MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Survey of Cyber Security in Fiji: Policy Creation & Implementation

Autor: Luis de la Mata Sánchez - Izquierdo

Director: Maurice Dawson

Madrid

I declare, under my own responsibility, that the Project submitted with the title

Survey of Cyber Security in Fiji: Policy Creation & Implementation carried out at the ICAI School of Engineering – Universidad Pontificia Comillas during the academic year 2024/2025 is my own work, original and unpublished, and has not been submitted previously for any other purpose.

The Project is not, either wholly or partially, a plagiarism of another work, and all information taken from other documents is properly referenced.

Luis de la Mata

Signed.: Luis de la Mata Date: 01/ 06/ 2025

Authorization for the submission of the project

PROJECT SUPERVISOR

Signed.: Maurice Dawson Date: 15/06/2025

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Luis de la Mata Sánchez-Izquierdo

DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Survey of Cyber Security in Fiji: Policy Creation & Implementation, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción

de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 13. de junio de 2025

ACEPTA

Fdo Luis de la Mata

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Survey of Cyber Security in Fiji: Policy Creation & Implementation

Autor: Luis de la Mata Sánchez-Izquierdo

Director: Maurice Dawson

Madrid

SURVEY OF CYBER SECURITY IN FIJI: POLICY CREATION & IMPLEMENTATION

Autor: de la Mata Sánchez-Izquierdo, Luis**.**
Director: Dawson, Maurice.
Entidad Colaboradora: Illinois Institute of Technology

RESUMEN DEL PROYECTO

Este proyecto trata de realizar un análisis acerca de la situación actual en cuanto al desarrollo de la inteligencia artificial y la ciberseguridad en un país en plena transformación digital, en concreto Fiji. A lo largo de este documento se hacen recomendaciones para enfrentar los diferentes retos a los que se enfrenta el país.

Palabras clave: Fiji, Ciberseguridad, IA, Políticas, Desarrollo, Dashboard, Educación, Panorama de Amenazas

1. Introducción

Tras varias conversaciones del Dr. Dawson con ciudadanos de las islas Fiji, se identificaron varios sectores del país donde no había un entorno adecuado para desarrollar actividades relacionadas con la inteligencia artificial o la ciberseguridad. Además, siendo Fiji un país que está atravesando una rápida transformación digital, se presentan continuamente nuevas oportunidades y amenazas que deben ser gestionadas.

Una de las principales oportunidades que se presenta es el uso de la inteligencia artificial para mejorar la productividad en diversos sistemas incluida la propia ciberseguridad. Sin embargo, el principal reto al que debe enfrentarse el país actualmente es el creciente número de ciberataques que esta recibiendo. Una legislación incompleta, la escasez de trabajadores cualificados y falta de acuerdos entre sectores en el país han sido la motivación para desarrollar este proyecto, el cual pretende analizar de forma integral el estado actual de la ciberseguridad y la adopción de IA en Fiji, proponiendo medidas concretas para potenciar el desarrollo digital del país a través de un entorno seguro.

2. Definición del proyecto

Como ya ha sido mencionado anteriormente, este proyecto trata la situación actual de la inteligencia artificial y la ciberseguridad en Fiji. Un país que ha dado sus primeros pasos en estos campos con regulaciones como el Cybercrime Act 2021 [1], pero aún carece de las herramientas necesarias para enfrentar los retos que llegarán al país en los próximos años.

Con el fin de mostrar las herramientas mencionadas, este proyecto ha identificado a lo largo de una serie de capítulos, en un formato parecido a un libro, las fortalezas y debilidades de Fiji para afrontar las oportunidades y desafíos que trae consigo la IA y la ciberseguridad. A través de estas fortalezas y debilidades además de ejemplos de otros países, se han realizado varias recomendaciones que pueden servir al país para asegurar un desarrollo optimo de todas las medidas necesarias para lograr un entorno digital seguro e innovador.

Por último, se ha desarrollado una herramienta estilo “dashboard”, que permite a cualquier usuario visualizar y entender de forma rápida la situación actual de Fiji, incluyendo los retos y oportunidades a los que está sometido y las acciones recomendadas para enfrentarlos.

3. Descripción de la herramienta de Dashboards

Como ya se ha mencionado, como parte de este proyecto se ha desarrollado una herramienta con un esquema similar al mostrado en la Figure 1, donde se puede escoger entre diferentes pestañas en las cuales habrá una serie de gráficos y información adicional que servirá para explicar un tema en concreto.

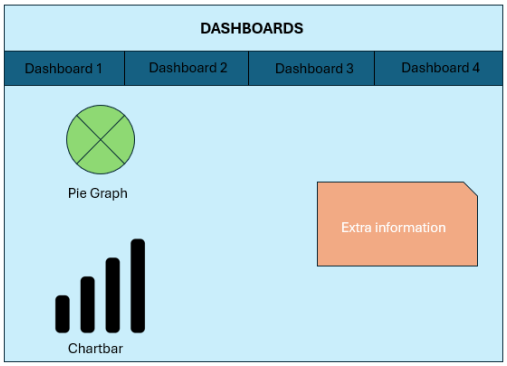

Figure 1. Dahsboards Draft

En la Figure 2, se muestra un ejemplo real de la aplicación sobre una sección de los dashboards diseñados.

