Journal of
International Relations
(JIR)

Cybersecurity Practices and International Relations Performance in Rwanda. A Case of Broadband Systems Corporation

Daniel Mirenge Kayonga, Malgit Amos Akims, PhD and Festus Irungu Ndirang

IPRJB

Cybersecurity Practices and International Relations Performance in Rwanda. A Case of Broadband Systems Corporation

Daniel Mirenge Kayonga[1]
Masters of Arts Student, International Relations and Diplomacy, Mount Kenya University

Malgit Amos Akims, PhD[2]
Mount Kigali University

Festus Irungu Ndirang[3]
Mount Kigali University

Article History

Received 2nd September 2024

Received in Revised Form 6th October 2024

Accepted 4th November 2024

How to cite in APA format:

Kayonga, D., Akims, M., & Ndirang, F. (2024). Cybersecurity Practices and International Relations Performance in Rwanda. A Case of Broadband Systems Corporation . *Journal of International Relations*, *4*(4), 28–40. https://doi.org/10.47604/jir.3055

Abstract

Purpose: The general objective of the research was to assess the effect of cybersecurity practices on international relations performance in Rwanda, a case of Broadband Systems Corporation. Specifically, the study determined the effect of cybersecurity policies on the international relations performance in Rwanda, to find out the effect of cybersecurity technology on the international relations performance in Rwanda and to assess the effect of cybersecurity training on the international relations performance in Rwanda.

Methodology: Descriptive, correlational, qualitative and quantitative based on primary and secondary data were used in the study. This research aimed to gather data from 229 employees, stakeholders of Broadband Systems Corporation, including company officials, cybersecurity staff and beneficiaries. Using Slovin's approach, the researcher determined the number of participants needed for the sample. Researcher had 146 participants in their sample, out of a total population of 229. The researcher used questionnaires question to gather primary data. The researcher analyzed the data using SPSS (Statistical Package for Social Scientists, version 25) to grasp statistics such as percentage, mean, standard deviation, and frequency. Bivariate correlation analysis was performed to investigate the hypotheses.

Findings: The model demonstrates a multiple correlation coefficient (R) of 0.877, signifying a robust positive correlation among cybersecurity policies, cybersecurity technology, and cybersecurity training with the dependent variable, international relations performance in Rwanda. Analysis of Variance results for the regression analysis shows the F-value is 141.583, which indicates a highly significant model fit. The significance level (Sig.) is .000, demonstrating that the predictors cybersecurity technology, cybersecurity policies, and cybersecurity training significantly contribute to explaining variations in international relations performance.

Unique Contribution to Theory, Practice and Policy: BSC should implement continuous cybersecurity awareness training to help employees recognize and respond to common cyber threats.

Keywords: *Cybersecurity Policies, Cybersecurity Practices, Cybersecurity Technology, Cybersecurity Training, International Relations Performance*

INTRODUCTION

The complexity and interconnectedness of global networks are expanding, rendering organizations worldwide more susceptible to cybersecurity threats. Organizations face an abundance of threats to their data and operations when they expand globally. Among these difficulties are developments in regulations, innovations in technology, and cyberattacks (Amoo *et al.*, 2024). In order to thrive in these unpredictable markets, businesses need to strengthen their cybersecurity measures. Organizations may improve their cybersecurity measures by responding to events, learning from them, and being resilient in the face of attacks. Protecting data and keeping operations running smoothly are two of the most important things for a resilient business to do if it wants to succeed in the long run (Abdel, 2023).

Problem Statement

A strong and safe digital infrastructure is crucial to the Rwandan goal of becoming a regional center for technology. Cybersecurity risks are at all-time high because of the country's heavy dependence on technology. Both Rwanda's domestic security and its performance in international relations are jeopardized by these dangers (Bowman, 2023).

