1. Introduction

The 21st century global economy is shaped by rapid digitalisation. The adoption and integration of Information and Communication Technology (ICT) with the use of digital goods continues to grow exponentially and is expected to account for 25% of global GDP by 2030.[1] This growth is due to the proliferation of the digital economy, including sectors such as e-commerce, artificial intelligence, and digital banking. Reflecting this trend, the Australian government has plans to prioritise the digital economy to enhance productivity, drive economic growth and support various business sectors.[2]

However, cybersecurity is a significant barrier to further digitalisation, as businesses and consumers remain hesitant to fully embrace digital technology due to the fears of cyberattacks and data breaches.[3] Therefore, cybersecurity policy implemented by the government is crucial in supporting the digitalisation of an economy. This paper aims to examine the relationship between cybersecurity policy and digitalisation with the economic growth of a country.

2. Background of Research

2. 1 Shortage of Cybersecurity Measures in the Private Sector – Misalignment of Incentives

A key reason for insufficient cybersecurity measures in the private sector is the misalignment of incentives.[4] Businesses in the private sector are responsible for implementing cybersecurity measures, but they often do not face the direct consequences of security failures. Instead, it is the consumers that bear the immediate impacts, including identity theft and financial loss. Thus, when businesses face the trade-off between improving security measures and reducing operating costs, they are often more incentivised to reduce operating costs, leading to compromises in cybersecurity measures.[5]

---

[1] Boston Consulting Group, "Charting Economic Opportunities in the New Digital Paradigm," BCG Global, November 18, 2022, https://www.bcg.com/publications/2022/charting-opportunities-in-the-digital-economy-growth.

[2] Department of Home Affairs , "2023-2030 Australian Cyber Security Strategy," Australian Government, Department of Home Affairs, November 22, 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.

[3] Victoria State Government, "Digital Economy," Department of Jobs, Skills, Industry and Regions, 2021, https://djsir.vic.gov.au/priorities-and-initiatives/digital-economy.

[4] Tyler Moore, "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection* 3, no. 3-4 (December 2010): 103–17, https://doi.org/10.1016/j.ijcip.2010.10.002.

[5] Ibid.

While this decision is cost-effective in the short term, it is suboptimal for society in the long run.[6] It results in inadequate cybersecurity measures in the private sector, ultimately constraining digitalisation and limiting economic growth. Therefore, regulatory measures are essential to address the inadequate cybersecurity measures and keep up with businesses and consumers' increasing reliance on digital products.

2.2 Shortage of Cybersecurity Measures in the Private Sector – Information Asymmetry

Information asymmetry between the supplier and consumer of cybersecurity also contributes to the shortage of high-quality cybersecurity measures in the private sector. Suppliers of software or technology designed to protect against cyberattacks often have more knowledge about the product's effectiveness than potential consumers. This creates a 'lemon problem', where consumers cannot verify whether the more expensive option is actually better and more effective compared with the cheaper and less effective alternatives.[7] In effect, consumers may be reluctant to pay a higher price for the superior technology and choose the cheaper and less secure alternatives instead.[8] This can ultimately drive higher-quality technology out of the market, undermining the overall cybersecurity in the private sector.

2.3 Cybersecurity Policy in Australia

To address the shortage of cybersecurity measure, the Australian government implemented the 2023-2030 Cyber Security Strategy Plan. This strategy focuses on strengthening Australia's cyber defences to protect businesses and citizens. It ensures economic security for consumers and industries that adopt new technologies, further encouraging digitalisation to boost productivity and promote sustainable economic growth within the evolving digital economy.[9]

3. Research question and hypothesis

The research question that this research paper will explore is: 'How do stronger cybersecurity policies impact economic growth by enhancing confidence and safety in digital economies?'

---

[6] Ibid.

[7] Joseph J. Cordes, "An Overview of the Economics of Cybersecurity and Cybersecurity Policy" (The George Washington University Cyber Security Policy and Research Institute, June 1, 2011), 6.

[8] ibid

[9] Department of Home Affairs , "2023-2030 Australian Cyber Security Strategy," Australian Government, Department of Home Affairs, November 22, 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.

We hypothesise that countries who have stronger and more established cybersecurity policies are more likely to experience greater economic growth, as these policies enhance confidence and safety in digital transactions, thus fostering a secure and conducive environment for economic activity.