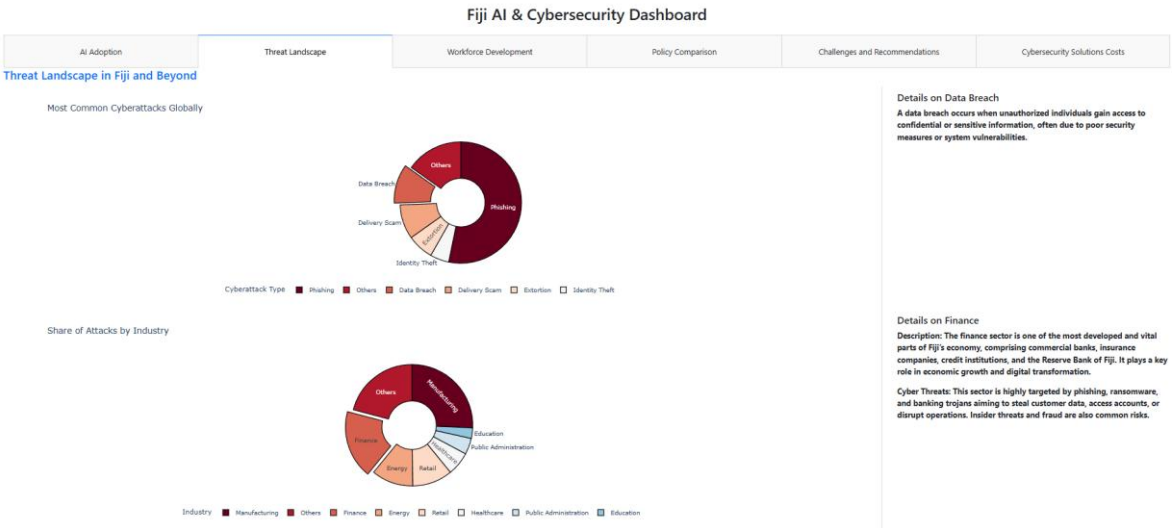

Figure 2. Dashboards Preview

4. Resultados

Los resultados del proyecto consisten en tanto la identificación de las oportunidades y dificultades a las que se enfrenta Fiji, como las recomendaciones que se realizan para

enfrentarse a ellas. Entre las recomendaciones destacan: la necesidad de desarrollar la regulación pertinente que sirva de guía para implementar ciberseguridad en las infraestructuras críticas partiendo de ejemplos como el NIST [2], desarrollar colaboraciones entre el sector de educación y sectores profesionales para aumentar el conocimiento de ciberseguridad medio de la población y ayudar a incrementar la capacidad técnica en dicho aspecto de los profesionales del futuro. En la Figure 3, se puede observar algunas de estas recomendaciones en el dashboard realizado.

Figure 3. Recommendations Overview

5. Conclusiones

Fiji se encuentra en un momento critico de su transformación digital. El desarrollo de tecnologías innovadoras como la inteligencia artificial sostenidas por un entorno seguro son la clave para ser referentes en innovación y seguridad en la región. Es por ello que medidas para aumentar el número de profesionales especializados en ciberseguridad, construir un marco normativo que abarque de forma completa todos los sectores y necesidades y aumentar el conocimiento acerca de la ciberseguridad en el país, resultan vitales para los próximos años.

6. Referencias

[1] VFiji Government. (2021). *Fiji Cybercrime Act 2021* [Statutory instrument]. Retrieved September 8, 2025, from https://www.fiji.gov.fj

[2] National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

SURVEY OF CYBER SECURITY IN FIJI: POLICY CREATION & IMPLEMENTATION

Author: de la Mata Sánchez-Izquierdo, Luis.
Supervisor: Dawson. Maurice.
Collaborating Entity: Illinois Institute of Technology

ABSTRACT

This project seeks to conduct an analysis about the current situation regarding the development of artificial intelligence and cybersecurity in a developing country, specifically Fiji. Throughout this paper, recommendations are made to address the various challenges facing the country.

Keywords: Fiji, Cybersecurity, AI, Policies, Development, Dashboard, Education, Threat Landscape

1. Introduction

Following several discussions by Dr. Dawson with citizens of the Fiji Islands, several sectors of the country were identified where there was not a suitable environment to develop activities related to artificial intelligence or cybersecurity. In addition, with Fiji being a country undergoing a rapid digital transformation, new opportunities and threats are continually presenting themselves that need to be addressed.

One of the main opportunities presented is the use of artificial intelligence to improve productivity in various systems including cybersecurity itself. However, the main challenge that the country must currently face is the increasing number of cyber-attacks it is receiving. Incomplete legislation, a shortage of skilled workers and a lack of agreements between sectors in the country have been the motivation to develop this project, which aims to comprehensively analyze the current state of cybersecurity and the adoption of AI in Fiji, proposing concrete measures to enhance the country's digital development in a secure environment.

2. Project Definition

As mentioned above, this project addresses the current situation of artificial intelligence and cybersecurity in Fiji. A country that has taken its first steps in these fields with regulations such as the Cybercrime Act 2021 [1] but still lacks the necessary tools to face the challenges that will come to the country in the coming years.

In order to showcase the mentioned tools, this project has identified over a series of chapters, in a book-like format, Fiji's strengths and weaknesses in addressing the opportunities and challenges that AI and cybersecurity bring. Through these strengths and weaknesses in addition to examples from other countries, a number of recommendations have been made that can serve the country to ensure optimal development of all measures necessary to achieve a secure and innovative digital environment.

Finally, a “dashboard” style tool has been developed, which allows any user to quickly visualize and understand Fiji's current situation, including the challenges and opportunities it is facing and the recommended actions to address them.

3. Dashboards Application

As already mentioned, as part of this project a tool has been developed with a scheme similar to the one shown in Figure 1, where you can choose between different tabs in which there will be a series of graphs and additional information that will serve to explain a particular topic.

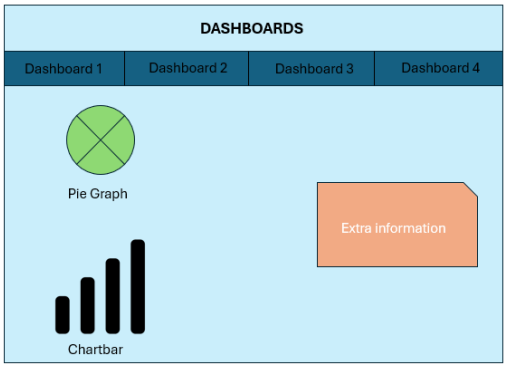

Figure 4. Dahsboards Draft

Figure 2 shows a real example of the application on a section of the dashboards designed.