A cybersecurity threat is threatening Rwanda's digital aspirations. Rwanda Information Society Authority reports (2023) present a troubling picture. Sophos reports (2024) that phishing attempts targeting Rwandan government institutions and vital infrastructure have increased by 32% since 2022, making it one of the most susceptible African countries. Not only do these assaults interrupt vital services, but they also damage confidence in Rwanda's cyber defenses, which might make prospective investors wary of the country's computer industry. Moreover, the number of data intrusions is increasing, with a 27% increase in incidents involving personal data disclosures in 2024 compared to 2023. In line with this, Comparitech (2024) ranked Rwanda as one of the top 20 countries for data breaches worldwide in 2024. The security of personal information is at risk, and Rwanda's standing as a trustworthy digital partner in global partnerships is damaged, as a result of these breaches. A severe shortage of cybersecurity skills is exacerbating these problems. There is a dearth of qualified cybersecurity experts in Rwanda, since the country was rated 134th in the world by the International Telecommunication Union in 2023. Carnegie Mellon University highlighted that 72% of Rwandan companies lack adequate cybersecurity personnel. As a result, Rwanda's reputation as a worldwide leader in cybersecurity suffers and the country is unable to adequately detect, prevent, and react to cyber-attacks. Rwanda has ambitions to become a regional technological powerhouse, and addressing these cybersecurity concerns is vital to that end (Comparitech, 2024).

As a result of its inadequate cybersecurity measures, Rwanda is unable to achieve its ambitions in the areas of digital leadership and international relations. The erosion of confidence caused by frequent cyberattacks has the potential to postpone partnerships on vital digital initiatives such as e-governance. The disclosure of sensitive information via data breaches further dissuades nations from working together to combat cybercrime and share intelligence. The cumulative effect of these problems is a diminished image of Rwanda as a trustworthy online partner, which might reduce investment from outside and slow the country's progress in economic and technical development.

The study on cybersecurity practices and international relations performance at Broadband Systems Corporation (BSC) enhanced Rwanda's digital security, restore investor confidence, and improve international relations by mitigating cyber threats, safeguarding sensitive data, and supporting the nation's ambition to become a regional technology hub.

The general objective of the research was to assess the effect of cybersecurity practices on international relations performance in Rwanda.

Specific Objectives

i. To determine the effect of cybersecurity policies on the international relations performance in Rwanda.
ii. To find out the effect of cybersecurity technology on the international relations performance in Rwanda.
iii. To assess the effect of cybersecurity training on the international relations performance in Rwanda.

Research Hypotheses

i. Cybersecurity policies have no significant effect on the international relations performance in Rwanda.
ii. Cybersecurity technology has no significant effect on the international relations performance in Rwanda.
iii. Cybersecurity training has no significant effect on the international relations performance in Rwanda.

LITERATURE REVIEW

Theoretical review

A theoretical framework is defined as an analysis and review of all prior work on the subject. Data mining is the practice of collecting and analyzing data from many sources in order to develop a more complete picture of a problem.

Organizational Learning Theory

According to Harvey *et al.* (2022), the core principle of organizational learning is that companies gain knowledge from their experiences and use that knowledge to enhance their strategies, processes, and structures. Organizations are defined as systems that rely on and adapt to their past in order to function effectively. Learning may occur in a variety of ways, including first-hand experience, planned learning (by understanding the experiences of others), unsystematic learning (by seeking knowledge via research, surveys, and experiments), and so on. Incorporating learning into routines allows for the accumulation and updating of knowledge repositories in response to events. Rules, tactics, technology, practices, and talents are all examples of routines. Peschl (2023) states that successful learning companies are able to absorb new ideas and overcome stagnation. Unlearning and learning go hand in hand in this process. Possible origins of such encounters include outsourcing, inter-firm cooperation, and unusual occurrences. Organizations may gain knowledge from both successful and unsuccessful events (Nujen *et al.*, 2023).

Cybersecurity crises may act as learning triggers, according to Naseer *et al.* (2024), who conducted interviews with cybersecurity decision-makers. In addition, they discover that big breaches influence cybersecurity enhancement decisions, whereas companies would rather keep things as they are when there have been no occurrences. After a big event that caused material damage, a company will want to make sure it doesn't happen again. Improving security capabilities begins with financial investments in security. In the case of companies with little resources, this is particularly true; these businesses will most likely only take action in response to disruptive events, rather than proactively preventing them (Shaikh & Siponen, 2023).

