

The Capacity Needs Analysis On Digital Rights and Cybersecurity



Funded by
the European Union



THE REPUBLIC OF UGANDA
MINISTRY OF GENDER,
LABOUR & SOCIAL DEVELOPMENT



Enabel 



REPORT FOR THE CAPACITY NEEDS ANALYSIS (CNA) ON DIGITAL RIGHTS & CYBERSECURITY FOR PSFU MEMBERS

CONDUCTED BY PRIVATE SECTOR FOUNDATION UGANDA (PSFU)

With Support From

**COLLABORATION ON INTERNATIONAL ICT POLICY FOR
EAST AND SOUTHERN AFRICA (CIPESA)**



Table of Contents

List of Figures	4	3.0 Conceptual and Policy Context	14
List of Tables	4	3.1 The overview of the Strengthening the SMEs on digital rights and cybersecurity resilience in Central Uganda	14
List of Acronyms	5	3.2 Strengthening SMEs on digital and cybersecurity resilience in central Uganda and related policies	15
Acknowledgement	6	3.3 policy and Legal Environment for digital Rights and Cybersecurity Resilience	15
Foreword	7		
Message from Director Policy Advocacy and Business Development	8		
1.0 Executive Summary	9	4.0 Methodology	18
2.0 Introduction	10	4.1 Description of data collection methods (surveys, interviews).	18
2.1 Background on digital rights and cybersecurity in Uganda	10	4.2 Analytical approaches (quantitative and qualitative).	19
2.2 The purpose of the study	10	4.3 Stakeholder engagement and validation process.	19
2.3 Overview of the ARBHR project and PSFU's role	11		
2.4 Importance of digital rights and cybersecurity for businesses.	11	5.0 Key Findings	20
2.5 Challenges faced by Ugandan businesses in promoting digital rights.	12	5.1 Digital Communication and Online Presence	20
2.6 Objectives of the CNA.	12	5.2. Data Storage and Management Practices	22
2.7 Scope of the study	12	5.3 Cybersecurity Awareness and Implementation	23
2.8 Critical Success Factors	13	5.4. Policy, Legal and Regulatory Awareness	25
2.9 Structure of the Report	13	5.5 Budgeting and Strategic Planning	26
		5. 6 Challenges and Support Needs	27
		7.0 Recommendations	29
		8.0 Conclusion	30
		9.0 References	31

List of Figures

Figure 1: Social Media Usage	20
Figure 2: Email Usage	21
Figure 3: Website Ownership	22
Figure 4: Cloud Storage	22
Figure 5: Customer Data Collection	23
Figure 6: Awareness of Cybersecurity Threats	23
Figure 7: Cybersecurity Policies	24
Figure 8: Regular Updates	25
Figure 9: Staff Training	26
Figure 10: Cybersecurity Incidents	27
Figure 11: Awareness of Uganda’s Data Protection and Privacy Act (2019)	28
Figure 12: Budget for Digital Tools and Cybersecurity	29
Figure 13: Willingness to Partner for Digital Resilience	30
Figure 14: Challenges Faced	31
Figure 15: Support Needs	32

List of Tables

Table 1: Respondent Disaggregation by District, Gender, and Sector	18
--	----

List of Acronyms

CNA	Capacity Needs Analysis
PSFU	Private Sector Foundation Uganda
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
ARBHR	Advancing Respect for Human Rights by Business in Uganda
SME(s)	Small and Medium-sized Enterprise(s)
ICT	Information and Communication Technology
CSO(s)	Civil Society Organization(s)
NITA-U	National Information Technology Authority - Uganda
UCC	Uganda Communications Commission
GDPR	General Data Protection Regulation
PDPO	Personal Data Protection Office
CSIRT(s)	Computer Security Incident Response Team(s)
ANCA	African Network of Cybersecurity Authorities
EAC	East African Community
AI	Artificial Intelligence
UGX	Uganda Shillings

Acknowledgement

The Private Sector Foundation Uganda (PSFU) extends its sincere appreciation to all individuals and institutions that contributed to the successful completion of this Capacity Needs Analysis (CNA) on Digital Rights and Cybersecurity for PSFU Members.

We are deeply grateful to the Collaboration on International ICT Policy for East and Southern Africa (CIPEA) for the financial and technical support provided under the Advancing Respect for Human Rights by Business (ARBHR) project. Their partnership has been instrumental in advancing digital rights awareness and strengthening cybersecurity resilience within Uganda's private sector.

Special appreciation goes to the 79 businesses from Kampala, Wakiso, and Mukono districts that participated in the surveys and interviews. Their openness, time, and willingness to share practical experiences provided the empirical foundation for this report. We particularly acknowledge the 24 stakeholders—representing agriculture, manufacturing, ICT, trade, construction, creative industries, and human resource sectors—who actively participated in the validation workshop held at the PSFU Board Room. Their insights, critiques, and recommendations enriched the analysis and ensured that the findings reflect the real challenges and priorities of SMEs in Central Uganda.

We also recognize the invaluable contributions of the consultant who led the data collection, analysis, and drafting process, as well as the PSFU technical team for their coordination, stakeholder engagement, and quality assurance support throughout the study.

Our appreciation further extends to key government and regulatory institutions, including the Ministry of ICT and National Guidance, NITA-U, the Personal Data Protection Office (PDPO), and the Uganda Communications Commission (UCC), whose policy frameworks and ongoing initiatives provided important context for this assessment.

Finally, we thank all development partners, civil society actors, and private-sector stakeholders committed to promoting responsible digital practices. It is through collective action and collaboration that Uganda will build a secure, inclusive, and resilient digital economy.

Foreword



On behalf of the Private Sector Foundation Uganda (PSFU), I am pleased to present this Capacity Needs Analysis (CNA) on Digital Rights and Cybersecurity for PSFU members. This report comes at a defining moment for Uganda's private sector, as digital transformation accelerates across all sectors while cyber risks, regulatory obligations, and data governance challenges continue to grow in scale and complexity.

The findings of this CNA are both encouraging and sobering. On one hand, Ugandan enterprises particularly small and medium-sized businesses are increasingly embracing digital tools to drive visibility, efficiency, and growth. The evidence that 71% of surveyed businesses own websites, 59% use cloud storage and 72% collect customer data signals a private sector that is actively participating in the digital economy. On the other hand, the analysis clearly shows that digital adoption is outpacing digital protection. While 81% of businesses are aware of cybersecurity threats, only 16% have cybersecurity policies, 23% train their staff, and just 28% allocate budgets for digital tools and cybersecurity. Even more concerning is that only 38% are aware of the Data Protection and Privacy Act (2019), exposing enterprises to legal, financial, and reputational risks.

These gaps are not merely technical; they are strategic and policy related. In an economy where cybercrime has cost billions of shillings and where trust is central to digital trade, weak cybersecurity and poor data governance undermine competitiveness, investor confidence, and consumer protection. This CNA therefore provides timely, evidence-based insights to guide action by government, development partners, regulators, the private sector and civil society.

PSFU's participation in the Advancing Respect for Human Rights by Business in Uganda (ARBHR) initiative, implemented with support from Collaboration on International ICT Policy for East and Southern Africa, reflects our firm belief that responsible business conduct today must include respect for digital rights, privacy, and security. Digital resilience is no longer optional; it is a prerequisite for sustainable enterprise growth and national economic transformation.

We are particularly encouraged that 82% of businesses expressed willingness to partner to strengthen digital resilience. This strong signal calls for decisive public-private collaboration—through policy reforms, targeted incentives, capacity building, and investment in affordable cybersecurity solutions. Government action to simplify compliance, expand awareness, and support SMEs, alongside partner support for skills development and infrastructure, will be critical. This report is therefore a call to action. PSFU commits to using these findings to deepen advocacy, strengthen member capacity, and work closely with government and partners to build a secure, inclusive, and competitive digital economy. Together, we can ensure that Uganda's digital future is not only innovative—but trusted, rights-respecting, and resilient.

A stylized, handwritten signature in white ink.

Stephen Asimwe

Chief Executive Officer

Message from Director Policy Advocacy and Business Development



The Private Sector Foundation Uganda (PSFU), in partnership with CIPESA under the Advancing Respect for Human Rights by Business (ARBHR) project, is pleased to present the Capacity Needs Analysis (CNA) on Digital Rights and Cybersecurity for PSFU members. This report provides an evidence-based assessment of 79 businesses across Central Uganda and offers clear direction for strengthening digital resilience within our private sector. The findings are both encouraging and sobering.