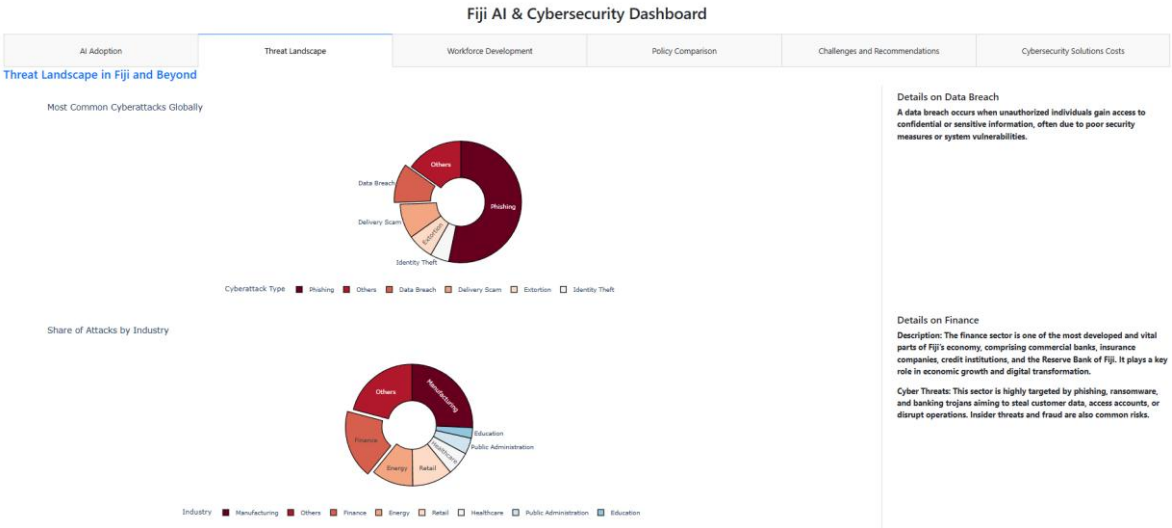

Figure 5. Dashboards Preview

4. Results

The results of the project consist of both the identification of the opportunities and challenges facing Fiji and the recommendations made to address them. Among the recommendations are: the need to develop relevant regulation to guide the

implementation of cybersecurity in topics such as critical infrastructures based on examples such as NIST [2], develop collaborations between the education and professional sectors to increase the average population's knowledge of cybersecurity, and help increase the technical capacity of future professionals in this area. In Figure 3, some of these recommendations can be seen in the dashboard.

Figure 6. Recommendations Overview

5. Conclusions

Fiji is at a critical point in its digital transformation. The development of innovative technologies such as artificial intelligence supported by a secure environment is the key to being a leader in innovation and security in the region. This is why measures to increase the number of cybersecurity professionals, build a regulatory framework that comprehensively covers all sectors and needs, and increase awareness of cybersecurity in the country are vital for the coming years.

6. Citations

[1] VFiji Government. (2021). *Fiji Cybercrime Act 2021* [Statutory instrument]. Retrieved September 8, 2025, from https://www.fiji.gov.fj

[2] National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Memory Index

Figure Index

SECTION 1 INTRODUCTION

The pacific islands, including Fiji, right now are in an ongoing development process where digital transformation has a critical role to play, AI if well used can cause a great impact for the country development. However, in recent years, cyberattacks have become a more relevant issue, affecting everything from personal data to critical infrastructure. With these threats becoming more sophisticated, it's essential for businesses and government entities to adopt strong security measures to protect against potential risks.

AI plays a critical role in both improving cybersecurity and creating new challenges. On one hand, AI can enhance security by automating threat detection, improving response times, and helping to identify vulnerabilities before they're exploited. On the other hand, as reliance on AI grows, so does the risk of malicious actors using AI for cyberattacks. This dual nature of AI can be dangerous, and it is essential to ensure that the benefits outweigh the risks.

This project will investigate how AI is being adopted across Fiji's public and private sectors, identifying both the successes and the challenges. It will also examine the current state of cybersecurity in the country, including the most relevant threats and vulnerabilities. Additionally, we'll review the existing regulatory frameworks regarding AI and cybersecurity and discuss the growing need for skilled workers in the field. By examining these topics, the project will provide valuable insights and recommendations for stakeholders to help create a safer and more secure digital future for Fiji.

1.1 PROJECT MOTIVATION

As previously stated, pacific islands had received recently persistent cyberattacks, most notably those orchestrated by a state-sponsored Chinese group have exposed significant vulnerabilities in both public and private institutions. Currently the country has an

underdeveloped cybersecurity workforce, leaving the country less prepared to counter these sophisticated threats. At the same time, private and public companies are starting to use artificial intelligence to enhance their services, including cybersecurity in some cases. These initiatives, are an example on how AI can automate threat detection, predict potential breaches, and automatize incident responses capabilities that are already transforming cybersecurity on the global stage.

Worldwide, nations with advanced technological infrastructures have established comprehensive AI and cybersecurity frameworks that set clear standards and guidelines, ensuring robust protection against emerging digital threats. In contrast, Fiji's current regulatory environment reveals critical gaps. While there is an existing cybersecurity framework, it lacks the depth needed to address modern challenges, and there is no dedicated policy for AI integration. This lack of regulatory frameworks and the need for more skilled professionals emphasizes the urgent need for innovative solutions. The motivation for this project is clear: to address Fiji current challenges regarding cybersecurity, especially because of the recent attacks that the region has received that could prevent it to continue its digital development which has been stated as a priority by the national development plan in the following years. Through a comprehensive analysis of the threat landscape, existing frameworks, and real-world applications of AI in cybersecurity, this project seeks to provide actionable recommendations. These insights are intended to guide policymakers, industry leaders, and educators in building a resilient, future-proof digital ecosystem in Fiji.

SECTION 2 TECHNOLOGIES DESCRIPTION

For the development of interactive dashboards, we will utilize Python Dash, a powerful open-source framework designed specifically for building analytical web applications with Python. Dash is built on top of Flask, Plotly.js, and React.js, allowing for the creation of highly interactive and customizable user interfaces.

To enhance the visual design and responsiveness of the dashboards, the Dash Bootstrap Components module will also be integrated. This module provides a suite of pre-built components styled with Bootstrap, one of the most widely used front-end frameworks. It allows for easier layout management and professional-looking UI elements, ensuring consistent user experience.

Together, Dash and Bootstrap enable rapid development of clean, functional, and visually appealing dashboards that are easy to maintain and extend.

SECTION 3 STATE OF THE ART

This section surveys existing research and institutional efforts in Fiji related to artificial intelligence (AI), cybersecurity, and their intersection, identifying key themes and gaps that frame the foundation for this project.

3.1 AI RESEARCH IN FIJI

Artificial intelligence has only recently begun to enter policy and academic discourse in Fiji. Most AI-related activity comes from international development initiatives rather than domestic research programs. Notably, the Fiji Digital Government Transformation Project [76], supported by the World Bank, mentions AI in the context of automating public services, though implementation remains limited.

AI's role in media and journalism is gaining traction. During a 2024 visit, Dr. Maurice Dawson engaged with journalism students at the University of the South Pacific (USP) to discuss AI's dual role in enabling and undermining news production. The group explored the use of AI for content generation, fact-checking, and audience analysis, while also examining threats such as misinformation and algorithmically amplified falsehoods. These early conversations demonstrate growing awareness of AI's potential and challenges, but research output in Fiji remains in its early stages. The country lacks a national AI strategy, formal AI governance frameworks, or substantial academic work in this domain.