Therefore, organizational Learning Theory shows that BSC can enhance its cybersecurity practices by learning from past incidents, promoting better international relations performance. This led to more strong security measures, reducing vulnerabilities and fostering trust with international partners.

Diffusion of Innovation (DOI) Theory

The Diffusion of Innovation (DOI) Theory, first out by Everett Rogers in 1962, provides an explanation for the how, why, and pace of dissemination of new ideas and technologies across cultures. Sociologist Carl Rogers first proposed this idea in his groundbreaking book "Diffusion of Innovations." A social system's members are able to learn about and implement new innovations via the steps outlined in the theory (Mbatha, 2024). A small number of individuals act as early adopters, and word gets around as the invention gains traction, according to Rogers's S-curve theory of adoption. According to the theory, there are five distinct types of adopters, each with its own degree of openness to new ideas: innovators, early adopters, early majority, late majority, and laggards (Putteeraj *et al.*, 2022). The relative benefit of the innovation, its conformity with current beliefs and practices, its simplicity, its trialability, and the visible effects are some of the other elements that DOI identifies as influencing the adoption rate. Important parts of the dissemination process also include social structures and avenues of communication. Public health, education, marketing, and technological adoption are just a few of the many areas that have made use of DOI since its first application to rural agricultural breakthroughs. One area where DOI has been useful is public health, specifically in tracing the dissemination of innovative health habits and medical procedures (Leng *et al.*, 2024).

Therefore, Diffusion of Innovation Theory indicates that by adopting best practices from other countries after a cyberattack, BSC can improve its cybersecurity posture and potentially become a leader in cybersecurity innovation, enhancing its international reputation.

Game Theory

Mathematical pioneer John von Neumann and economist Oskar Morgenstern laid the groundwork for game theory in their 1944 book "Theory of Games and Economic Behavior." Game theory provides a mathematical framework for understanding strategic interactions among rational decision-makers. When people's results are dependent on both their own and other people's activities, the theory offers a methodical framework for studying such circumstances (Weiss & Agassi, 2023). Different kinds of strategic interactions are shown by the many games included, which range from cooperative to non-cooperative, symmetric to asymmetric, zero-sum to non-zero-sum. John Nash, a mathematician, created the Nash Equilibrium in the 1950s, and it is one of the basic ideas in game theory. At a Nash Equilibrium, all players' tactics are stable and no one can gain an advantage by switching up their approach. Many fields, including politics, economics, military strategy, and the social sciences, stand to benefit greatly from this idea (Barron, 2024).

In economics, for instance, game theory sheds light on the decision-making processes of competing enterprises in relation to pricing, production, and market entrance. As a field of study in international relations, it sheds light on how nations act in situations involving potential conflict or cooperation, including trade talks, alliance formation, and weapons races.

Another famous game, The Prisoner's Dilemma, shows how difficult it is for nations or people to work together and trust one another. Despite its usefulness as an analytical tool, game theory suffers from a number of major shortcomings. For example, it presumes complete information and reason, which are not always present in the real world. Nevertheless, its ability to analyze and predict strategic behavior in many contexts makes it an invaluable tool in both theoretical and practical research across several disciplines (Huang & Zhu, 2022).

Therefore, Game Theory highlights that by cooperating with international partners on cybercrime investigations and sharing threat intelligence, BSC can create a situation where both countries benefit from improved cybersecurity, ultimately strengthening international relations.

Empirical Review

Radanliev (2024) examined cyber diplomacy, which was defined as the potential for cybersecurity and the risks associated with Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Cyber diplomacy is crucial for dealing with the dynamic cybersecurity threats and possibilities in the modern day. In this post, we will take a look at how cyber diplomacy is being impacted by AI, the IoT, blockchains, and quantum computing. The combination of AI's danger detection capabilities with the IoT's worldwide data sharing capabilities makes for a formidable combination. Despite blockchains' usefulness in document verification and secure data sharing, they also bring new dangers like AI-driven cyberattacks, privacy lapses in the IoT, blockchain vulnerabilities, and the prospect of quantum computing cracking encryption. This report employs case study reviews and secondary data analysis to emphasize the need of global cooperation in managing responsible technology usage. Cyber diplomacy aims to promote cybersecurity, protect national interests, and foster trust among governments in the digital arena by using opportunities and minimizing dangers.