On the positive side, 71% of businesses own websites, 59% use cloud storage, and 81% are aware of cybersecurity threats. Additionally, 82% have expressed willingness to partner in building digital resilience. These figures demonstrate a private sector that is increasingly conscious of the digital shift and ready to collaborate.

However, critical gaps remain. Only 29% of businesses use email for formal communication. Just 23% conduct staff cybersecurity training. Only 16% have formal cybersecurity policies in place, and a mere 28% allocate a dedicated budget for digital tools and cybersecurity. Most concerning, only 38% are aware of the Data Protection and Privacy Act (2019), despite 72% collecting customer data. Furthermore, while 13% reported cybersecurity incidents, national data shows cybercrime losses running into billions of shillings annually highlighting likely underreporting and weak incident response systems.

These findings point to an urgent policy and institutional imperative. Digital transformation without digital trust is unsustainable. Uganda's Digital Transformation Roadmap (2023–2028) sets ambitious targets, including connecting 90% of SMEs to the internet and digitizing 95% of government services. Yet, without adequate cybersecurity investment, legal compliance, and skills development, these gains risk being undermined. As PSFU, we call for coordinated action. Government must strengthen awareness campaigns on digital rights and data protection, expand SME-focused cybersecurity training, and incentivize investment in secure digital infrastructure. Development partners should support scalable capacity-building initiatives and innovation hubs. The private sector must prioritize digital governance, budget for cybersecurity, and embed data protection into core business strategy.

Digital resilience is no longer optional, it is a security competitiveness issue, a trust issue and a national development issue. By working together, we can build a secure, inclusive, and globally competitive digital economy that protects businesses, safeguards citizens' rights, and accelerates Uganda's ten-fold economic growth strategy.

A handwritten signature in blue ink, appearing to read 'Julius Byaruhanga', with a stylized flourish at the end.

Dr. Julius Byaruhanga

Director, Policy Advocacy and Business Development

1.0 Executive Summary

The Capacity Needs Analysis (CNA) assessed 79 businesses under the Private Sector Foundation Uganda (PSFU) to determine their readiness in digital rights, data protection, and cybersecurity. Conducted among Small and Medium-sized Enterprise (SMEs) in Central Uganda across sectors such as agriculture, manufacturing, Information and Communication Technology (ICT), and trade, the study sought to identify gaps in digital awareness, infrastructure, and compliance with national frameworks—particularly Uganda’s Digital Transformation Roadmap (2023–2028).

Digital communication adoption varies widely: 56% of businesses use social media for engagement, only 29% rely on email for formal communication, while 71% own websites for visibility and branding. These variations indicate a stronger focus on online presence than on structured communication systems, reflecting uneven digital maturity across fields.

Data management practices show progress but raise compliance risks. While 59% use cloud storage and 72% collect customer data, only 38% are aware of the Uganda Data Protection and Privacy Act (2019). This exposes businesses to legal and reputational vulnerabilities, underscoring the need for targeted awareness and governance training.

Cybersecurity awareness is relatively high (81%), yet implementation remains weak. Only 16% have cybersecurity policies and 23% conduct staff training, resulting in exposure to phishing, ransomware, and social engineering attacks. Moreover, only 28% allocate budgets for digital tools and cybersecurity, limiting investment in secure infrastructure.

Incident reporting is low (13%), with data breaches (25 businesses) and malware attacks (19 businesses) being the most common issues among those affected. Weak detection and reporting systems remain a key concern.

Encouragingly, 82% of businesses expressed willingness to collaborate on digital resilience, opening opportunities for public–private partnerships to strengthen capacity and accelerate digital transformation.

Support needs identified included data protection (32%), staff training (26%), secure communication tools (16%), and policy development (16%). These directly align with the Digital Transformation Roadmap’s goals of achieving 90% SME internet connectivity and 95% digitization of government services. These priorities highlight the need for improved data governance, stronger cybersecurity structures, enhanced skills, and better-aligned digital policies.

Overall, the findings demonstrate the urgent need for coordinated investments in digital literacy, regulatory compliance, and cybersecurity infrastructure. Strengthening these areas will enhance business competitiveness, protect citizens’ digital rights, and advance Uganda’s transition toward a secure, inclusive, and resilient digital economy.

2.0 Introduction

2.1 Background on digital rights and cybersecurity in Uganda.

Uganda's digital rights framework is anchored in constitutional and statutory provisions. Article 27 of the Constitution guarantees the right to privacy, further reinforced by the Data Protection and Privacy Act (2019) and its Regulations (2021). These laws regulate personal data handling by both local and foreign entities. Additional legislation includes the Computer Misuse Act (2011, amended 2022), which addresses cyberbullying and unauthorized access, and the Regulation of Interception of Communications Act (2010, updated 2023), which permits lawful surveillance under judicial oversight. Despite these laws, enforcement remains inconsistent, especially regarding digital labor rights and online freedoms.

Cybersecurity threats in Uganda are rising. In 2023, the Uganda Police Cyber Unit reported a 37% increase in cybercrime incidents, with financial institutions and SMEs being the most affected. Common threats include phishing, mobile money fraud, and AI-driven impersonation scams. The National Cybersecurity Strategy, developed by NITA-U and the Ministry of ICT, outlines goals such as infrastructure protection and public awareness. However, implementation is hindered by limited technical capacity and fragmented coordination among agencies.

Digital access continues to expand. As of 2025, internet penetration stands at 28.0%, representing 14.2 million users, while mobile connections total 38.6 million, covering 76.2% of the population. Social media users' number 2.4 million. Cybercrime cost the economy UGX 19.2 billion in 2022, though this dropped to UGX 1.5 billion in 2023 due to improved detection and response.

Key stakeholders include the government, civil society, and international partners. The Ministry of ICT and NITA-U lead awareness campaigns and legal reforms. Civil society groups like CIPESA and Initiative for Social and Economic Rights (ISER) promote digital inclusion and rights advocacy. International bodies such as the World Bank and the International Criminal Police Organisation (INTERPOL) support Uganda through funding and policy guidance.

Current debates focus on surveillance versus privacy, digital labor protections, and internet shutdowns during elections. Recent publications highlight the need for inclusive digital public infrastructure and stronger safeguards for vulnerable groups, especially considering the 2023 Anti-Homosexuality Act, which triggered increased online harassment.

2.2 The purpose of the study

The purpose of this study was to comprehensively investigate and address the pressing need for strengthening PSFU members on digital rights and cybersecurity resilience. By conducting an in-depth assessment of current awareness and understanding of digital rights and cybersecurity among the PSFU Members, this study aims to identify the existing gaps and challenges that hinder their ability to protect their digital assets and mitigate cyber threats. Through this research, targeted interventions will be developed to enhance SMEs' digital rights and cybersecurity posture, ultimately fostering a safer and more secure digital environment that promotes economic growth, innovation and competitiveness in the region. By achieving this purpose, the study seeks to contribute to the development of a robust and resilient digital economy in Uganda, where SMEs can thrive and drive sustainable economic development.

2.3 Overview of the ARBHR project and PSFU's role

The Advancing Respect for Human Rights by Business in Uganda (ARBHR) project is a multi-stakeholder initiative implemented by CIPESA, with support from Enabel and the European Union. Its core objective is to reduce human rights abuses linked to business activities, particularly those affecting vulnerable groups such as women and children. In the digital era, the project emphasizes the importance of safeguarding digital rights- including privacy, freedom of expression, and cybersecurity -as essential components of responsible business conduct.

Digital transformation in Uganda has exposed businesses to new risks and responsibilities. Many enterprises, especially SMEs, lack the capacity to protect digital rights due to limited awareness, inadequate infrastructure, and weak policy frameworks. The ARBHR project addresses these gaps by supporting civil society organizations (CSOs) and business associations to promote digital rights advocacy and resilience.

The Private Sector Foundation Uganda (PSFU) was selected as a key Business Member Organisation for partnership under the ARBHR project. As part of PSFU's initiatives, is conducting a Capacity Needs Analysis (CNA) focused on digital rights and cybersecurity among its member organizations in Central Uganda. This initiative aims to identify knowledge gaps, skill deficiencies, and institutional challenges that hinder digital safety and rights protection.

To achieve this, PSFU is engaging a consultant to analyze field data, validate findings through stakeholder workshops, and produce a comprehensive CNA report. The report will guide future programming, advocacy, and training interventions.

Ultimately, PSFU's involvement in ARBHR strengthens its leadership in promoting responsible digital practices, enhancing cybersecurity resilience, and shaping inclusive digital policy frameworks for Uganda's private sector.

