (KNBS) for providing us with the dataset in the study. We would also like to thank the anonymous reviewers for their constructive comments.

Funding No funding to report.

Data availability The data used in this study was obtained from the Kenya National Bureau of Statistics (KNBS). Data request may be sent directly to the KNBS.

Code availability Code is available upon reasonable request.

Declarations

Conflicts of interest On behalf of the authors, the corresponding author indicates that there is no conflict of interest.

Ethics approval Not applicable.

Consent to participate Not applicable.

Consent for publication Not applicable.

References

Acemoglu, D., & Restrepo, P. (2020). Robots and jobs: Evidence from us labor markets. *Journal of Political Economy, 128*(6), 2188–2244. https://doi.org/10.1086/705716

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems, Milwaukee*. https://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Acs, Z. J., Song, A. K., Szerb, L., Audretsch, D. B., & Komlósi, É. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics, 57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors, 21*(20), 6901.

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science, 124*, 691–697. https://doi.org/10.1016/j.procs.2017.12.206

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers and Security*, *129(3)*. https://doi.org/10.1016/j.cose.2023.103208

Al-Saleh, M. I., AbuHjeela, F. M., & Al-Sharif, Z. A. (2015). Investigating the detection capabilities of antiviruses under concurrent attacks. *International Journal of Information Security, 14*(4), 387–396. https://doi.org/10.1007/s10207-014-0261-x

Angrist, J. D., Imbens, G. W., & Rubin, D. B. (1996). Identification of causal effects using instrumental variables. *Journal of the American Statistical Association, 91*(434), 444–455.

Apolinário, S., Yoshikuni, A. C., & Larieira, C. L. C. (2023). Resistance to information security due to users' information safety behaviors: Empirical research on the emerging markets. *Computers in Human Behavior, 145*, 107772. https://doi.org/10.1016/j.chb.2023.107772

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership and Control, 15*(2), 70–83. https://doi.org/10.22495/cocv15i2art6

Audrin, B., Audrin, C., & Salamin, X. (2024). Digital skills at work – Conceptual development and empirical validation of a measurement scale. *Technological Forecasting and Social Change, 202*, 123270. https://doi.org/10.1016/j.techfore.2024.123279

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly, 24*(1), 169–196.

Bloom, N., Draca, M., & Van Reenen, J. (2016). Trade induced technical change? The impact of chinese imports on innovation, IT and productivity. *Review of Economic Studies, 83*(1), 87–117. https://doi.org/10.1093/restud/rdv039

Bokhari, S. A. A., & Manzoor, S. (2022). Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. *American Journal of Industrial and Business Management, 12*(05), 934–954. https://doi.org/10.4236/ajibm.2022.125048

Bouwman, H., Nikou, S., Molina-Castillo, F. J., & de Reuver, M. (2018). The impact of digitalisation on business models. *Digital Policy, Regulation and Governance, 20*(2), 105–124. https://doi.org/10.1108/DPRG-07-2017-0039

Bradley, R. V., Byrd, T. A., Pridmore, J. L., Thrasher, E., Pratt, R. M. E., & Mbarika, V. W. A. (2012). An empirical examination of antecedents and consequences of IT governance in US hospitals. *Journal of Information Technology, 27*(2), 156–177. https://doi.org/10.1057/jit.2012.3

Brynjolfsson, E., & Hitt, L. M. (2000). Beyond computation: Information technology, organisational transformation and business performance. *Journal of Economic Perspectives, 14*(4), 23–48.

Cainelli, G., Evangelista, R., & Savona, M. (2006). Innovation and economic performance in services: A firm-level analysis. *Cambridge Journal of Economics, 30*(3), 435–458.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Castiglione, C., & Infante, D. (2014). ICTs and time-span in technical efficiency gains: A stochastic frontier approach over a panel of Italian manufacturing firms. *Economic Modelling, 41*, 55–65. https://doi.org/10.1016/j.econmod.2014.04.021

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems, 14*, 65–75. https://doi.org/10.17705/1cais.01403

Chang, H. (2013). Is ISMS for financial organisations effective on their business? *Mathematical and Computer Modelling, 58*(1–2), 79–84. https://doi.org/10.1016/j.mcm.2012.07.018

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers & Security, 19*(8), 698–709.