A study conducted by Hasani *et al.* (2023) examined the impact of cybersecurity adoption on organizational performance. All throughout the world, businesses are seeing a decline in performance due to cyberattacks. There is a lack of research on the elements that influence businesses' cybersecurity adoption and awareness, even as organizations are investing more in cybersecurity to prevent cyberattacks. In this study, researcher integrate the balanced scorecard method with the diffusion of innovation theory (DOI), the technology acceptance model (TAM), and the technology-organization-environment (TOE) frameworks to assess the impact of cybersecurity adoption on organizational performance. The data was compiled via a poll that received 147 valid answers from IT professionals employed by UK SMEs. An analysis of the model was conducted using structural equation modeling, which is a component of SPSS, a social science statistical program. The research confirms the significance of eight variables that influence cybersecurity adoption by SMEs and identifies them. Organizational performance is favorably affected by cybersecurity technology adoption. An evaluation of the significance of the factors impacting the adoption of cybersecurity technology is presented in the suggested framework. Information technology and cybersecurity managers may use this study's findings as a springboard for further research and to determine which cybersecurity solutions will have the most beneficial effect on their business.

Kala (2023) looked at how important cyber security is for the world's economy. With the advent of information operations, in which all players use computers, new dangers to national security have emerged as a result of IT advancements. This research delves into the topic of power imbalances in military engagements throughout history, specifically focusing on how international law has formed the battlefield of cyberspace. The importance of cybersecurity in preserving economic stability and safeguarding vital infrastructures is emphasized by the study. According to the results, internet has become a major battlefield due to the fact that advances in IT have produced major dangers. In order to keep up with the ever-changing cyber threats and maintain economic stability, the study suggests the following actions: increasing defense spending, bolstering cybersecurity measures, creating thorough policies, promoting international cooperation to build a strong legal framework, and routinely revising strategies.

Cremer *et al.* (2022) investigated cyber risk and cybersecurity. Cybercrime increased its global economic effect by about 50% between 2018 and 2020, with estimates putting the toll at little under USD 1 trillion. As the average cost of cyber insurance claims rises from $145,000 in 2019 to $359,000 in 2020, there is a growing need to improve cyber information sources, standardize databases, mandate reporting, and raise public awareness. The current academic and business literature on cybersecurity and cyber risk management is reviewed in this research, with a focus on data availability. From a preliminary search of 5219 online peer-reviewed journals, 79 different datasets were obtained by using the systematic procedure. Based on research findings, stakeholders dealing with cyber risk have a major hurdle in the shape of inadequate data. Our combined attempts to address these threats are thwarted by a lack of publicly accessible datasets, which we have identified in particular. The data categorization and evaluation findings could help cybersecurity researchers and the insurance industry better understand, measure, and control cyber threats.

AlDaajeh *et al.* (2022) evaluated the impact of several national cybersecurity initiatives on cybersecurity education. There will be consequences for a nation's economy, culture, infrastructure, and people's safety if its digital information and communication technology is not easily accessible and used effectively. It is very important to safeguard a nation's cyber sovereignty from hostile parties. Cyber sovereignty and the growth of a robust cybersecurity ecosystem are both bolstered by adequate cybersecurity education, as this shows. This research examined the current situation of cybersecurity education and training enhancement initiatives and assessed a number of top-tier NCSPs. Achieving national cybersecurity strategic objectives may be facilitated by incorporating the Goal-Question-Outcomes (GQO)+Strategies paradigm into cybersecurity education and training programs. Utilizing the NICE Framework, the proposal establishes a connection between cybersecurity strategic objectives and cybersecurity competences. New cybersecurity education and training programs are based on the GQO+Strategies paradigm, which has three primary strategic goals: (1) ensuring the security of digital and IT infrastructure and services; (2) protecting critical infrastructure from sophisticated cyber threats; and (3) enhancing individuals' cybersecurity knowledge and abilities.