2.4 Importance of digital rights and cybersecurity for businesses.

In Uganda's expanding digital economy, digital rights and cybersecurity are vital for business sustainability, trust, and competitiveness. As of 2024, Uganda had 13.3 million internet users, with mobile penetration reaching 76.2% of the population (Milima Cyber Academy, 2024). This digital growth has enabled businesses to adopt e-commerce, mobile banking, and cloud services, but it has also exposed them to increasing cyber threats.

Cybercrime poses a significant financial and reputational risk. In 2022, Uganda lost UGX 19.2 billion to cyberattacks across 245 reported cases, with SMEs and financial institutions being the most affected (Milima Cyber Academy, 2024). Common threats include phishing, ransomware, and social engineering. A single data breach can erode customer trust, disrupt operations, and lead to legal consequences under Uganda's Data Protection and Privacy Act (2019).

Businesses must prioritize cybersecurity as a strategic investment. This includes adopting firewalls, multi-factor authentication, and staff training on digital hygiene. Cybersecurity insurance is also emerging as a safety net, offering financial protection in case of breaches (Milima Cyber Academy, 2024).

Government and private sector actors are responding. The National Cybersecurity Strategy (2022–2026) emphasizes protecting critical infrastructure, building cyber skills, and supporting MSMEs with guidelines and resources (Digital Watch Observatory, 2023). Companies like Milima Security offer vulnerability assessments and cybersecurity maturity programs to help businesses stay ahead of evolving threats.

2.5 Challenges faced by Ugandan businesses in promoting digital rights.

Ugandan businesses face a range of challenges in promoting digital rights, many of which stem from infrastructural, economic, and regulatory limitations. One of the most pressing issues is the digital divide. Only 9% of Ugandans in rural areas have access to the internet, compared to significantly higher rates in urban centres, creating a 70% disparity in digital access (Abaho et al., 2025). This gap limits rural businesses' ability to engage in digital rights advocacy or adopt secure digital practices.

In urban areas, 60% of the population live in slums, where digital literacy is low and infrastructure is inadequate (Abaho et al., 2025). Many SMEs lack the technical expertise and financial resources to implement data protection measures, leaving them vulnerable to breaches and non-compliance with Uganda's Data Protection and Privacy Act (2019). This challenge is compounded by limited access to cybersecurity professionals and affordable digital tools.

Regulatory uncertainty also hinders progress. Businesses must navigate evolving laws such as the Computer Misuse Act (2022) and new licensing frameworks introduced by the Uganda Communications Commission. These frameworks, while intended to improve governance, have raised concerns about overregulation and operational restrictions (Paradigm Initiative, 2023).

Cultural and educational barriers persist. Many business owners, especially in underserved communities, lack awareness of digital rights and perceive cybersecurity as a luxury. Bridging these gaps requires targeted training, inclusive policy design, and multi-stakeholder collaboration to ensure businesses can uphold digital rights while remaining competitive in Uganda's growing digital economy.

2.6 Objectives of the CNA

The objective of the Capacity Needs Analysis was to conduct a comprehensive assessment so as to identify the knowledge gaps, skill deficiencies, resource constraints, and policy/practice needs of PSFU members concerning digital rights and cybersecurity.

2.7 Scope of the study

This study focuses on small and medium-sized enterprises (SMEs) operating in central Uganda, covering various sectors like agriculture, manufacturing, ICT, Construction and many others. The study assessed the awareness and understanding of digital rights and cybersecurity among SMEs, examining current practices, challenges, threats and availabilities as well as existing policies and regulations. The research targeted SMEs' owners, managers, employees as well as relevant stakeholders that include policy makers, industry associations and cybersecurity experts. Geographically, the study focused on urban and peri-urban areas in Central Uganda. By exploring these aspects, the study aims to provide comprehensive understanding of digital rights and cybersecurity landscape for SMEs in the region, informing strategies to strengthen their resilience and promote a safer digital environment.

2.8 Critical Success Factors

The successful implementation of initiatives aimed at strengthening SMEs' digital rights awareness and cybersecurity resilience in Central Uganda depended on several critical success factors that include;

- i. Awareness and Knowledge for adequate understanding of digital rights and cybersecurity risks among SME owners and staff.
- ii. Policies and Procedures for establishment and enforcement of clear digital security policies and operational guidelines.
- iii. Top Management Commitment for a strong leadership support in prioritizing and investing in cybersecurity measures.
- iv. Capacity Building through regular training programs to enhance digital literacy and cybersecurity skills.
- v. Collaboration and Partnerships by having engagements with key stakeholders, including government agencies, private sector actors and development partners.
- vi. Access to Resources including the availability of financial support, tools, and technical expertise to implement cybersecurity solutions.
- vii. Continuous Risk Assessment through the ongoing identification, monitoring and testing of vulnerabilities.
- viii. Incident Response Planning by developing effective mechanisms to detect, respond to, and recover from cyber incidents.

2.9 Structure of the Report

This report follows a structured format, and it began with executive summary providing an overview of key findings and recommendations. The introduction covered the background, objectives and the scope of the report, highlighting the importance of digital rights and cybersecurity for SMEs in Central Uganda.

A literature overview provides an overview of existing research on digital rights and cybersecurity in SMEs, focusing on Uganda especially the Central region. The methodology section outlined the research methods used which included the surveys, interviews and case studies. The findings and the analysis section presents the research results, identifying the current state of digital rights and cybersecurity among the SMEs. The report also highlights challenges and gaps faced by SMEs and provided actionable recommendations for SMEs, policy makers and stakeholders. Finally, the conclusion summarised key takeaways and the report concluded with references and appendices with supporting materials.

By focusing on these key areas, SMEs can enhance their digital resilience, protect their digital assets and promote a safer and more secure digital environment that supports business growth and economic development.

2.9.1 Rationale for conducting the CNA.

The rationale for conducting the CNA stems from the urgent need to strengthen digital rights awareness and cybersecurity resilience among Ugandan businesses. As of 2025, Uganda has over 14.2 million internet users, with mobile penetration at 76.2% (Milima Cyber Academy, 2024). This digital expansion has exposed businesses to increased risks of data breaches, online fraud, and regulatory non-compliance, especially among SMEs that lack adequate digital safeguards.

Despite the existence of the Data Protection and Privacy Act (2019) and the Computer Misuse Act (2022), many businesses remain unaware of their obligations and the implications of digital rights violations. A recent study found that over 60% of SMEs in Uganda do not have internal data protection policies or trained cybersecurity personnel (Abaho et al., 2025). This gap highlights the need for targeted interventions to build institutional capacity and promote responsible digital practices.

The CNA aims to identify specific knowledge gaps, skill deficiencies, and resource constraints among PSFU member organizations. By analyzing field data and stakeholder feedback, the CNA will generate actionable recommendations to guide training, advocacy, and policy development. This evidence-based approach ensures that future programming is aligned with actual needs and challenges.

Moreover, the CNA supports Uganda's broader digital transformation agenda by fostering inclusive and secure digital ecosystems. It aligns with the objectives of the ARBHR project, which seeks to reduce human rights abuses linked to business activities. Through this analysis, PSFU can play a pivotal role in shaping a private sector that respects digital rights and is resilient against cyber threats.

3.0 Conceptual and Policy Context

3.1 The overview of the Strengthening the SMEs on digital rights and cybersecurity resilience in Central Uganda.

SMEs are the small and medium sized enterprises that have a limited number of employees and revenues. The rapid growth of Uganda's digital economy has increased the vulnerability of Small and Medium-sized Enterprises (SMEs) to cyber threats. Consequently, the government and private sector have launched initiatives to strengthen cybersecurity and promote digital resilience. One such initiative is the Cybersecurity Awareness Month, now in its sixth edition, which aims to boost cyber resilience and encourage public-private collaboration against digital threats.

Uganda has made progress in strengthening its cybersecurity framework through the National Cybersecurity Strategy and the Data Protection and Privacy Act. However, the country still faces significant challenges, including limited awareness and understanding of digital rights and cybersecurity threats, insufficient skills and resources to adopt safe online practices and vulnerability to cyber threats. SMEs are particularly vulnerable, with 40% experiencing cyberattacks and less than 1% having cyber insurance.

Cyber threats can have devastating consequences for SMEs, including financial loss, reputational damage and operational disruptions. The Uganda Police's Annual Cyber Crime Report shows that the country lost UGX 72.1 billion to fraud and cyber incidents in 2024, with digital fraud accounting for 31.9% of all reported cases. SMEs must prioritize cybersecurity to protect themselves from these threats and ensure sustainable growth.