3.2 CYBERSECURITY RESEARCH IN FIJI

Cybersecurity, while more developed than AI in terms of institutional attention, remains fragmented in both research and practice. However, as of 2025, there remains no comprehensive cybersecurity directive that spans all government levels or sectors, leaving businesses and institutions without clear operational guidelines.

Dr. Dawson's 2024 engagement with Fijian officials revealed widespread concern across sectors about the lack of standard cybersecurity policy implementation. Businesses, educators, and civil society groups have expressed a need for centralized guidance on network defense, digital hygiene, and cyber risk management. Additionally, online safety particularly concerning children's exposure to inappropriate content, has emerged as a significant societal concern.

3.3 INTERSECTION OF AI AND CYBERSECURITY

The intersection of AI and cybersecurity in Fiji remains largely unexplored in both research and practice. Dr. Dawson's visit highlighted this as a pressing frontier. As AI technologies become more accessible, their use in generating deepfakes, automated scams, and misinformation presents urgent cybersecurity implications. Yet these risks have not been formally addressed in Fiji's cybersecurity strategy or regulatory frameworks.

Moreover, while AI has clear potential for enhancing cybersecurity capabilities, there is currently little to non-documented use of AI-powered security tools in Fiji's public or private sectors. The security of AI systems themselves, including concerns over adversarial attacks and data poisoning, has not entered the national conversation.

3.4 GAPS

Several research and policy gaps have been identified:

- Absence of empirical studies on AI adoption and governance.
- Fragmented cybersecurity policy, lacking a nationwide operational framework.
- No formal research on the dual-use nature of AI in the Fijian context.
- Limited local technical capacity to evaluate or deploy AI and cybersecurity systems.
- Minimal integration of cybersecurity principles into digital transformation agendas.

SECTION 4 PROJECT DEFINITION

4.1 JUSTIFICATION

Fiji has not yet developed a comprehensive cybersecurity directive that applies across all levels of government and sectors. This absence of unified operational guidance leaves businesses, institutions, and civil society in a difficult position as they navigate an increasingly complex and vulnerable digital environment.

The importance of this project is highlighted by recent fieldwork and policy dialogues led by Dr. Maurice Dawson in 2024. During his engagement with Fijian government officials, students, journalists, and community leaders, several conversations emerged that reveal a deep and urgent need for applied, context-sensitive research. Government representatives voiced concern about gaps between policy intent and practical implementation, while students and educators highlighted the lack of clear pathways for building cybersecurity skills and integrating emerging technologies like artificial intelligence into existing frameworks. The rise in online safety issues was noted by multiple stakeholders as a new and concerning social development.

Equally important, Dr. Dawson's discussions at the University of the South Pacific drew attention to the growing presence of AI in the media landscape. Students and faculty acknowledged the opportunities AI offers in journalism and public communication, but also expressed concern about the threats it poses especially in the form of misinformation, deepfakes, and synthetic content. This dual-edged nature of AI demands a more sophisticated understanding of how digital technologies intersect with cybersecurity, public trust, and information integrity.

Moreover, conversations with young Fijians revealed growing economic anxieties and aspirations for migration to countries like Australia and New Zealand. These perspectives mirror trends observed in other developing nations and highlight a potential loss of digital

talent if domestic opportunities are not cultivated. This project responds to that concern by identifying areas for investment in human capital development.

Dr. Dawson's engagement with local communities, including Fijians, Samoans, and other Pacific Islanders, has contributed to a deeper understanding of regional values, priorities, and constraints. This positions the research to be not only analytically rigorous but also socially responsive and aligned with local aspirations.

4.2 GOAL OF THE PROJECT

The main goal of this project is to achieve a set of recommendations for Fiji regarding cybersecurity and AI giving it specific situation.

- Analysis of the current cybersecurity situation in the country including (workforce, infrastructure, use of AI, frameworks and threat landscape)
- Analysis of international AI and cybersecurity frameworks
- Research about the solutions that AI has achieved in cybersecurity around the world
- Provide the needed recommendations to Fiji in order to achieve a secure environment that allows innovation and digital development. According to frameworks, AI uses in cybersecurity, etc.
- Develop a dashboards site to show visually Fiji current AI and cybersecurity situation and some recommendations for the current challenges in those areas

4.3 WORK METHODOLOGY

The needed work for the project can be divided into 3 different groups of tasks, firstly the research about Fiji current situation regarding AI and cyber security, in this group the following topics will be researched: Cyber Security Threat Landscape in Fiji, Regulatory and Policy Frameworks, Cyber Security Education and Workforce Development, AI in

Enhancing Cyber Security: Use Cases in Fiji, Collaboration and Partnerships and Challenges in Cyber Security Implementation. Once all of these topics were analyzed, a set of recommendations for the situation of the country were made. The last group of tasks includes all of the development of the different dashboards to represent in a more visual way all the work done, including the analysis of Fiji current situation and the recommendations for the future.

SECTION 5 FIJI CYBERSECURITY AND AI

In this section the main part of the project will be presented, this will include the analysis of Fiji current situation regarding AI and specially cybersecurity comparing it to other parts of the world. The analysis will be divided into chapters in a book-like structure where the last 2 chapters will contain actionable recommendations for the country's current situation in these fields.

5.1 INTRODUCTION TO AI AND CYBER SECURITY IN FIJI

5.1.1 INTRODUCTION

Fiji, akin to several undeveloped countries, is experiencing a substantial digital transition. The rising implementation of Artificial Intelligence and the escalating demand for cybersecurity are influencing the country's technical environment. Although AI offers improved efficiencies, automation, and creativity, cybersecurity issues present considerable obstacles, necessitating a balanced strategy for digital advancement.

The geographical position of Fiji is significant, as it serves as a leader in the South Pacific region. Numerous technology governance policies are being borrowed from Australia and New Zealand due to geographical proximity and historical colonial influence. The United States maintains a presence on the island, where the US Embassy and the United States Agency for International Development (USAID) are essential in influencing policy development and technological progress in recent years.