Collectively, the studies that were evaluated shed light on several facets of cybersecurity, such as training, risk management, policy formulation, and technology adoption. Nevertheless, the comprehension of the direct impact of these cybersecurity measures on the effectiveness of international relations is noticeably lacking. Additional study is necessary to delve into certain strategic cybersecurity approaches, identify moderating variables, and assess their impact on improving international relations from a BSC perspective. Strong cybersecurity measures that enhance organizational performance and international collaboration may be achieved via the findings of this study, which might be useful for firms functioning in a globalized setting.

METHODOLOGY

This research used a mixed-methods strategy, combining quantitative and qualitative techniques. Quantitative and qualitative methods were used in this study's descriptive and correlational research design. Research variables in correlational studies were the relationships between the elements under investigation.

The study's population consisted of 229 employees, stakeholders of Broadband Systems Corporation (BSC), including company officials, cybersecurity staff and beneficiaries. The sample size was determined with the help of Slovin's formula. Researcher used stratified sampling 146. The population was divided into groups based on each person's role within BSC. Each study goal was investigated with detailed inquiries to ensure a successful conclusion. Questionnaire sources were used to collect information for the study. Social Science Statistical Package (SPSS) 25 was used in the study.

FINDINGS AND DISCUSSIONS

Response Rates

The study presented the questionnaire's response rate at Broadband Systems Corporation, showing that out of 146 distributed questionnaires, 131 were completed, representing a high response rate of 89.7%, while 15 remained unreturned, accounting for 10.3%. This strong engagement among participants indicates a willingness to share insights regarding cybersecurity practices and their effects on international relations performance. Such a high response rate enhances the reliability and validity of the data collected, thereby strengthening the findings and conclusions of the study on cybersecurity practices at Broadband Systems Corporation.

Inferential Statistics for Hypotheses Test

The objective of inferential statistics is to derive inferences from a statistical sample. Correlation analysis, hypothesis testing, confidence intervals, and regression analysis exemplify methods used in inferential statistics.

Table 1: Correlations

		International relations performance	Cybersecurity policies	Cybersecurity training	Cybersecurity technology
International relations performance	Pearson Correlation	1	.711**	.722**	.762**
	Sig. (2-tailed)		.000	.000	.000
	N	131	131	131	131
Cybersecurity policies	Pearson Correlation	.711**	1	.499**	.548**
	Sig. (2-tailed)	.000		.000	.000
	N	131	131	131	131
Cybersecurity training	Pearson Correlation	.722**	.499**	1	.586**
	Sig. (2-tailed)	.000	.000		.000
	N	131	131	131	131
Cybersecurity technology	Pearson Correlation	.762**	.548**	.586**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	131	131	131	131

**. Correlation is significant at the 0.01 level (2-tailed).

Table 1 presents the correlation analysis between international relations performance and the three cybersecurity variables: cybersecurity policies, cybersecurity training, and cybersecurity technology. The results indicate that the correlation between international relations performance and cybersecurity policies is strong (r = .711, p < .001), indicating that stronger cybersecurity policies positively influence international relations performance. Additionally, cybersecurity training shows a strong positive correlation with international relations performance (r = .722, p < .001), highlighting that enhanced training significantly improves diplomatic outcomes. Finally, the correlation between cybersecurity technology and international relations performance is the strongest (r = .762, p < .001), showing the crucial role of technology in enhancing international engagements.

All correlations are statistically significant at the 0.05 level, reinforcing the significance of these cybersecurity factors in promoting effective international relations. A study conducted by Hasani *et al.* (2023) examined the impact of cybersecurity adoption on organizational performance. An analysis of the model was conducted using structural equation modeling, which is a component of SPSS, a social science statistical program. The research confirms the significance of eight variables that influence cybersecurity adoption by SMEs and identifies them. Organizational performance is favorably affected by cybersecurity technology adoption.