To address the growing threat of cybercrime, the government and private sector are working together to promote cybersecurity awareness, education and capacity building. Initiatives include the Cybersecurity Awareness Month, which features regionally hosted events and weekly themes such as AI risks, digital fraud and cybersecurity training. Additionally, companies like Milima Security and MTN Uganda are providing cybersecurity training, awareness campaigns and managed security services to support SMEs.

In the heart of Central Uganda, a groundbreaking project is underway to strengthen the digital resilience of SMEs. With the support of CIPESA, this initiative aims to equip SMEs with the knowledge and skills necessary to navigate the digital world with confidence.

3.2 Strengthening SMEs on digital and cybersecurity resilience in central Uganda and related policies.

The project aims to strengthen the digital resilience of SMEs in Central Uganda, aligning with Uganda's National Digital Transformation Policy and the East African Community's (EAC) Digital Strategy. With the support of CIPESA, this initiative equips SMEs with the knowledge and skills necessary to navigate the digital world with confidence, while promoting a secure and inclusive digital environment.

The project aligns with key policies, including Uganda's National Cybersecurity Strategy, which enhances the country's cybersecurity posture and protects against cyber threats. Additionally, it adheres to the Data Protection and Privacy Act, regulating personal data collection, storage, and use in Uganda. The EAC's Digital Strategy also guides the project, promoting the development of a digital economy in the region.

By enhancing SMEs' awareness and understanding of digital rights and cybersecurity best practices, the project unlocks Central Uganda's digital potential. SMEs are empowered to thrive in the digital age, protecting against cyber threats and promoting online safety and security. Through capacity building, advocacy and policy support, the project shapes a safer digital future for SMEs in Central Uganda, creating a more secure and inclusive digital environment for all stakeholders.

3.3 Policy and Legal Environment for digital Rights and Cybersecurity Resilience

Uganda has made significant strides in developing policies and frameworks to promote digital rights and cybersecurity. The National Cybersecurity Strategy aims to enhance the country's cybersecurity posture and protect against cyber threats, while the Data Protection and Privacy Act regulate the collection, storage and use of personal data. Additionally, the National Digital Transformation Policy promotes the development of a digital economy and inclusivity, providing a comprehensive framework for Uganda's digital growth. While challenges persist, including limited resources and infrastructure, cybercrime and digital divide issues, the policy environment in Uganda supports digital rights and cybersecurity, and ongoing efforts are being made to strengthen implementation and enforcement.

3.3.1 Existing Legal and Policy Framework

Uganda has established various legal and policy frameworks to promote digital rights and cybersecurity resilience. The Data Protection and Privacy Act (2019) regulate the collection, storage, and use of personal data, while the Computer Misuse Act (2011) and Cybercrime prevention measures address online harassment and cybercrime. The Electronic Transactions Act (2011) provides a framework for electronic transactions and digital signatures. Additionally, the National Cybersecurity Strategy and National Digital Transformation Policy guide the country's cybersecurity and digital development efforts. Regulatory bodies such as the Uganda Communications Commission and National Information Technology Authority also play a crucial role in overseeing the implementation of these frameworks, ensuring a secure and inclusive digital environment for all stakeholders.

3.3.2 Data Protection and Privacy Act (2019)

The Data Protection and Privacy Act, 2019 is a comprehensive law that regulates the collection, storage, and use of personal data in Uganda.

- i. **Data Protection Principles:** The Act outlines principles for data processing, including transparency, fairness, and lawfulness.
- ii. **Consent:** Organizations must obtain consent from individuals before collecting and processing their personal data.
- iii. **Data Subject Rights:** Individuals have rights to access, correct, and delete their personal data.
- iv. **Data Breach Notification:** Organizations must notify the National Information Technology Authority (NITA-U) and affected individuals in case of a data breach.
- v. **Enforcement:** The Act establishes penalties for non-compliance and provides for enforcement mechanisms.

Overall, the Data Protection and Privacy Act, 2019 provides a framework for protecting personal data and promoting responsible data handling practices in Uganda.

3.3.3 Benefits of enacting the Data Protection and Privacy Act, 2019

The Data Protection and Privacy Act, 2019 is a significant legislation that regulates the collection, storage, and use of personal data in Uganda. The Act aims to protect individuals' personal data, promote transparency, and empower individuals to make informed decisions about their data. By enacting this law, Uganda joins the global community in recognising the importance of data protection and privacy in the digital age. The Act applies to various entities, including businesses, government agencies, and organizations that process personal data, and provides for penalties for non-compliance. Its implementation is expected to enhance trust in digital services, support the growth of the digital economy, and safeguard individuals' rights to privacy and data protection. Overall, the Data Protection and Privacy Act, 2019 is a crucial step towards creating a secure and trustworthy digital environment in Uganda.

3.3.4 Harmonization with the existing Frameworks

The Data Protection and Privacy Act, 2019 in Uganda harmonizes with existing frameworks to ensure consistency and effectiveness. It aligns with the Constitution of Uganda, international best practices such as the General Data Protection Regulation (GDPR), and regional frameworks like the African Union's Convention on Cybersecurity and Personal Data Protection. Additionally, it complements Uganda's National Information Technology policies and sectoral regulations in finance, health, and telecommunications. This harmonization enables a cohesive approach to data protection and privacy, facilitating implementation and promoting a secure digital environment in Uganda.

3.3.5 Institutional and Local support

The Data Protection and Privacy Act, 2019 in Uganda receives institutional and local support from key stakeholders, including the National Information Technology Authority (NITA-U), Uganda Communications Commission (UCC), Parliament of Uganda and civil society organizations. These entities play a crucial role in regulating, overseeing and advocating for the implementation of the Act. Additionally, the private sector, comprising businesses and industries, also supports the Act by complying with its provisions and promoting a culture of data protection and privacy in Uganda. This collective support ensures the effective implementation and enforcement of the Act, ultimately protecting the personal data and privacy of Ugandan citizens.

3.3.6 Regional and International perspective

The Data Protection and Privacy Act, 2019 in Uganda aligns with regional and international perspectives, reflecting the country's commitment to global data protection standards. Uganda's law is informed by frameworks such as the African Union's Convention on Cybersecurity and Personal Data Protection and the General Data Protection Regulation (GDPR) of the European Union. This alignment enables Uganda to facilitate cross-border data transfers, enhance regional and international cooperation and also support digital trade and economic integration. By adopting globally recognised principles, Uganda promotes a secure digital environment and demonstrates its dedication to protecting the personal data of its citizens in accordance with international best practices.

3.3.7 Challenges of failing to Enact the Data Protection and Privacy Act, 2019

Failing to enact the Data Protection and Privacy Act, 2019 would have exposed Uganda to significant challenges, including loss of trust in digital services, increased risk of data breaches and economic implications. Without a data protection law, citizens' personal data would be vulnerable to unauthorized access, theft and misuse, hindering the growth of the digital economy and discouraging foreign investment. Additionally, Uganda would likely fail to meet international data protection standards, impacting global partnerships and increasing the risk of cyber-attacks. Ultimately, the absence of this law would compromise citizens' right to privacy and undermine the country's digital development.

3.3.8 International experiences and Lessons for Uganda

Failing to enact the Data Protection and Privacy Act, 2019 would have exposed Uganda to significant challenges, including loss of trust in digital services, increased risk of data breaches, and economic implications. Without a data protection law, citizens' personal data would be vulnerable to unauthorized access, theft and misuse, hindering the growth of the digital economy and discouraging foreign investment. Additionally, Uganda would likely fail to meet international data protection standards, impacting global partnerships and increasing the risk of cyber-attacks. Ultimately, the absence of this law would compromise citizens' right to privacy and undermine the country's digital development.

3.3.9 Lessons for Uganda.

Uganda can draw valuable lessons from global experiences in data protection and privacy. By examining successful frameworks and regulations, Uganda can develop effective strategies to safeguard personal data and promote digital trust. Key lessons for Uganda include:

Implement robust data protection laws: Enacting and enforcing strong laws protects citizens' personal data.

- i. **Establish an independent regulatory body** ensures compliance and accountability.
- ii. **Promote public awareness** through educating citizens about data protection empowers them.

4.0 Methodology

4.1 Description of data collection methods (surveys, interviews).

To assess the digital rights and cybersecurity capacity of PSFU member organizations, data was collected from 79 respondents across key sectors including manufacturing, agriculture, trade and commerce, ICT, transport and logistics, education, energy, and the creative industry as indicated in Table 1. A mixed-methods design was applied, combining structured surveys with semi-structured interviews conducted through both physical engagements and online platforms.