Digital technologies have made their way into a variety of Fijian industries over the course of the last ten years, including banking, healthcare, tourism, and governance, among others. According to the United States Agency for International Development (USAID), the Digital Ecosystem Country Assessment [1] highlights the fact that Fiji's digital ecosystem is rapidly evolving, with increasing internet penetration and digital services. Furthermore, as stated in

the Fiji National Development Plan [2], the intention for the following years is to continue investing in digital service in order to grow as a nation. Nevertheless, the development is being slowed down by obstacles like inadequate infrastructure, concerns associated with cybersecurity, and a digital skills gap in the workforce that is currently in practice. A vision to promote digital governance and cybersecurity is outlined in the previously described strategy. This approach acknowledges the significant role that cybersecurity plays in the advancement of the nation.

5.1.2 THE ROLE OF AI AND CYBERSECURITY IN FIJI'S DIGITAL GROWTH

AI is gradually gaining traction in a variety of industries, including finance, healthcare, and government. While AI is not widely used in Fiji, there is growing interest in deploying AI-powered technologies to improve public and private sector services. Airlines, for example, are beginning to use AI technology to improve operational efficiency, while the tourism industry is investigating AI-powered chatbots to improve visitor experiences. Natural disaster recovery uses AI to analyze property damage and restore livelihoods as quickly as possible.

However, as digital infrastructure increases, the cybersecurity landscape presents new vulnerabilities. Cyberattacks on businesses and government entities have exposed flaws in Fiji's digital infrastructure. Small firms, which typically lack adequate security processes, are especially vulnerable to phishing assaults and ransomware outbreaks, the number of which is increasing year after year. With the rise of cyber dangers, improving security systems has become a national priority.

5.1.3 CURRENT LANDSCAPE OF AI IN FIJI

Several Fijian businesses have begun artificial intelligence-related projects. An increasing number of companies recognize the significance of artificial intelligence data analytics and automation solutions, particularly in customer service and operational efficiency. The use of AI for risk assessment and fraud detection is also being investigated by providers of

financial services. This is especially true for large corporations like Vodafone Fiji, which has begun offering this service.

Although considerable improvements have been made, the progress of artificial intelligence is still being hindered by several problems, including a shortage of specialized personnel, restrictions in infrastructure, and budgetary restraints. Because most AI solutions in Fiji are imported rather than developed domestically, the country's capacity to fully integrate and tailor AI technologies to its specific requirements is severely constrained.

The utilization of artificial intelligence also generates concerns regarding ethical issues and data safety. There is a need for a thorough assessment of the possible hazards of misuse and prejudice in artificial intelligence systems without a comprehensive regulatory framework for AI. In addition, as artificial intelligence becomes increasingly integrated into decision-making processes, it will be vital to guarantee that AI models display openness and accountability to maintain public trust and confidence. These conversations will shape the direction of artificial intelligence development in the US, even though they are still in the preliminary phases.

5.1.4 CYBERSECURITY CHALLENGES AND EMERGING THREATS

Cybersecurity dangers are increasing as the digital world expands. According to the Digital Ecosystem Country Assessment, Fiji is facing an increase in cyber dangers such as ransomware, data breaches, and fraud. The advent of e-commerce, online banking, and cloud computing has broadened the danger landscape, making cybersecurity a crucial priority for businesses and government institutions seeking to prevent financial losses.

For example, in recent years, cyberattacks on financial institutions and government agencies have exposed flaws in Fiji's digital infrastructure. Phishing scams and virus attacks have grown as more people and organizations rely on internet transactions. For example, a Fiji

Village article [3] revealed that a local company lost over US$500,000 as a result of a business email compromise scam, an incident that mirrors larger trends of revenue losses across the private sector, demonstrating that many businesses in the islands, particularly smaller ones, are still unprepared to deal with sophisticated cyber threats.

Fiji presents numerous challenges in developing a strong cybersecurity environment. A shortage of experienced personnel, antiquated IT infrastructure, and a lack of cybersecurity awareness across industries all contribute to the country's vulnerability. Furthermore, the country's current cybersecurity framework is insufficient to proactively battle specific cyberattacks, such as those affecting vital infrastructure, which are particularly dangerous and lacks a dedicated component. There is an urgent need to invest in security infrastructure, skill development, and policy design to solve these difficulties.

One of Fiji's most pressing cybersecurity challenges is a lack of public awareness and education about digital hazards. Many people and small organizations fail to adopt simple cybersecurity safeguards like multi-factor authentication and regular software upgrades, making them easy targets for fraudsters. Addressing these concerns would necessitate a nationwide push to increase cybersecurity education and awareness.

5.1.5 TRENDS SHAPING AI AND CYBERSECURITY IN FIJI

The Fijian government acknowledges the significance of artificial intelligence and cybersecurity, formulating policies and strategic plans to establish a more secure digital landscape. These efforts encompass a notable emphasis on cybersecurity as a priority within the National Development Plan for the upcoming years, alongside the establishment of a security framework known as the Cybercrime Act 2021 [4]. Although it may not be as thorough as frameworks from more developed nations, it represents a significant initial step toward advancing cybersecurity in the country.

Collaborations among government entities, private companies, and international organizations are facilitating investment and knowledge exchange in artificial intelligence

and cybersecurity. Businesses are increasingly collaborating with cybersecurity firms to improve their security frameworks and compliance standards.

Workforce development training initiatives and academic programs are being implemented to enhance AI and cybersecurity expertise within Fiji's workforce. Universities and technical institutions are enhancing their curricula to incorporate cybersecurity training and AI fundamentals, aiming to cultivate the next generation of digital professionals. Collaboration between government and private companies with universities is instrumental in achieving this objective.

The increasing focus on AI ethics and data security regulations is expected to result in more organized governance of digital innovation. Although regulations on data protection and cybersecurity are already in place, there is currently no national regulation addressing AI, highlighting an increasing need for such measures.

Organizations are increasingly investing in cybersecurity solutions, such as AI-driven security systems, cloud-based security services, and automated threat detection tools. This trend indicates a growing recognition of cybersecurity risks and the necessity for proactive security measures.

5.1.6 PUBLIC CONCERNS

Interviews and discussions with government officials, educators, and citizens revealed significant concerns regarding the state of the Internet for various reasons. A government office expressed concern regarding Internet safety and its impact on children in Fiji. Another individual expressed concern regarding the utilization of social media to provoke violence among various ethnic groups, as observed recently. Journalists expressed concerns regarding the potential for AI to supplant their roles and its implications for the dissemination of disinformation, as well as the resultant impact on the public. Nevertheless, the positive insights included the capacity to enhance essential roles that would remain unfilled as citizens sought employment in neighboring countries for higher wages. Consequently, government officials expressed concern regarding regulation and the sources

from which such regulations are adopted, including Europe, the US, or Australia. Some factions expressed concerns regarding the control of this technology and the training of the algorithms that would ultimately be deployed.