The findings are consistent with Abdel (2023), who stresses the importance of robust cybersecurity measures for organizational resilience in unpredictable markets. The strong correlations between international relations performance and cybersecurity policies, training, and technology underscore the necessity for organizations like BSC to enhance their cybersecurity frameworks. By learning from cyber incidents and strengthening these measures, BSC can protect vital data and maintain smooth operations, ultimately fostering successful international engagements.

Table 2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.877[a]	.770	.764	.12959

a. Predictors: (Constant), Cybersecurity technology, Cybersecurity policies, Cybersecurity training

Table 2 presents the model summary for the regression analysis conducted to assess the impact of cybersecurity technology, cybersecurity policies, and cybersecurity training on international relations performance.

The model shows a strong correlation (R = .877), indicating a strong relationship between the predictors and the dependent variable. The R Square value of .770 indicate that approximately 77.0% of the variance in international relations performance can be explained by the combined influence of the three predictors. The adjusted R Square value of .764 indicates a slightly lower estimate, accounting for the number of predictors in the model, and reflects a good fit.

Overall, these findings indicate that cybersecurity factors significantly contribute to enhancing international relations performance in Rwanda. Cremer *et al.* (2022) investigated cyber risk and cybersecurity. Cybercrime increased its global economic effect by about 50% between 2018 and 2020, Based on research findings, stakeholders dealing with cyber risk have a major hurdle in the shape of inadequate data. The data categorization and evaluation findings could help cybersecurity researchers and the insurance industry better understand, measure, and control cyber threats.

The findings align with Ukhanova (2022), who emphasizes the importance of cybersecurity in protecting technological advancements and economic stability in Japan. Similar to Japan's proactive approach to cyber threats, BSC's strong correlation indicates that effective cybersecurity technology, policies, and training are crucial for enhancing international relations performance in Rwanda. These elements not only mitigate risks but also foster strategic collaborations and support economic resilience in the international arena.

Table 3: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.133	3	2.378	141.583	.000[b]
	Residual	2.133	127	.017		
	Total	**9.265**	**130**			

a. Dependent Variable: International relations performance
b. Predictors: (Constant), Cybersecurity technology, Cybersecurity policies, Cybersecurity training

Table 3 presents the ANOVA results for the regression analysis. The F-value is 141.583, which indicates a highly significant model fit. The significance level (Sig.) is .000, demonstrating that the predictors cybersecurity technology, cybersecurity policies, and cybersecurity training significantly contribute to explaining variations in international relations performance. As per Kam *et al.* (2022), this is intriguing: The role of interest theory and self-determination in cybersecurity training inside organizations is being investigated. This study provides valuable insights into workplace information security awareness training, which aims to reduce data breaches via behavioral alterations. It incorporates user exposure, stringency of coercion, and response to threat into behavior prediction discretions.

The findings are supported by Hassan *et al.* (2024), who emphasize that Nigeria's proactive measures against cyber threats significantly enhance its international relations. They argue that effective cybersecurity regulations, such as the Nigerian Cybercrime Act and NITDA's data protection standards, not only address pressing digital challenges but also improve the country's ability to attract foreign investment. This aligns with the observed positive contributions of cybersecurity factors to international relations performance in the context of BSC.

Table 4: Coefficients

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	.363	.196		1.850	.067
	Cybersecurity policies	.280	.044	.335	6.358	.000
	Cybersecurity training	.288	.048	.328	6.029	.000
	Cybersecurity technology	.357	.052	.386	6.844	.000

a. Dependent Variable: International relations performance

The model used in the study can be represented by the following equation:

$$Y=\beta_0+\beta_1X_1+\beta_2X_2+\beta_3X_3+\epsilon$$

Where:

International Relations Performance = 0.363 + 0.280 (Cybersecurity Policies) + 0.288 (Cybersecurity Training) + 0.357 (Cybersecurity Technology).