Surveys which were administered via digital forms and printed questionnaires, facilitated broad participation across Kampala, Wakiso, and Mukono districts. This enabled the collection of quantitative data on digital rights awareness, cybersecurity practices, institutional vulnerabilities, and readiness. Respondents rated their familiarity with concepts such as digital rights, data protection, cyber-hygiene, and compliance with the Data Protection and Privacy Act (2019).

To deepen the analysis, interviews were conducted with selected participants. These provided qualitative insights into institutional experiences, including trust in digital systems, internal policy gaps, resource limitations, and perceptions of cybersecurity risk. The mixed-methods approach ensured triangulation, enhancing the credibility and validity of findings (Creswell & Creswell, 2018).

The geographic, gender, and sectoral diversity of respondents strengthened the dataset, enabling a nuanced understanding of how digital rights and cybersecurity issues manifest across Uganda's private sector. This diversity was essential in identifying differentiated capacity gaps and informing tailored recommendations for PSFU's future programming, training, and advocacy initiatives.

Table 1: Respondent Disaggregation by District, Gender, and Sector

District	 Male	 Female	Sector Representation	
Kampala	40	20		Finance, Technology, Agriculture, Manufacturing, ICT transport and Logistics, Creatives and arts
Wakiso	10	05		Agriculture, Services, construction
Mukono	03	01		Manufacturing, Trade and commerce

This disaggregated dataset reflects varied realities of digital engagement and provides a strong empirical foundation for targeted capacity-building and policy interventions.

4.2 Analytical approaches (quantitative and qualitative)

The CNA employed both quantitative and qualitative analytical approaches to ensure a comprehensive understanding of digital rights and cybersecurity gaps among PSFU member organizations. Quantitative analysis was conducted using structured survey data from 79 respondents across Kampala, Mukono, and Wakiso, representing sectors such as agriculture, ICT, manufacturing, and trade. Descriptive statistics were used to assess digital tool usage, cybersecurity awareness, and policy implementation.

Qualitative insights were derived from open-ended survey responses and interviews, focusing on perceptions of risk, institutional challenges, and support needs. Themes such as lack of compliance knowledge, limited budgets, and low awareness of the Data Protection and Privacy Act (2019) emerged prominently. This dual approach enabled triangulation of findings and informed targeted recommendations for capacity building and policy advocacy.

4.3 Stakeholder engagement and validation process.

To ensure the credibility, accuracy, and contextual relevance of the CNA, a stakeholder validation workshop was held on Wednesday, 5th November 2025 at 9:00 AM in the PSFU Boardroom, Kampala.

The workshop aimed to validate preliminary CNA findings and refine recommendations relating to digital rights awareness and cybersecurity resilience among SMEs in Central Uganda. A total of 24 participants—7 women and 17 men—attended, representing eight sectors: agriculture (3), manufacturing (4), ICT (4), trade (3), arts and creative industries (2), human resources and health (2), and construction (6). All participants were from Central Uganda, predominantly Kampala. Discussions focused on practical, sector-specific strategies for strengthening SMEs' digital security practices, improving data governance, and enhancing digital rights awareness in alignment with Uganda's socio-economic context and the Digital Transformation Roadmap (2023–2028).

The consultant presented a structured PowerPoint summary of key findings, including statistics such as 81% awareness of cybersecurity threats compared to only 16% with formal cybersecurity policies. These figures stimulated rich dialogue, highlighting persistent capacity gaps and the urgent need for targeted intervention. The highly participatory engagement allowed stakeholders to critique the findings, validate gaps, and suggest actionable refinements to ensure the CNA reflects private-sector realities.

Feedback from the workshop is being systematically documented and integrated into the revised CNA report. This validation step is essential for:

- i. Building consensus among diverse actors;
- ii. Strengthening ownership of recommendations; and
- iii. Aligning future programming with sector needs and national digital transformation priorities.

By incorporating these insights, the CNA becomes a stronger foundation for capacity building, policy advocacy, and the advancement of a secure, inclusive, and resilient digital ecosystem for Uganda's SMEs.

5.0 Key Findings

5.1 Digital Communication and Online Presence

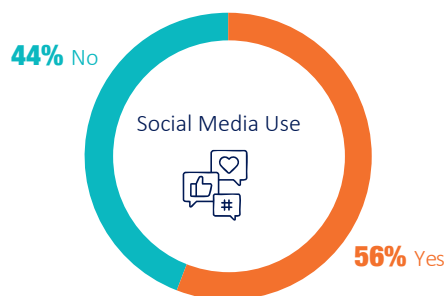
5.1.1 Social Media Usage

In the CNA study, 56% of businesses (44 out of 79) reported using social media platforms such as WhatsApp, Facebook, and Instagram for business engagement, indicating moderate adoption. This aligns with national trends, as Uganda had 2.4 million active social media users in early 2025, representing 4.7% of the population (DataReportal, 2025). The relatively low penetration suggests that while digital engagement is growing, significant gaps remain, especially among small and medium-sized enterprises (SMEs).

The effectiveness of these platforms is evident. WhatsApp, with over 9.3 million subscribers, is Uganda's most used app, followed closely by TikTok and Facebook (Pulse Uganda, 2025). A study in Wakiso District found that WhatsApp adoption explained 20.6% of SME performance variance, emphasizing its role in customer engagement and marketing (Mugarura et al., 2023). Facebook, with 3.2 million users, and Instagram, with 966,900 users, are also vital for brand visibility and customer interaction (NapoleonCat, 2025).

These findings support Uganda's Digital Transformation Roadmap (2023–2028), which aims to connect 90% of SMEs to the internet and digitize 95% of government services (Ministry of ICT & National Guidance, 2023). The moderate uptake shown in Figure 1 of the CNA report highlights the need for targeted interventions in digital literacy, infrastructure development, and affordable data access to fully leverage social media for inclusive economic growth.

Figure 1: Social Media Usage



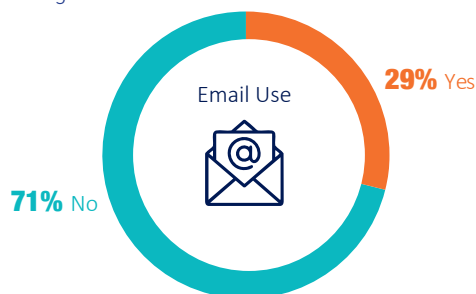
5.1.2 Email Usage

In Figure 2 of the CNA analysis, only 29% of businesses (23 out of 79) reported using email for communication, highlighting a significant gap in formal digital communication practices. This limited adoption contrasts with global trends, where 92% of online adults use email, and 86% of professionals prefer it for workplace communication (cloudHQ, 2025).

The low uptake of email usage in Uganda may be attributed to limited digital literacy, infrastructure challenges, and a preference for more accessible platforms like WhatsApp. According to the National IT Survey (NITA-U, 2022), many SMEs lack formal IT policies and structured communication systems, which hinders the adoption of email and other enterprise tools.

This finding underscores the need for targeted interventions in Uganda's Digital Transformation Roadmap (2023–2028), which aims to enhance digital skills and infrastructure for SMEs. Strengthening email usage can improve record-keeping, customer service, and access to e-government services, aligning with national goals for inclusive digital development (Ministry of ICT & National Guidance, 2023).

Figure 2: *Email Usage*



5.1.3 Website Ownership

In Figure 3 of the CNA analysis, 71% of businesses (56 out of 79) reported owning a website, indicating a stronger inclination toward establishing an online presence than using email. This is notable given Uganda's relatively low internet penetration of 28% (14.2 million users out of 50.7 million people) (DataReportal, 2025).

Website ownership among businesses suggests a strategic shift toward visibility and credibility in the digital economy. Despite limited email usage (29%), websites offer a platform for marketing, e-commerce, and customer engagement. This aligns with Uganda's Digital Transformation Roadmap (2023–2028), which prioritizes SME digital inclusion and aims to connect 90% of SMEs to the internet (Ministry of ICT & National Guidance, 2023).

The trend also reflects broader digital growth: Uganda had 38.6 million mobile connections (76.2% of the population) and 2.4 million social media users in early 2025 (DataReportal, 2025). As more businesses adopt websites, the potential for digital trade, online services, and global reach expands, reinforcing the CNA report's emphasis on digital readiness.