Finnemore, M., & Hollis, D. B. (2020). Beyond naming and shaming: Accusations and international law in cybersecurity. *European Journal of International Law, 31*(3), 969–1003. https://doi.org/10.1093/ejil/chaa056

Fu, X., Mohnen, P., & Zanello, G. (2018). Innovation and productivity in formal and informal firms in Ghana. *Technological Forecasting and Social Change, 131*, 315–325. https://doi.org/10.1016/j.techfore.2017.08.009

Gaglio, C., Kraemer-Mbula, E., & Lorenz, E. (2022). The effects of digital transformation on innovation and productivity: Firm-level evidence of South African manufacturing micro and small enterprises. *Technological Forecasting and Social Change, 182*, 121785. https://doi.org/10.1016/j.techfore.2022.121785

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Automatika, 58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. L. (2023). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management and Data Systems, 123*(3), 843–861. https://doi.org/10.1108/IMDS-05-2022-0313

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity, 1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security, 7*(2), 49–59. https://doi.org/10.4236/jis.2016.72004

Graham, M., & Mann, L. (2013). Imagining a Silicon Savannah? Technological and conceptual connectivity in Kenya's BPO and software development sectors. *Electronic Journal of Information Systems in Developing Countries., 27*(4), 595–608.

Greene, W. H. (1998). Gender economics courses in liberal arts colleges: Further results. *Journal of Economic Education, 29*(4), 291–300. https://doi.org/10.1080/00220489809595921

Grimes, A., Ren, C., & Stevens, P. (2012). The need for speed: Impacts of internet connectivity on firm productivity. *Journal of Productivity Analysis, 37*(2), 187–201. https://doi.org/10.1007/s11123-011-0237-z

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726 Contents. https://doi.org/10.1016/j.jisa.2020.102726

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). The devastating business impacts of a cyber breach. *Havard Business Review*. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Huang, K., Ye, R., & Madnick, S. E. (2019). *Both sides of the coin: The impact of cyber attacks on business value*. *Working Paper CISL# 2019–25*. MIT Sloan School of Management. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699756

Islam, A. M., & Muzi, S. (2022). Does mobile money enable women-owned businesses to invest? Firm-level evidence from Sub-Saharan Africa. *Small Business Economics, 59*(3), 1245–1271. https://doi.org/10.1007/s11187-021-00562-w

Islam, A., Muzi, S., Luis, J., & Meza, R. (2018). Does mobile money use increase firms ' investment ? Evidence from Enterprise Surveys in Kenya, Uganda, and Tanzania. *Small Business Economics, 51*, 687–708.

ITU. (2021). *Global cybersecurity index*. Geneva: ITU.

ITU/UNDP. (2023). *SDG digital acceleration agenda*. ITU/UNDP, Geneva/New York. https://www.undp.org/sites/g/files/zskgke326/files/2023-09/SDG%20Digital%20Acceleration%20Agenda.pdf

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kergroach, S. (2021). *SMEs going digital: Policy challenges and recommendations- Going digital toolkit note, No. 15*. OECD, Paris. https://doi.org/10.1787/c91088a4-en

Kher, R., Terjesen, S., & Liu, C. (2021). Blockchain, Bitcoin, and ICOs: A review and research agenda. *Small Business Economics, 56*(4), 1699–1720. https://doi.org/10.1007/s11187-019-00286-y

Kılıçaslan, Y., Sickles, R. C., AtayKayış, A., & ÜçdoğrukGürel, Y. (2017). Impact of ICT on the

productivity of the firm: Evidence from Turkish manufacturing. *Journal of Productivity Analysis, 47*(3), 277–289. https://doi.org/10.1007/s11123-017-0497-3

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lee, J., & Choi, S. J. (2021). Hospital productivity after data breaches: Difference-in-differences analysis. *Journal of Medical Internet Research, 23*(7), 1–8. https://doi.org/10.2196/26157

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(October 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems, 15*(1), 66–81. https://doi.org/10.1016/j.accinf.2013.02.001

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement, 43*, 59–83. https://doi.org/10.3233/JEM-180450

Masenyetse, R., & Manamathela, M. (2023). Firm growth, exporting and information communication technology (ICT) in Southern Africa. *Journal of Innovation and Entrepreneurship*, *12*(8). https://doi.org/10.1186/s13731-023-00273-4

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market price effects of data security breaches. *Information Security Journal, 20*(6), 263–273.

Motta, V. (2020). Lack of access to external finance and SME labor productivity: Does project quality matter? *Small Business Economics, 54*(1), 119–134.