4. Literature Review

Researchers have explored the economic and policy implications of cybersecurity, with a growing focus on the integration of cybersecurity into broader economic framework, emphasising that companies tend to ignore security investments as they do not understand their full benefits.[10] Other research papers suggest that information asymmetry and lack of transparency in the cybersecurity market increase risks, as firms often conceal cybersecurity breaches to avoid repetitional damage.[11]

4.1 Supporting Theory

Reinsch and Caporal highlight that the digital economy generates significant spillover effects.[12] Positive spillovers are often undercounted but are critical for measuring the true impact of the digital economy. In their analysis they find that the overall contribution of ICT capital to the economy is 3.5 times greater than the private returns on investment.[13] This suggests that digital spillovers generate economic gains three times larger than currently measured, with the global digital economy, including these effects, being worth $11.5 trillion.[14]

Jin and Cho emphasise that ICT infrastructure is a fundamental component of economic growth in an information society.[15] They suggest that strong ICT investment, when coupled with robust cybersecurity policies, can enhance a country's economic resilience by supporting labour productivity and organisational efficiency.[16] The integration of these theories highlights

---

[10] Cordes, 1.
[11] Tyler Moore, "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection* 3 (2010): 108, https://doi.org/doi:10.1016/j.ijcip.2010.10.002.
[12] William Reinsch and Jack Caporal, "The Digital Economy & Data Governance," Key Trends in the Global Economy through 2030 (Center for Strategic and International Studies (CSIS), 2020), 19, JSTOR, http://www.jstor.org/stable/resrep26050.6.
[13] Reinsch and Caporal, 19.
[14] Reinsch and Caporal, 19.
[15] Sangki Jin and Cheong Moon Cho, "Is ICT a New Essential for National Economic Growth in an Information Society?," *Government Information Quarterly* 32, no. 3 (July 1, 2015): 1, https://doi.org/10.1016/j.giq.2015.04.007.
[16] Jin and Cho, 3.

that cybersecurity policies do more than just protect companies and individuals, as they also enable the safe, secure adoption of digital technologies that are vital for economic development.

4.2 Limitations in Current Research

While existing literature has established the relationship between digitalisation, cybersecurity, and economic growth, there remain significant gaps. Current studies tend to focus on theoretical models and overlook important variables such as the availability of infrastructure, income levels, and other technological factors. Additionally, the role of cybersecurity in supporting broader digitalisation efforts and its indirect effects on economic growth are often acknowledged but under examined in empirical research. The connection between cybersecurity, digitalisation, and economic growth requires more sophisticated models that can account for the intricate relationships between these variables.

This research aims to explore these gaps by examining the economic benefits of cybersecurity policy in a more detailed context, particularly focusing on its role in supporting digitalisation and its broader impact on economic performance.

5. Research Plan

This research paper explores the role of cybersecurity policy in promoting economic growth through improving digitalisation of the economy. It firstly examines the relationship between the digitalisation and economic growth in Australia, highlighting the direct impact of digitalisation on the economy. It will then explore how effective cybersecurity policies not only protect digitalisation but also further encourages it, ultimately contribute to economic growth by enabling a safer and more resilient digital economy.

6. Data Source

6.1 Time Series Data

Internet access is a key indicator of digitalisation in any country. Similarly, ICT access and usage by businesses directly reflects the level of digitalisation, as the adoption of ICT serves as the backbone of the digital economy by enabling companies to engage in e-commerce, digital finance and marketing. Therefore, these two factors, Internet access and ICT access and usage by businesses, are used as the measure me digitalisation of the Australian economy.

This research uses GDP level and labour productivity (GDP per hour) to evaluate economic and productivity growth in Australia. The relationship between Internet access and

ICT access and usage by businesses and GDP level and labour productivity are plotted to illustrate the impact of digitalisation on the Australian Economy. All data are sourced from the World Bank Database and the OECD database.[17][18]

6.2 Cross-sectional analysis

To explore the relationship between cybersecurity and digitalisation globally, the Global Cyber Security Index (GCI) is used as a measure of cybersecurity, while Mobile Cellular Subscription is chosen to represent the digitalisation of a country. Mobile Cellular Subscription is chosen as it reflects individuals' demand for digital technology, unlike supply-side factors such as internet penetration, which reflects more on government infrastructure decisions rather than individual demand. The data consists of 2022 cross-sectional data for all countries that are recognised by the World Bank.