Figure 3: *Website Ownership*



5.2. Data Storage and Management Practices

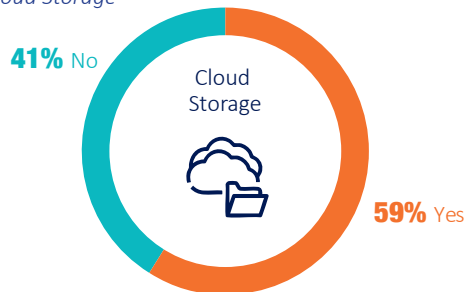
5.2.1 Cloud Storage

In Figure 4 of the CNA analysis, 59% of businesses (47 out of 79) reported using cloud storage, reflecting a growing awareness of modern data management solutions. This adoption aligns with national trends, as cloud computing in Uganda has grown by over 30% in the past three years, driven largely by SMEs, fintechs, and government agencies (Raxio Data Centre, 2025).

The uptake of cloud storage is fueled by its scalability, cost-efficiency, and enhanced data security. With Uganda's youth-driven economy- where 73% of the population is under 30 - businesses are increasingly embracing cloud and AI-powered solutions to meet growing digital demands (Raxio Data Centre, 2025). Cloud platforms offer SMEs the flexibility to manage data remotely, collaborate in real-time, and reduce IT infrastructure costs.

This trend supports Uganda's Digital Transformation Roadmap (2023–2028), which aims to digitize 95% of government services and connect 90% of SMEs to the internet (Ministry of ICT & National Guidance, 2023). The CNA findings highlight the importance of continued investment in cloud infrastructure and digital literacy to ensure inclusive and secure digital growth.

Figure 4: Cloud Storage



5.2.2 Customer Data Collection

In Figure 5 of the CNA analysis, 72% of businesses (57 out of 79) reported collecting customer data, reflecting a strong shift toward data-driven decision-making. This trend aligns with the rise of digital platforms and e-commerce in Uganda, where businesses increasingly rely on customer insights to tailor services and improve engagement (DataReportal, 2025).

However, this widespread data collection raises critical concerns about data privacy and protection. Uganda's Data Protection and Privacy Act, 2019 mandates that all entities handling personal data must register with the Personal Data Protection Office (PDPO) and maintain clear records of data processing activities. Failure to comply can result in administrative fines or legal action (PDPO, 2025).

The PDPO's 2025 ruling against Google LLC emphasized that all entities—local or foreign—handling Ugandan citizens' data must comply with national laws, including registration and cross-border data transfer safeguards. This underscores the urgent need for businesses to adopt robust data governance frameworks to protect customer information and build trust (Mbuga & Muhawe, 2025).

Figure 5: Customer Data Collection

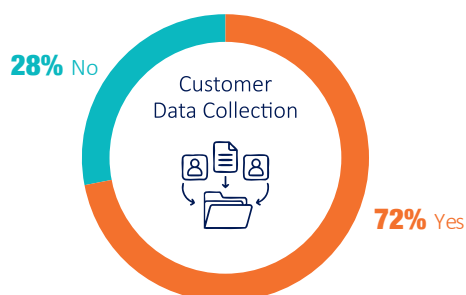


Figure 6: *Awareness of Cybersecurity Threats*

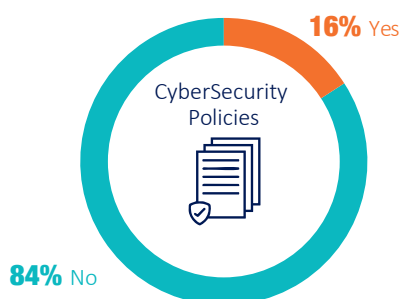
5.3 Cybersecurity Awareness and Implementation

5.3.1 Awareness of Cybersecurity Threats

In Figure 6 of the CNA analysis, 81% of businesses (64 out of 79) reported awareness of cybersecurity threats, indicating a strong understanding of digital risks among Ugandan enterprises. This aligns with national efforts like the “Beera Ku Guard” campaign launched by NITA-U and the Personal Data Protection Office to raise cybersecurity awareness across the country (Business Times, 2025).

Despite this high awareness, Uganda remains vulnerable. The Uganda Police Force’s 2024 Crime Report revealed a sharp rise in cyber fraud, including mobile money theft and phishing scams. Experts warn that actual losses are underreported, and only 13.6% of Ugandans understand data protection laws, highlighting a gap between awareness and actionable knowledge (Business Times, 2025).

The Digital Transformation Roadmap (2023–2028) emphasizes cybersecurity as a pillar of a trusted digital economy. NITA-U aims to register 1,000 organizations and train 500 data protection officers by 2026. These efforts are crucial to translating awareness into robust cybersecurity practices and ensuring Uganda’s digital growth is secure and inclusive (Ministry of ICT & National Guidance, 2023).

Figure 7: *Cybersecurity Policies*

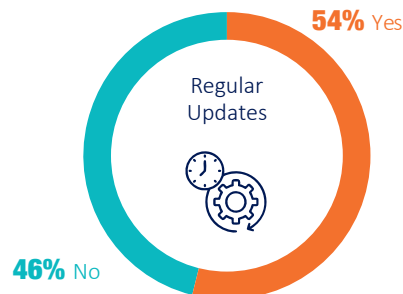
5.3.2 Regular Updates

In Figure 8 of the CNA analysis, 54% of businesses (43 out of 79) reported performing regular software updates, a positive indicator of growing cybersecurity maturity. Regular updates are essential for patching vulnerabilities and maintaining system integrity, especially as Uganda’s digital economy expands (MoldStud, 2025).

Globally, organizations that apply patches within 14 days of release experience a 48% reduction in breach incidents, while 60% of companies that suffer cyberattacks lack a formal update process (MoldStud, 2025). Regular updates can mitigate 85% of exploited vulnerabilities, making them a cost-effective *Défense* against evolving threats.

This practice aligns with Uganda’s National Cybersecurity Strategy (2022–2026), which emphasizes proactive risk management and system resilience. As cybercrime costs continue to rise, regular updates are a foundational step toward securing digital infrastructure and ensuring business continuity (Ministry of ICT & National Guidance, 2023).

Figure 8: *Regular Updates*



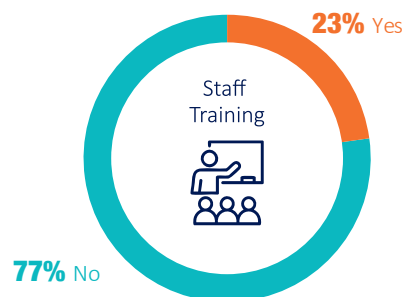
5.3.3 Staff Training

In Figure 9 of the CNA analysis, only 23% of businesses (18 out of 79) reported training staff on cybersecurity, highlighting a critical gap in capacity building. This is concerning given the rising cyber threats in Uganda, where cybercrime cost the economy UGX 19.2 billion in 2022 alone across 245 reported cases (Milima Cyber Academy, 2024).

Despite growing awareness—81% of businesses acknowledge cybersecurity threats—many SMEs lack the resources or expertise to implement effective training programs. Without proper staff education, businesses remain vulnerable to phishing, ransomware, and social engineering attacks, which often exploit human error as the weakest link in cybersecurity (Milima Cyber Academy, 2024).

The National Cybersecurity Strategy (2022–2026) emphasizes the need for a “cyber-skilled Uganda,” promoting training programs and awareness campaigns. Organizations like Milima Security are stepping in to fill the gap, offering tailored training and cybersecurity maturity programs for SMEs. However, broader adoption is needed to ensure Uganda’s digital economy is secure and resilient (Ministry of ICT & National Guidance, 2023).

Figure 9: *Staff Training*



5.3.4 Cybersecurity Incidents

In Figure 10 of the CNA analysis, only 13% of businesses (10 out of 79) reported experiencing cybersecurity incidents in the past year. While this figure appears low, it likely reflects significant underreporting. According to the Uganda Police Force, 286 cybercrime cases were officially recorded in 2022, resulting in losses of UGX 19.2 billion, with only Shs 16.7 million recovered (The Independent, 2024).

Despite 81% of businesses acknowledging awareness of cyber threats, the low incident reporting rate suggests a gap in detection, response, or willingness to disclose breaches. Many SMEs lack formal incident response plans or trained personnel, which hinders their ability to identify and report cyberattacks effectively. This underreporting may also stem from fear of reputational damage or legal consequences.

The National Cybersecurity Strategy (2022–2026) emphasizes the need for a centralized incident register and sector-specific Computer Security Incident Response Teams (CSIRTs). Strengthening incident reporting mechanisms and building trust in regulatory frameworks are essential to improving Uganda’s cyber resilience and ensuring that threats are accurately tracked and mitigated (Ministry of ICT & National Guidance, 2023).