5.1.7 THE ROAD AHEAD

AI and cybersecurity are essential components of Fiji's digital future. AI has the potential to transform multiple industries; however, it is essential to implement strong cybersecurity measures to address the associated risks. Addressing infrastructure deficiencies, promoting local expertise, and formulating robust policies are essential for sustainable digital advancement.

The collaboration among government, private sector, and academia is essential for establishing a robust AI and cybersecurity framework as the country progresses in its technological development. The future of Fiji's digital landscape relies on a proactive strategy that harmonizes innovation with security, thereby establishing a secure and innovative technological ecosystem.

With the evolution of the digital landscape, Fiji has the potential to establish itself as a leader in AI-driven innovation and cybersecurity resilience in the Pacific region. The endeavor necessitates dedication, resources, and ongoing adjustment; however, with a well-defined strategic vision, Fiji has the potential to establish an innovative digital ecosystem utilizing AI while ensuring its future sustainability.

5.2 AI ADOPTION IN FIJI: OPPORTUNITIES AND CHALLENGES

5.2.1 PREFACE

As Fiji progresses towards the integration of artificial intelligence, both the public and business sectors are acknowledging the critical importance of AI technologies in the nation's ongoing digital advancement. The implementation of AI in Fiji has numerous benefits, although it also poses certain problems mostly attributable to the country's limited resources. This chapter examines the practical consequences of AI for public services and enterprises in Fiji, addressing both the benefits it presents and the challenges encountered throughout its implementation.

5.2.2 PROSPECTS

The Fijian government aims to advance AI within the nation to generate high-value employment and augment productivity across several sectors. This is a fundamental aspect of the National Development Plan as referenced in [5]. This plan emphasizes the intention to foster collaboration between the public and private sectors to formulate policies and strategies that promote research, development, and innovation. It also underscores the necessity of prioritizing artificial intelligence and comprehending its advantages. The government's assistance for the implementation of these technologies gives an opportunity for numerous firms to advance their digital ecosystems.

The inaugural instance of AI in Fiji is Limitless Marketing [6], a marketing firm established in 2022 that provides AI-driven customer support to its local clientele. This established a precedent for innovation and created an opportunity to enhance productivity in the customer service sector. Nonetheless, AI in Fiji presents numerous unexplored prospects, some of which are evident in other industries like manufacturing and agriculture. To enhance understanding of AI's influence on these sectors, its applications in these areas in other nations will be analyzed.

In contemporary nations, AI has been employed in numerous capacities to enhance agricultural productivity and minimize resource wastage. The enhancement in crop yields observed in other countries is approximately 30% [7-10]. To attain this enhancement, AI was implemented in various domains, specifically in the utilization of AI-guided robots and AI-driven precision agriculture methodologies. Each of these deployments influenced various aspects of the process.

- AI-assisted robots can decrease pesticide usage by 90%.
- AI-driven precision agriculture methods can diminish water waste by 50% and decrease fertilizer consumption by 20%.

Employing these strategies, either in entirety or partially, has been demonstrated to markedly enhance the efficiency of the agricultural sector.

The implementation of 'smart' factories in manufacturing has demonstrated a 30% enhancement in product quality alongside a 30% reduction in expenses compared to traditional factories [11]. The term 'smart' denotes the integration of AI with IoT and 5G to enhance the optimization of all operations involved. Estimating the precise improvement in productivity attributable to AI in the factory is challenging; however, it is evident that digital investment in manufacturing significantly influences the sector's economy, as illustrated in the subsequent graphic.

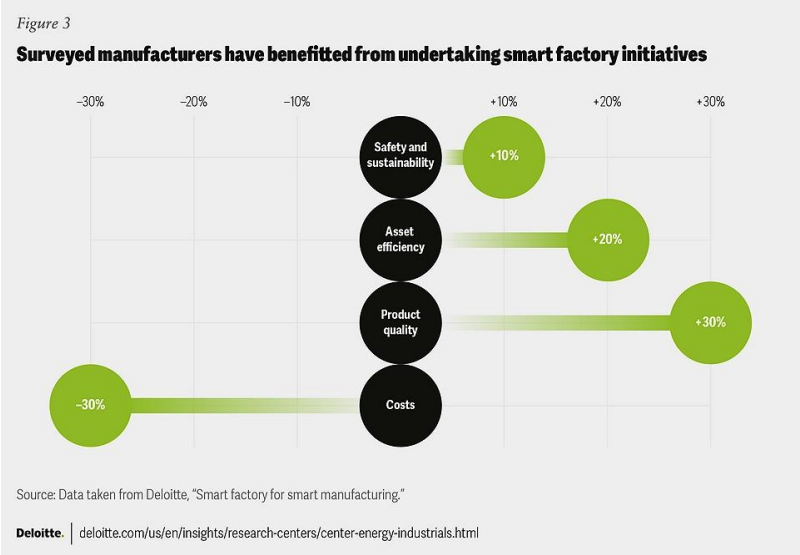

Figure 7. 'Smart' factory benefits [11]

In the realm of tourism, numerous aspects can be enhanced through the integration of modern AI technology. These three principal concepts would significantly impact the industry: Generative artificial intelligence specifically designed to provide personalized travel recommendations for the islands based on consumer preferences, budget, and past behavior.

Intelligent itineraries that include meteorological conditions, trip durations, or peak visitation times at prominent destinations. Utilize AI to improve demand forecasts for optimizing pricing in the hotel and airline industries. Implementing these concepts in the tourism sector would enhance both the consumer experience in Fiji and the advantages for the enterprises involved in the industry.

In Fiji, the aforementioned industries are the three most significant for the national economy, with tourism accounting for approximately 21% of GDP, while manufacturing and agriculture contribute 9.1% and 7.1%, respectively [12-13]. Enhancing each of these industries would significantly benefit the national economy.

Additionally, it is crucial to note Fiji's public sector and the potential of AI to augment its strengths. Numerous sectors within the public domain could benefit from the

implementation of AI for enhancement. Fiji is among the nations most adversely affected by natural disasters, and artificial intelligence can serve as a valuable tool to alleviate the impacts of these events. It can be utilized to forecast and categorize the damage inflicted by the disaster and can also aid in comprehending the logistics required for an efficient and rapid recovery post-disaster [15]. Cooperation is underway between the United Nations, Tractable, and Fiji to implement AI for this specific purpose [16]. The subsequent image visually illustrates how artificial intelligence can be employed to alleviate the effects of natural disasters.