7. Assumptions

7.1 Time Series Analysis

In each analysis, one digitalisation indicator is used as the dependent variable, and one economic growth indicator is used as the independent variable. While this simplification is not realistic as GDP growth or productivity growth is influenced by numerous different factors, this assumption is used in this case to simplify the analysis. The aim is to isolate and demonstrate the relationship between digitalisation indicators and economic growth indicators. This approach helps to highlight the specific contribution of digitalisation to economic growth and productivity.

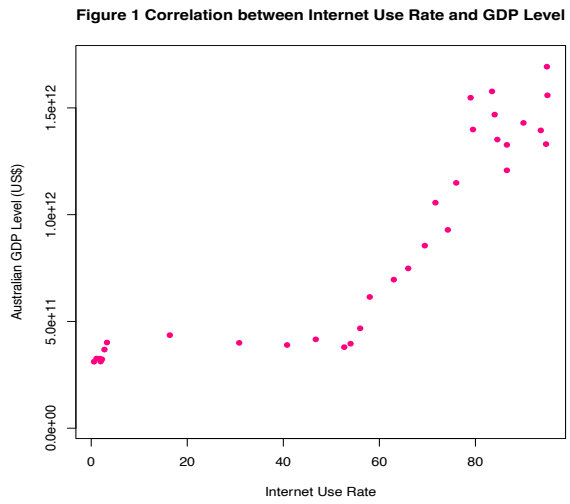
7.2 Cross-sectional Analysis

Similarly, only one cybersecurity policy indicator (GCI) and one digitalisation indication (Mobile Cellular Subscription) are chosen. Likewise, it is acknowledged that many factors contribute to digitalisation, but this approach isolates the impact of cybersecurity policy on digitalisation.

[17] World Bank, "DataBank," Worldbank.org, 2023, https://databank.worldbank.org/home.aspx.
[18] OECD, "Data," OECD, 2024, https://www.oecd.org/en/data.html.

8. Results

8.1 Australian Economic growth and Digitalisation



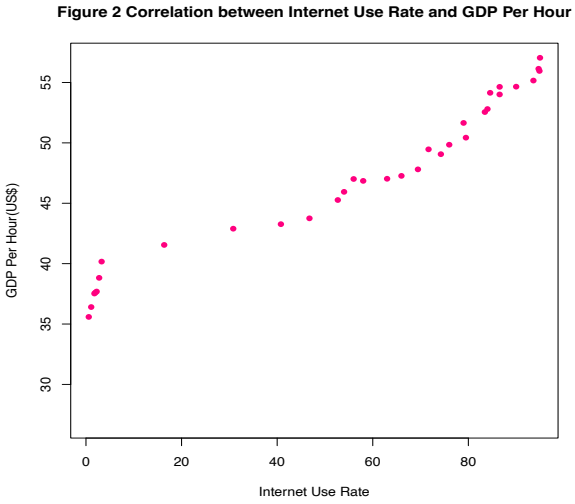
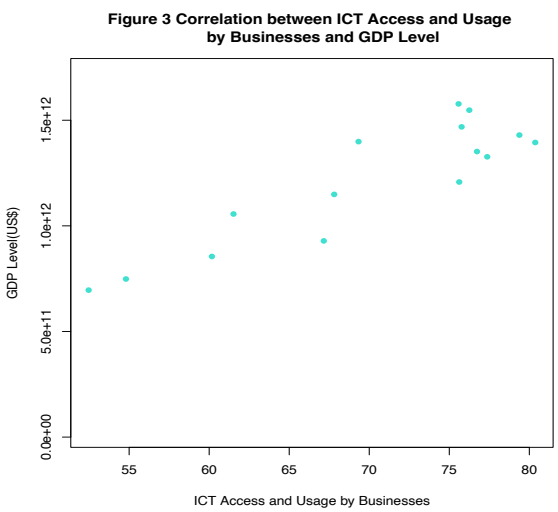
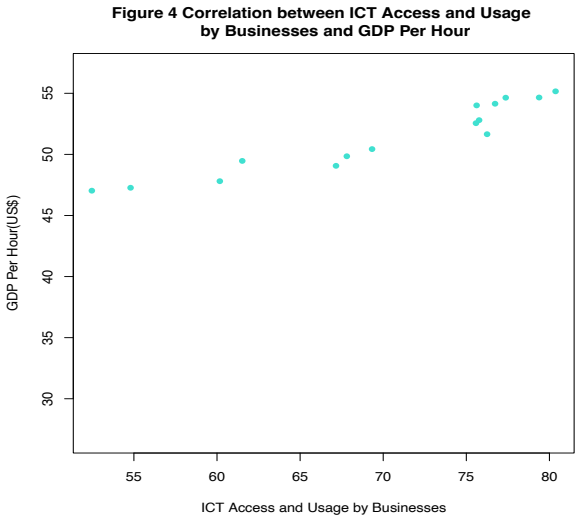