Figure 10: *Cybersecurity Incidents*

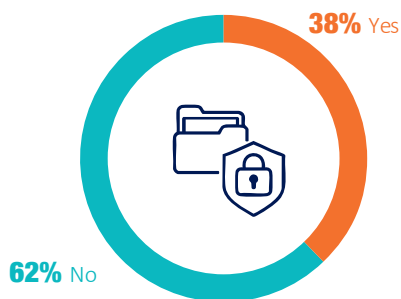


5.4. Policy, Legal and Regulatory Awareness

In Figure 11 of the CNA analysis, only 38% of businesses (30 out of 79) reported awareness of Uganda’s Data Protection and Privacy Act (2019), highlighting a significant policy, legal, and regulatory gap within the business ecosystem. This low level of legal literacy is particularly concerning as more businesses transition to digital operations and increasingly collect, store, and process personal data. Despite the Act being in force since May 3, 2019, and the establishment of the Personal Data Protection Office (PDPO), compliance remains weak. National data further reflects this challenge: a recent NITA-U survey shows that although 48.8% of Ugandans have heard of cybersecurity, only 13.6% understand data protection and privacy laws, exposing enterprises to operational, legal, and reputational risks.

To strengthen national legal and regulatory compliance, the “Beera Ku Guard” campaign—launched in 2025 by NITA-U and PDPO—aims to raise cybersecurity and data protection awareness to 70% of the population through mass media, institutional sensitization, and public engagement. The campaign emphasizes responsible data governance, digital trust, and adherence to national regulatory frameworks. Integrating policy, legal, and regulatory awareness into business practices is essential for ensuring compliance, reducing vulnerabilities, and building a safer and more competitive digital economy in Uganda.

Figure 11: *Awareness of Uganda’s Data Protection and Privacy Act (2019)*



5.5 Budgeting and Strategic Planning

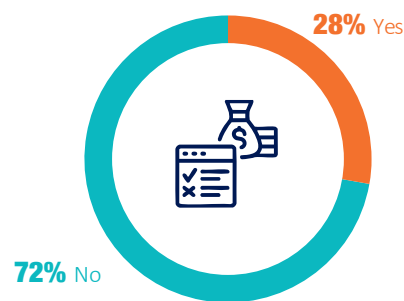
5.5.1 Budget for Digital Tools and Cybersecurity

In Figure 12 of the CNA analysis, only 28% of businesses (22 out of 79) reported having a dedicated budget for digital tools and cybersecurity. This limited allocation restricts their ability to implement robust digital infrastructure and security measures, despite the increasing reliance on digital platforms for operations and customer engagement (Business Times, 2025).

Most SMEs in Uganda operate without essential cybersecurity tools such as firewalls, antivirus software, or secure data backup systems. The lack of financial and technical capacity means that basic digital hygiene practices—like multi-factor authentication or phishing awareness—are often neglected. This leaves businesses vulnerable to cyber threats, which are becoming more frequent and sophisticated (Business Times, 2025).

The National Cybersecurity Strategy (2022–2026) emphasizes the need for increased investment in cybersecurity, especially among SMEs. It advocates for affordable, easy-to-use solutions and public-private partnerships to support digital resilience. Without dedicated budgets, SMEs risk data breaches, financial losses, and reputational damage, undermining Uganda’s broader digital transformation goals (Ministry of ICT & National Guidance, 2023).

Figure 12: Budget for Digital Tools and Cybersecurity



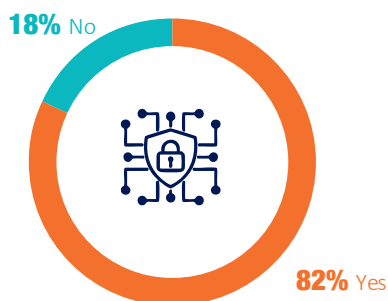
5.5.2 Willingness to Partner for Digital Resilience

In Figure 13 of the CNA analysis, 82% of businesses (65 out of 79) expressed willingness to partner for digital resilience, signalling a strong appetite for collaboration. This openness is crucial in a context where 96% of Ugandan businesses are SMEs, often lacking the resources to independently implement robust digital solutions (ILO, 2025).

Collaborative efforts can bridge gaps in infrastructure, skills, and cybersecurity. The International Labour Organization’s (ILO’s) 2025 digitalization guide emphasizes partnerships as key to building capacity, sharing tools, and fostering innovation among micro and small enterprises. These partnerships can include digital service providers, government agencies, and development partners offering training, funding, and infrastructure support (ILO, 2025).

This willingness aligns with Uganda's Digital Transformation Roadmap (2023–2028), which promotes public-private partnerships to accelerate digital inclusion and resilience. By leveraging collective strengths, businesses can better navigate digital risks, access shared platforms, and scale their operations sustainably in an increasingly digital economy (Ministry of ICT & National Guidance, 2023).

Figure 13: *Willingness to Partner for Digital Resilience*



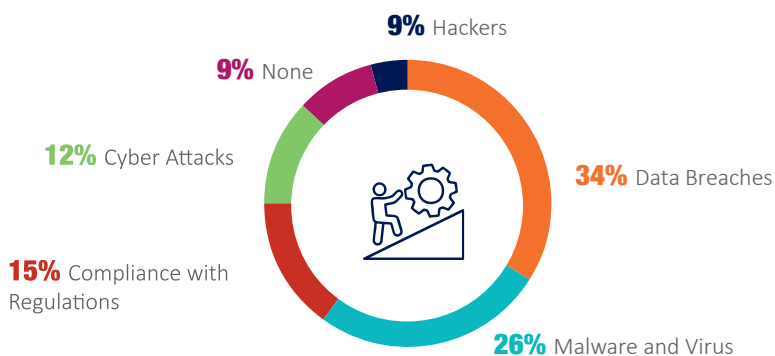
5. 6 Challenges and Support Needs

5.6.1 Challenges Faced

In Figure 14 of the CNA analysis, data breaches (25 businesses) and malware/virus attacks (19 businesses) emerged as the most common cybersecurity challenges. This aligns with the Allianz Risk Barometer 2024, which ranked cyber-attacks—including ransomware and data breaches—as the top business risk in Uganda, surpassing theft, fraud, and natural disasters (The Independent, 2024).

Despite growing awareness, many businesses lack the resources to implement robust cybersecurity measures. The Uganda Police Force reported 286 cybercrime cases in 2022, resulting in losses of UGX 19.2 billion, with only UGX 16.7 million recovered. This highlights the severity of threats and the limited capacity for response and recovery (The Independent, 2024). Compliance challenges and broader cyber-attacks also featured prominently. Experts emphasize the need for a holistic cybersecurity approach, including vendor assessments, staff training, and shared threat intelligence. The National Cybersecurity Strategy (2022–2026) calls for increased vigilance and institutional controls to protect Uganda's digital economy from escalating cyber threats (Ministry of ICT & National Guidance, 2023).

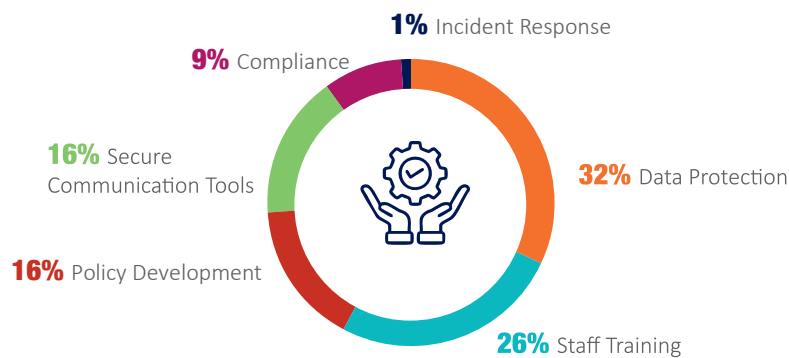
Figure 14: *Challenges Faced*



5.6.2 Support Needs:

In Figure 15 of the CNA analysis, 32% of businesses identified data protection as their top support need, highlighting strong demand for tools such as data encryption solutions, secure data backups, intrusion detection and prevention systems, and ERP platforms to modernize and safeguard operations. This aligns with Uganda's Digital Transformation Roadmap (2023–2028), which aims for 90% household connectivity and 90% broadband coverage by 2040. Staff training represents 26% of identified needs, while secure communication tools and policy development each account for 16%, reflecting diverse but interlinked capacity gaps. However, low digital literacy and limited regulatory compliance continue to impede meaningful digital adoption. The roadmap emphasizes digital skills, cybersecurity, and data privacy as foundational pillars, calling for increased ICT investment, expanded e-services, and targeted capacity building. Addressing these needs through strong public–private partnerships and donor support will be essential for achieving inclusive, secure, and sustainable digital transformation across Uganda's business ecosystem.