Table 4 presents the coefficients that provide insights into the relationships between the predictors (cybersecurity policies, cybersecurity training, and cybersecurity technology) and the dependent variable (international relations performance) in the context of Rwanda.

The constant term (α) is 0.363, indicating the expected level of international relations performance when all cybersecurity practices are at zero. The unstandardized coefficients (B) demonstrate how international relations performance changes for each unit increase in the corresponding predictor while controlling for other variables.

Cybersecurity policies have a coefficient of 0.280, indicating that a one-unit increase in cybersecurity policies corresponds to a 0.280 improvement in international relations performance. Cybersecurity training shows a coefficient of 0.288, highlighting that a one-unit increase leads to a 0.288 enhancement in international relations performance, highlighting its significant contribution. Cybersecurity technology exhibits a coefficient of 0.357, signifying that a one-unit increase results in a 0.357 improvement in international relations performance, emphasizing the importance of technology in the field.

All predictors have statistically significant p-values ($p = .000 < 0.05$), confirming their individual impact on international relations performance. These results indicate the essential role of cybersecurity policies, training, and technology in enhancing international relations performance in Rwanda. Chitadze (2023) states that cybersecurity is the process of preventing the loss, misuse, or change of data, computer systems, and networks. Antivirus software, firewalls, and encryption techniques are all part of this larger security framework, which aims to protect sensitive data and keep digital systems running smoothly in the face of cyber dangers like phishing and malware.

The findings are supported by Mwangi *et al.* (2022), who assert that robust cybersecurity measures are essential for Kenya to safeguard its growing digital economy and enhance international relations. They highlight the role of institutions like the Communications Authority of Kenya in addressing significant cyber threats, including attacks on critical infrastructure and data breaches. This aligns with the observed positive impact of cybersecurity policies, training, and technology on international relations performance in Rwanda, indicating the universal importance of effective cybersecurity strategies for enhancing global connections.

Limitations

The study relies on a sample size of 131, which limited the generalizability of the findings. If the sample is not representative of the broader population or includes biases in selection, it affected the accuracy of the inferences. The study's context, focusing on Rwanda is not directly applicable to other countries with different cultural, economic, and technological landscapes, thus limiting the applicability of the results in a global context.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

This research aimed to investigate the influence of cybersecurity practices on enhancing international relations performance in Rwanda, particularly through the implementation of cybersecurity policies, technologies, and training at the BSC. The study focused on three areas: cybersecurity policies, cybersecurity technology, and cybersecurity training. Results indicated a strong consensus among respondents regarding the significance of these practices in bolstering diplomatic efforts.

Respondents strongly agreed that cybersecurity policies play a pivotal role in enhancing diplomatic meetings with international stakeholders. Effective access control policies were identified as crucial for securing sensitive information, fostering trust among parties involved. This highlights the necessity of robust cybersecurity frameworks for facilitating open communication and ensuring that diplomatic engagements are not compromised by cyber threats.

Findings related to cybersecurity technology were equally promising. Participants agreed that implementing advanced technologies significantly improves the negotiation and execution of trade agreements with international partners. Respondents highlighted the effectiveness of disturbance detection systems and encryption tools in protecting sensitive data, underscoring the view that investing in cybersecurity technology mitigates risks while enhancing the efficacy of international collaboration.

Cybersecurity training also emerged as critical, with respondents strongly endorsing initiatives such as phishing awareness and incident simulation exercises. Participants noted that these programs enhance employees' abilities to recognize and respond to cyber threats, strengthening the organization's capacity to maintain effective international relations. Insights from training contribute to a proactive approach in safeguarding diplomatic communications.

Regarding the impact of cybersecurity practices on international relations performance, findings provide evidence to reject the null hypothesis (p-values < 0.005). Results demonstrated a strong positive correlation between cybersecurity regulations and diplomatic ties. Furthermore, the significant role of cybersecurity technology in boosting trade agreements was confirmed, alongside the effectiveness of training programs in supporting meaningful connections with global stakeholders.

Recommendations

BSC is advised to develop incident response protocols that outline steps for managing cyber incidents effectively.