Figure 1 illustrates a strong positive correlation between Internet Use Rate and GDP level. This positive correlation becomes particularly pronounced after internet usage exceeds 60%, where data points are spread out more vertically. This suggests that the economic impact of higher internet penetration is exponential and once Australia adopts a sufficient digital infrastructure and internet access, the positive impact on GDP becomes significantly stronger.

Likewise, Figure 2 demonstrates a positive correlation between Internet Use Rate and labour productivity (GDP per hour). This suggests that as internet access (a key indicator of digitisation in a country) increases, the labour productivity of the economy increases.





Figures 3 and 4 both illustrate a positive correlation between ICT access and usage by businesses and both the GDP level and labour productivity of the Australian economy. These

findings support the notion that digitalisation is positively associated with both economic growth and productivity improvements in the Australian economy.

8.2 Cybersecurity on Digitalisation and Economic Growth

Table 1 Impact of Cybersecurity on Digitalisation

	Dependent variable:
	Mobile Cellular Subscriptions (per 100 people)
	Regression
Global Cybersecurity Index (GCI)	2.725***
	(0.659)
Constant	97.661***
	(5.328)
Observations	144
R^2	0.107
Adjusted R^2	0.101
Residual Std. Error	32.417 (df = 142)
F Statistic	17.079*** (df = 1; 142)
Note:	*p<0.1; **p<0.05; ***p<0.01

The regression results demonstrate a positive relationship between a country's cybersecurity and digitalisation, supporting the hypothesis. The data is significant at the 1% significance level. The R-squared value is 0.107, indicating that cybersecurity, measured by GCI, accounts for only 10.7 of digitalisation. Although this number is small, it reflects the reality as various factors contribute to digitalisation. This includes economic factors such as income level and affordability of technology, and technological factors such as availability of mobile networks and internet access.

Nevertheless, the positive and statistically significant relationship highlights the importance of cybersecurity in supporting digitalisation. By combining this result with the earlier analysis that demonstrates a positive relationship between digitalisation and GDP, it can be suggested that cybersecurity policy indirectly contributes to economic growth by supporting digitalisation.

8.3 Limitations

Table 3 Impact of Cybersecurity policy on

	Dependent variable:
	The Impact of Different Factors on GDP
	Regression
Global Cybersecurity Index (GCI)	10,769,891,393.000
	(106,242,900,476.000)
Human Development Index	1,076,142,625,599.000
	(3,551,815,345,185.000)
Foreign Direct Investment (current US)	27.683***
	(4.211)
Research and Development (%of GDP)	519,088,420,832.000**
	(252,394,158,110.000)
Population	12,778.830***
	(1,459.742)
Trade (% of GDP)	1,962,535,084.000
	(4,224,440,922.000)
Constant	-1,266,813,421,196.000
	(1,767,383,387,135.000)
Observations	70
R^2	0.752
Adjusted R^2	0.728
Residual Std. Error	1,949,838,501,069.000 (df = 63)
F Statistic	31.830*** (df = 6; 63)
Note:	*p<0.1; **p<0.05; ***p<0.01

It is worth mentioning that regression 3 in Table 3 is an attempt to model the relationship between cybersecurity policy (measured by GCI) and the GDP level of a country while controlling for other factors typically associated with GDP. However, neither cybersecurity policy nor some important factors, including human development (measured by HDI) and trade, have statistical significance. This is because this model is oversimplified and has omitted variable bias.