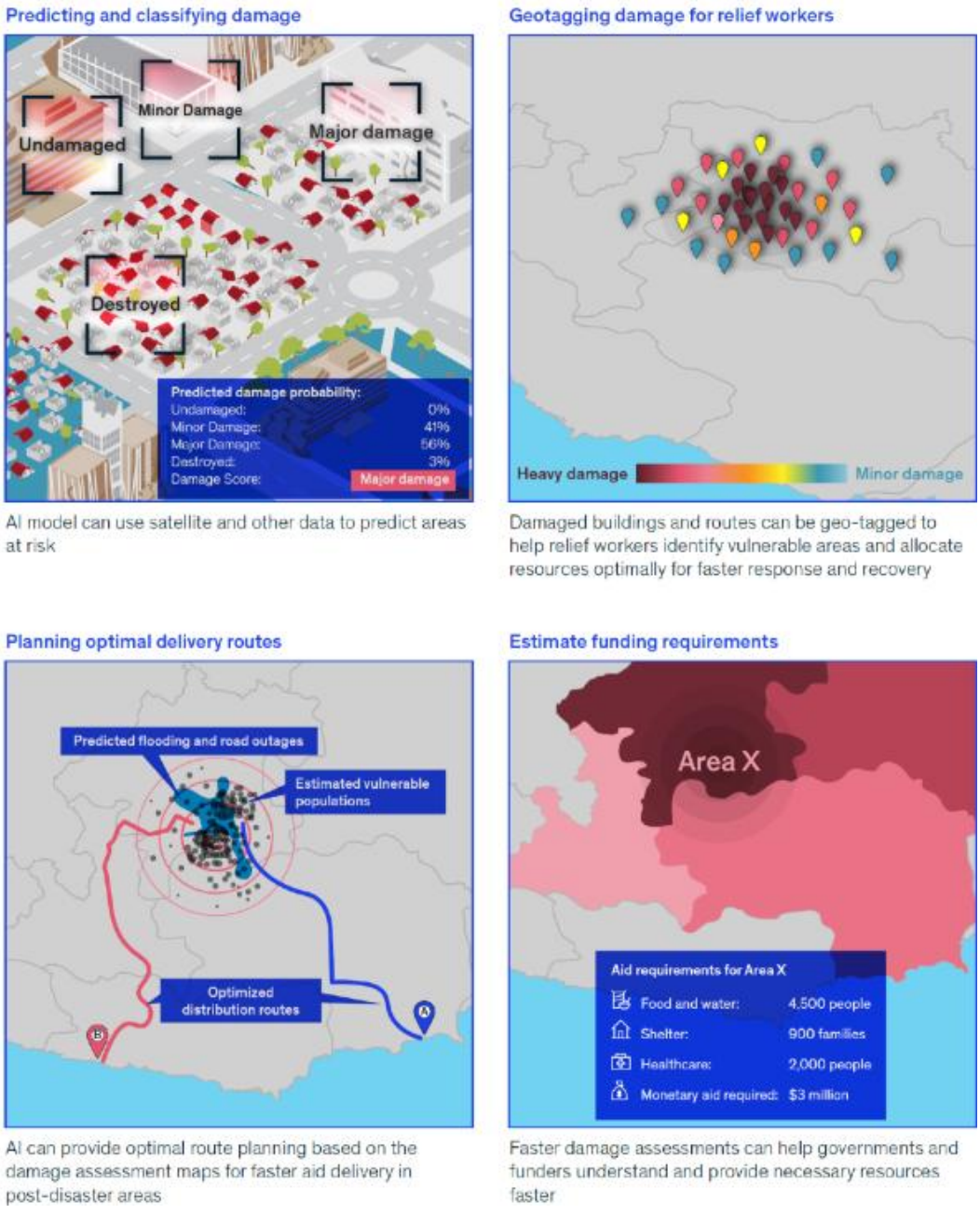

Figure 8.AI tools to mitigate Natural Disasters[16]

Other areas within the public sector of Fiji, such as public health or resource management in government operations, include those that could potentially benefit from the application of artificial intelligence. When it comes to public health, AI presents a multitude of options.

These potentials range from the prediction of the spread of a disease in order to distribute resources and create health plans to the interpretation of magnetic resonance imaging (MRI), computed tomography (CT) scans, or X-rays with an accuracy that sometimes even exceeds that of human experts.

It is also important to note that there are opportunities inherent to artificial intelligence that are not particular to any industry but will be beneficial to Fiji society as a whole because they are inherent to the nation. There are a few options that stand out as particularly intriguing among these opportunities, and those are as follows: The development of high-skilled jobs and the enhancement of innovation that would result from the implementation of this technology would contribute to the development of a competitive digital economy for the nation. This, in turn, might eventually result in the establishment of new businesses and technological endeavors that are tailored to meet the requirements of Fiji.

5.2.3 CHALLENGES OF AI IN FIJI

The myriad opportunities presented by AI for the Fiji Islands, encompassing both the private and public sectors, could signify a profound shift in the country's paradigm. This transformation is not merely a harbinger of optimism; it also unveils a range of challenges that must be navigated to prevent more significant impediments to Fiji's rapid development in the future.

The primary and most apparent challenge that will arise with the advent of AI in Fiji is the substantial implementation cost, as the requisite software, hardware, and infrastructural technology demand a significant initial investment. The majority of enterprises within the nation are categorized as small to medium-sized businesses. For such entities, the financial implications of this investment may prove to be prohibitive, thereby complicating the rationale for many organizations to embrace AI adoption.

Another significant challenge that warrants attention is the requisite skills within the Fijian workforce to foster an AI-driven environment. At present, the qualifications of professionals

fall short of the necessary standards to advance AI across various beneficial domains. Nonetheless, a pivotal objective outlined in Fiji's National Development Plan, articulated in 2017, pertains to this issue. It asserts: "we will cultivate a world-class skilled workforce to propel economic growth by investing in our educators, modernizing our educational institutions, and ensuring universal access to all tiers of education, encompassing early childhood, vocational, and higher education." This indicates that, although the workforce may not be adequately prepared for an abrupt digital transformation at present, efforts are underway to address this issue within the country. In examining the evolution of the workforce in recent years, the graph derived from [14] illustrates the shifts within the technological sector. While it may appear stagnant in recent times, this perception is largely attributable to the repercussions of Covid on the islands. Absent this disruption, the data indicates a propensity for growth in technological activities, suggesting a forthcoming transformation in the national workforce toward careers in technology.