BSC should conduct regular reviews and updates of cybersecurity policies to adapt to evolving threats and technological changes.

BSC is advised to utilize strong encryption tools for protecting sensitive data during diplomatic negotiations and communications.

BSC should adopt multi-factor authentication (MFA) for all access to sensitive systems and data to enhance security.

BSC should implement continuous cybersecurity awareness training to help employees recognize and respond to common cyber threats.

Researchers in the future should look into how cybersecurity policy, technology adoption rates, employee training programs, incident response preparedness, stakeholder collaboration, and public awareness campaigns affect international cooperation in order to better understand how cybersecurity practices at Broadband Systems Corporation (BSC) improve international relations.

REFERENCES

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology,* 7(1), 138-158.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754.

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, 11(1), 1304-1310.

Barron, E. N. (2024). *Game theory: an introduction*. John Wiley & Sons.

Chitadze, N. (2023). Basic Principles of Information and Cyber Security. *In Analyzing New Forms of Social Disorders in Modern Virtual Environments* (pp. 193-223). IGI Global.

Comparitech. (2024, April). Data breaches: Statistics by location. Retrieved from https://techjury.net/blog/data-breach-statistics/

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Papers on Risk and Insurance - Issues and Practice,* 47(3), 698-736.

Harvey, J. F., Bresman, H., Edmondson, A. C., & Pisano, G. P. (2022). A strategic view of team learning in organizations. *Academy of Management Annals*, 16(2), 476-507.

Hasani, T., O'Reilly, N., Dehghantanha, A., *et al.* (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics,* 3, 97.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal, 5*(1), 41-59.

Huang, Y., & Zhu, Q. (2022). Game-theoretic frameworks for epidemic spreading and human decision-making: A review. *Dynamic Games and Applications*, 12(1), 7-48.

Kala, E. S. M. (2023). Critical role of cyber security in global economy. *Open Journal of Safety Science and Technology*, 13(4).

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, 32(4), 888-926.

Khan, W. M., & Padhy, D. (2022). Cybersecurity, international relations and India's foreign policy - Historical perspective and prospects. *International Journal of Scientific Development and Research (IJSDR),* 7(7), 488.

Leng, Y., Dong, X., Moro, E., & Pentland, A. (2024). Long-range social influence in phone communication networks on offline adoption decisions. *Information Systems Research,* 35(1), 318-338.

Mbatha, B. (2024). *Diffusion of Innovations: How Adoption of New Technology Spreads in Society*. In Information, Knowledge, and Technology for Teaching and Research in Africa: Human Machine Interaction and User Interfaces (pp. 1-18). Cham: Springer Nature Switzerland.

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems*, 33(2), 200-220.

Nujen, B. B., Kvadsheim, N. P., Mwesiumo, D., Reke, E., & Powell, D. (2023). Knowledge obstacles when transitioning towards circular economy: an industrial intra-organisational perspective. *International Journal of Production Research*, 61(24), 8618-8633.

Peschl, M. F. (2023). Learning from the future as a novel paradigm for integrating organizational learning and innovation. *The Learning Organization*, 30(1), 6-22.

Putteeraj, M., Bhungee, N., Somanah, J., & Moty, N. (2022). Assessing E-Health adoption readiness using diffusion of innovation theory and the role mediated by each adopter's category in a Mauritian context. *International Health*, 14(3), 236-249.

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology, 1*–51.

Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*, 1-12.

Sophos. (2024, May). The State of Phishing in Q1 2024. Retrieved from https://www.sophos.com/en-us/products/phish-threat

Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. In SHS Web of Conferences (Vol. 134, p. 00159). EDP Sciences.

Von Stein zu Nord-und Ostheim, H. F. (2022). The UKUSA Agreement: The History of an Enduring Relationship (Doctoral dissertation).

Weiss, U., & Agassi, J. (2023). Game Theory and Social Science. In Games to Play and Games not to Play: Strategic Decisions via Extensions of Game Theory (pp. 61-83). Cham: Springer Nature Switzerland.