Likewise, these variables are correlated with each other as they are all key drivers of economic development. This correlation led to multicollinearity, which inflates the standard errors of the coefficients and makes it extremely difficult to capture and isolate the individual effect of this variable. For example, research and development (R&D) and foreign direct investment (FDI) can be correlated. Countries that have high R&D spending tend to have more innovation products and services, which likely attracts more FDI. Similarly, population and

trade can be correlated, as a larger population often need higher imports to meet domestic demand. Therefore, multicollinearity likely explains the insignificance of each factor.

Nevertheless, multicollinearity is often present in macroeconomics models, as many variables, including the ones in the models, are drivers of economic growth and often overlap in capturing similar aspects of economic growth. Recognising the problem of multicollinearity, we acknowledge that a much-sophisticated model is required to accurately examine the direct relationship between cybersecurity policy and the economic growth of a country. It needs to account for the complex interactions between each variable and include additional factors that have been omitted.

9. Future implications

Looking forward, the integration of cybersecurity policies with digital infrastructure development will be critical to harnessing the full potential of the digital economy. As countries continue to adopt new technological innovations, the indirect spillover effects on sectors such as finance, healthcare, and manufacturing will become even more pronounced. Without sufficient cybersecurity infrastructure, these industries could face heightened risks of data breaches, cyber-attacks, and loss of consumer trust, which could stifle growth and limit the economy's broader spillover benefits. Therefore, robust cybersecurity measures will be critical for maintaining trust and ensuring that the positive externalities of digital investments are fully realised.

Additionally, as the global digital economy, including spillover effects, is estimated to be worth $11.5 trillion, cybersecurity policies will play a pivotal role in safeguarding this immense economic value. Governments and companies must work together to foster innovation while ensuring that security standards keep pace with technological advancements. Doing so will not only protect private returns but will also maximise the broader societal benefits. Ultimately, future growth in the digital economy will rely on the ability to secure data and networks, allowing for continued innovation and diffusion of technology. Failing to prioritise cybersecurity could undermine these potential gains.

10. Conclusion

In conclusion, this paper has explored the critical relationship between cybersecurity policy, digitalisation, and economic growth. The positive correlation between cybersecurity, digitalisation, and economic growth highlights the role that effective policy plays in not only protecting the digital economy but also enabling its continued expansion. However, it is

important to acknowledge that more work needs to be done to examine the actual causal effect of cybersecurity policy. The effects of cybersecurity policy thus have to be disentangled from other factors of economic growth. In doing so, the government will be able to decide the correct subsidy amount and create possible positive externalities.

In a world where digital infrastructure underpins much of global economic activity, cybersecurity will continue to be a key driver of economic resilience and growth in the decades to come.

11. Bibliography

Boston Consulting Group. “Charting Economic Opportunities in the New Digital Paradigm.” BCG Global, November 18, 2022. https://www.bcg.com/publications/2022/charting-opportunities-in-the-digital-economy-growth.

Cordes, Joseph J. “An Overview of the Economics of Cybersecurity and Cybersecurity Policy.” The George Washington University Cyber Security Policy and Research Institute, June 1, 2011

Department of Home Affairs . “2023-2030 Australian Cyber Security Strategy.” Australian Government, Department of Home Affairs, November 22, 2023. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.

Jin, Sangki, and Cheong Moon Cho. “Is ICT a New Essential for National Economic Growth in an Information Society?” *Government Information Quarterly* 32, no. 3 (July 2015): 253–60. https://doi.org/10.1016/j.giq.2015.04.007.

Moore, Tyler. “The Economics of Cybersecurity: Principles and Policy Options.” *International Journal of Critical Infrastructure Protection* 3, no. 3-4 (December 2010): 103–17. https://doi.org/10.1016/j.ijcip.2010.10.002.

OECD. “Data.” OECD, 2024. https://www.oecd.org/en/data.html.

Reinsch, William, and Jack Caporal. “The Digital Economy & Data Governance.” Key Trends in the Global Economy through 2030. Center for Strategic and International Studies (CSIS), 2020. JSTOR. http://www.jstor.org/stable/resrep26050.6.

Victoria State Government. “Digital Economy.” Department of Jobs, Skills, Industry and Regions, 2021. https://djsir.vic.gov.au/priorities-and-initiatives/digital-economy.

World Bank. “DataBank.” Worldbank.org, 2023. https://databank.worldbank.org/home.aspx.