Figure 15: *Support Needs*



7.0 Recommendations

The Capacity Needs Analysis (CNA) revealed several critical gaps and opportunities for strengthening digital resilience among businesses. Based on the findings, the following eight key recommendations are proposed in the following categories.

1. Government:

- i. **Enhance Digital Literacy and Skills Development:** With only 23% of businesses providing cybersecurity training, there is a pressing need for structured capacity-building programs. Government and partners should invest in training initiatives targeting SMEs, focusing on digital tools, cybersecurity and data protection.
- ii. **Promote Awareness of Legal Frameworks:** Only 38% of businesses are aware of the Data Protection and Privacy Act (2019). Awareness campaigns and simplified legal guides should be developed to improve compliance and understanding of data protection obligations.
- iii. **Support Policy Development:** Just 16% of businesses have formal cybersecurity policies. Technical assistance should be provided to help SMEs develop and implement cybersecurity and data governance policies tailored to their operations.
- iv. **Increase Budget Allocation for Digital Tools:** With only 28% of businesses allocating budgets for digital tools and cybersecurity, financial incentives, grants, or tax reliefs should be introduced to encourage investment in digital infrastructure.
- v. **Improve Incident Reporting Mechanisms:** Only 13% of businesses reported cybersecurity incidents, suggesting underreporting. Establishing anonymous reporting channels and sector-specific CSIRTs can improve threat visibility and response.
- vi. **Expand Access to Cloud and Web Services:** With 71% of businesses owning websites and 59% using cloud storage, efforts should focus on expanding affordable internet access and promoting secure cloud adoption through training and subsidies.
- vii. **Prioritize Digital Transformation Support:** Digital transformation was the top support need for 48 businesses. Tailored programs should be developed to guide SMEs through digital adoption, including e-commerce, CRM systems, and digital marketing.

2. Private Sector:

- i. **Foster Public-Private Partnerships:** A promising 82% of businesses are open to partnerships. Stakeholders should leverage this willingness to build collaborative platforms for knowledge sharing, joint investments, and innovation.
- ii. **Invest in digital technologies:** Increase budget allocation for digital tools and cybersecurity.

3. SMEs:

- i. **Develop digital strategies:** Adopt digital tools and platforms, including e-commerce, CRM systems, and digital marketing.
- ii. **Implement cybersecurity policies:** Develop and implement cybersecurity and data governance policies tailored to their operations.

4. Multi-Stakeholder Collaboration:

- i. **Establish digital innovation hubs:** Build collaborative platforms for knowledge sharing, joint investments, and innovation.
- ii. **Promote digital literacy and awareness:** Collaborate to promote digital literacy and awareness among businesses and individuals.

8.0 Conclusion

The CNA conducted among 79 businesses reveals a sector that is advancing in digital adoption yet constrained by significant gaps that threaten long-term resilience and competitiveness. While many businesses have embraced social media, cloud storage, and website ownership, formal digital communication, structured cybersecurity practices, and compliance with the Data Protection and Privacy Act (2019) remain weak. Awareness of cybersecurity risks is high, but implementation of policies, staff training, and budgeting for digital tools is notably low, leaving businesses vulnerable to threats such as data breaches and malware attacks. Encouragingly, most businesses express strong willingness to collaborate on digital resilience, identifying digital transformation, data protection, staff training, and policy development as their top needs. These insights underscore an urgent need for targeted investments in digital literacy, legal awareness, capacity building, and public–private partnerships. Strengthening these areas will be essential for achieving Uganda’s Digital Transformation Roadmap (2023–2028) targets and for building a resilient, inclusive, and competitive digital economy that empowers businesses and safeguards citizens in the digital age.

9.0 References

Abaho, E., Aguma, D., Beronda, J., Nkambwe, I., Obang, H., & Kituyi, G. M. (2025). E-Booster Uganda: Towards an inclusive digital economy. *Universal Access in the Information Society*, 24, 1863–1872. <https://doi.org/10.1007/s10209-024-01152-9>

Business Times Uganda. (2025). Cybersecurity and data protection challenges facing SMEs in Uganda. <https://businesstimesug.com>

Business Times. (2025, August 4). Cybersecurity and data protection challenges facing SMEs in Uganda. <https://businesstimesug.com/cybersecurity-and-data-protection-challenges-facing-smes-in-uganda/>

Business Times. (2025, September 5). How Uganda is to save businesses from losing billions to cybercrime. <https://businesstimesug.com/how-uganda-is-to-save-businesses-from-losing-billions-to-cybercrime/>

CloudHQ. (2025). Workplace email statistics 2025: Usage, productivity, trends. <https://blog.cloudhq.net/workplace-email-statistics/>

DataReportal. (2025). Digital 2025: Uganda. <https://datareportal.com/reports/digital-2025-uganda>

DataReportal. (2025). Digital 2025: Uganda. <https://datareportal.com/reports/digital-2025-uganda>

NITA-U. (2024). National Cybersecurity Strategy 2022–2026. <https://nita.go.ug>

Digital Watch Observatory. (2023). Ugandan National Cybersecurity Strategy 2022–2026. <https://dig.watch/resource/ugandan-national-cybersecurity-strategy-2022-2026>

International Labour Organization (ILO). (2025). Embracing Digital in Uganda: A Practical Guide for Freelancers, Digital Entrepreneurs and Owners of Micro and Small Enterprises. Geneva: International Labour Office. <https://www.ilo.org/sites/default/files/2025-10/25026-ILOP-Embracing-digital-Uganda-report-v5-1-E.pdf>

Mbuga, P., & Muhawe, R. (2025, August 6). Uganda: Data protection regulator clarifies compliance requirements for offshore entities. *Privacy Matters*. <https://privacymatters.dlapiper.com/2025/08/uganda-data-protection-regulator-clarifies-compliance-requirements-for-offshore-entities/>

Milima Cyber Academy. (2024). Harnessing cybersecurity for businesses in Uganda’s growing digital economy. <https://mca.ac.ug/harnessing-cybersecurity-for-businesses-in-ugandas-growing-digital-economy/>

Ministry of ICT & National Guidance. (2023). Uganda Digital Transformation Roadmap 2023–2028. Kampala: Government of Uganda.

Mugarura, R., Osunsan, O. K., Byamukama, V., & Timbirimu, M. (2023). Integration of WhatsApp and its influence on small and medium enterprise performance in Buloba Town, Wakiso, Uganda. *International Journal of Recent Advances in Multidisciplinary Topics*, 4(11). <https://www.researchgate.net/publication/375877759>

NapoleonCat. (2025). *Social media users in Uganda 2025*. <https://stats.napoleoncat.com/social-media-users-in-uganda/2025/>

National Information Technology Authority - Uganda (NITA-U). (2022). *National Information Technology Survey Final Report 2022*. <https://nita.go.ug/sites/default/files/2022-12/National%20IT%20Survey%20Report%202022%20-%20Final.pdf>

National Information Technology Authority - Uganda (NITA-U). (2025, September 3). *Beera Ku Guard Campaign to Promote Cybersecurity, Data Protection and Privacy*. <https://media.gcic.go.ug/wp-content/uploads/2025/09/Press-Release-NITA-U-LAUNCHES-NATIONWIDE-BEERA-KU-GUARD-CAMPAIGN-TO-PROMOTE-CYBERSECURITY-DATA-PROTECTION-AND-PRIVACY.pdf>

Paradigm Initiative. (2023). *LONDA: Digital Rights and Inclusion in Africa Report 2022*. <https://paradigmhq.org/wp-content/uploads/2023/06/Uganda-Londa-2022.pdf>

Pulse Uganda. (2025, July 6). *Ugandans spend Shs 55bn a day on TikTok data - Report*. <https://www.pulse.ug/articles/business/ugandans-spend-shs-55bn-a-day-on-tiktok-data-report-2025070500515982422>

Raxio Data Centre. (2025, May 14). *Cloud computing in Uganda has grown by over 30% in 3 years*. <https://thebrinknews.com/report-cloud-computing-in-uganda-has-grown-by-over-30-in-3-years-raxio-data-centre-s-data-centre/>

TechAfrica News. (2025). *ANCA grows as six nations signal intent to join*. <https://techafricanews.com>