Muzi, S., Jolevski, F., Ueda, K., & Viganola, D. (2023). Productivity and firm exit during the COVID-19 crisis: Cross country evidence. *Small Business Economics, 60*, 1719–1760.

Nambisan, S., Wright, M., & Feldman, M. (2019). The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Research Policy, 48*(8), 103773. https://doi.org/10.1016/j.respol.2019.03.018

National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC). (2023). Cybersecurity report: April to June 2023. Communications Authority of Kenya, Nairobi.

Ndubuisi, G., Otioma, C., & Tetteh, G. K. (2021). Digital infrastructure and employment in services: Evidence from Sub-Saharan African countries. *Telecommunications Policy, 45*(8), 102153. https://doi.org/10.1016/j.telpol.2021.102153

Pedota, M., Grilli, L., & Piscitello, L. (2023). Technology adoption and upskilling in the wake of Industry 4.0. *Technological Forecasting and Social Change, 187*, 122085. https://doi.org/10.1016/j.techfore.2022.122085

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity and Emergency Planning, 12*(3), 224–232.

Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business and Economics, 22*(12), 13–23.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilisation of the cyber security risk reasonable and judicious? *Computers and Security, 78*, 198–211. https://doi.org/10.1016/j.cose.2018.06.006

Roodman, D. (2011). Fitting fully observed recursive mixed-process models with cmp. *The Stata Journal, 11*(2), 159–206.

Schatz, D., Wall, J., Schatz, D., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Fornsics, Security and Law, 12*(2), 8.

Selznick, L. F., & Lamacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law, 13*(2), 217–253.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers and Security, 124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Sonnenreich, W., Albanese, J., & Stout, B. (2005). Return on security investment: A practical quantitative model. *Journal of Research and Practice in Information Technology, 38*(1), 239–252. https://doi.org/10.5220/0002580202390252

Sulaiman, N., Hamdan, A., & Al Sartawi, A. (2022). The influence of cybersecurity on the firms' financial performance. In A. Hamdan, A. Harraf, P. Arora, B. Alareeni, & R. K. Hamdan (Eds.), *Future of organisations and work after the 4th Industrial Revolution:The role of artificial Intelligence, big data, automation and robotics* , pp. 443–461. Springer,Cham. https://doi.org/10.1007/978-3-030-99000-8_25

Tchernykh, A., Schwiegelsohn, U., Talbi, E. Ghazali., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36*, 100581. https://doi.org/10.1016/j.jocs.2016.11.011

The Government of Kenya. (2022). *National Cybersecurity Strategy*. The Government of Kenya, Nairobi. https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBER SECURITY-STRATEGY-2022.pdf

Tripathi, M., & Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organizational Computing and Electronic Commerce, 30*(4), 381–400.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers and Security, 24*(2), 105–108. https://doi.org/10.1016/j.cose.2005.02.001

UNCTAD. (2022). Trade in services: A niche for export diversification in Africa. In *Economic Development in Africa Report 2022* (pp. 71–100). UNCTAD, Geneva. https://doi.org/10.18356/9789210018753c007

Van Grembergen, W. (2002). Introduction to the minitrack "IT governance and its mechanisms." *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://ieeexplore.ieee.org/document/994349/authors#authors

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Idea Group Publishing, Hershey. https://doi.org/10.4018/9781591401407.ch001

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263–290. https://doi.org/10.2753/MIS0742-1222290410

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralisation on information security policy violations across cultures. *Information and Management, 57*(4), 103212. https://doi.org/10.1016/j.im.2019.103212

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. *Proceedings - 3rd International Conference on Information Systems and Computer Science, INCISCOS 2018, Quito*, 294–300. https://doi.org/10.1109/INCISCOS.2018.00049

Vu, K., Hanafizadeh, P., & Bohlin, E. (2020). ICT as a driver of economic growth: A survey of the literature and directions for future research. *Telecommunications Policy, 44*(2), 101922. https://doi.org/10.1016/j.telpol.2020.101922

Wang, J., Ho, C. Y. (Chloe), & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis, 91*, 103028. https://doi.org/10.1016/j.irfa.2023.103028

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Zhen, J., Xie, Z., & Dong, K. (2021). Impact of IT governance mechanisms on organisational agility and the role of top management support and IT ambidexterity. *International Journal of Accounting Information Systems, 40*, 100501. https://doi.org/10.1016/j.accinf.2021.100501