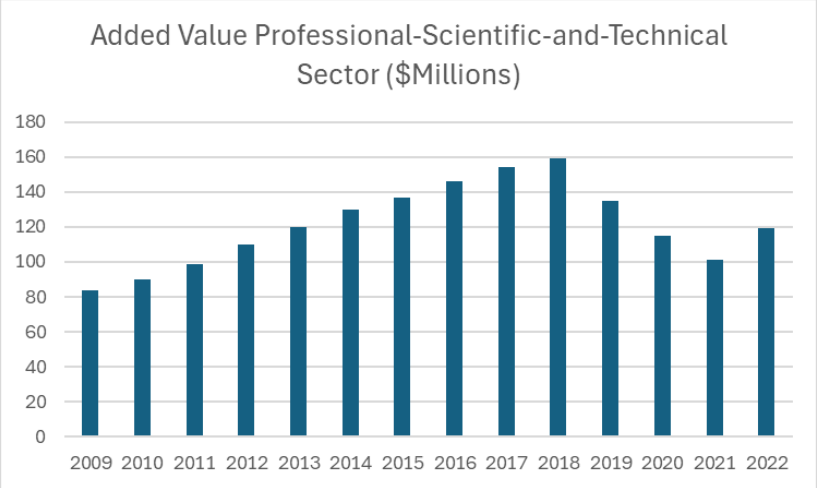

Figure 9.Evolution in Scientific and Technical Sector 2009-2022 [14]

The myriad opportunities presented by AI for the Fiji Islands, encompassing both the private and public sectors, could signify a profound shift in the country's paradigm. This transformation is not merely a harbinger of optimism; it also unveils a range of challenges

that must be navigated to prevent more significant impediments to Fiji's rapid development in the future.

The primary and most apparent challenge that will arise with the advent of AI in Fiji is the substantial implementation cost, as the requisite software, hardware, and infrastructural technology demand a significant initial investment. The majority of enterprises within the nation are categorized as small to medium-sized businesses. For such entities, the financial implications of this investment may prove to be prohibitive, thereby complicating the rationale for many organizations to embrace AI adoption.

A significant challenge that warrants attention is the requisite skills within the Fijian workforce to foster an AI-driven environment. At present, the qualifications of professionals fall short of the necessary standards to advance AI across various beneficial domains. Nonetheless, a pivotal objective outlined in Fiji's National Development Plan, articulated in 2017, pertains to this issue. It asserts: "we will cultivate a world-class skilled workforce to propel economic growth by investing in our educators, modernizing our educational institutions, and ensuring universal access to all tiers of education, encompassing early childhood, vocational, and higher education." This indicates that, although the workforce may not be adequately prepared for an abrupt digital transformation at present, efforts are underway to address this issue within the country. In examining the evolution of the workforce in recent years, the graph derived from [14] illustrates the shifts within the technological sector. While it may appear stagnant in recent times, this perception is largely attributable to the repercussions of Covid on the islands. Absent this disruption, the data indicates a propensity for growth in technological activities, suggesting a forthcoming transformation in the national workforce toward careers in technology.

5.3 CYBER SECURITY THREAT LANDSCAPE IN FIJI

5.3.1 INTRODUCTION

Fiji is undergoing a significant digital transformation that brings opportunities for economic growth and societal advancement. However, with increased digitalization comes heightened

cybersecurity risks that threaten critical infrastructure, businesses, and personal privacy. Understanding these evolving threats is essential to developing effective strategies for mitigating cyber risks.

This chapter explores the current cybersecurity landscape in Fiji by examining various incidents that have exposed vulnerabilities across different sectors, including government institutions and private companies. By analyzing global trends in cyber threats and assessing their impact on Fiji, this discussion highlights the key challenges the nation faces in securing its digital future.

5.3.2 GLOBAL CYBERSECURITY THREATS

Understanding the threat landscape in Fiji, is a fundamental task to analyze the current cyber security situation in the country and what are the most vulnerable areas. This exploration will help us to reveal the key challenges Fiji faces in its cybersecurity journey and value the importance of the needed measures to prevent and mitigate risks in an increasingly digitalized world.

The first thing that will be explored is the different cybersecurity threats that have been detected around the world and how those threats are affecting the country. To get a first impression on how threats are distributed by type, take a look at this graph which compares the mentioned distribution in 2017 and 2023.

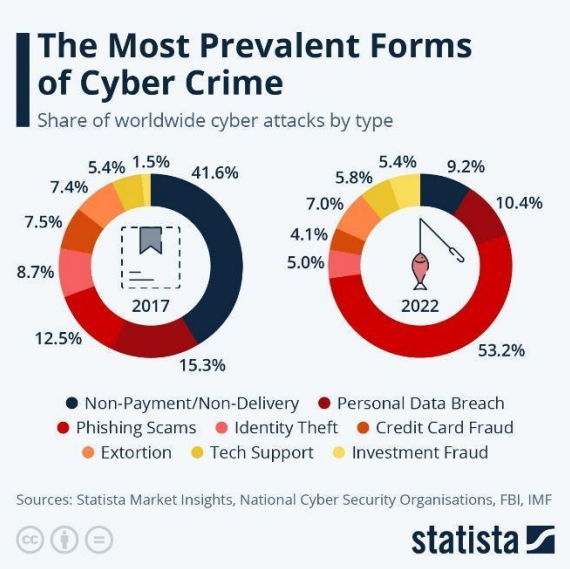

Figure 10. Most common cybercrime by type [18]

As can be seen in the provided graph, the main cyber attack in 2017 was non-payment or non-delivery of a service of product sold, that attack successfully reduced from a 42% to a 9% of all the attacks. However, the main cyber attack that is taking place recently is phishing which has become the most prevalent form of cybercrime, accounting for over 50% of all the cybercrime in the world, unlike other cyberattacks that target system vulnerabilities, phishing exploits human error, making it difficult to prevent. Since it represents such an important percentage of the total attacks, it is important to analyse the impact that this attack can have on a company and how common it is. Statistics indicate that 1.2% of all global email traffic consists of phishing attempts, translating to approximately 3.4 billion malicious emails daily. With 88% of companies experiencing phishing attempts annually, the challenge of combating these attacks continues to grow as cybercriminals refine their strategies. Improving the design and personalization of these emails is what makes it such a difficult task to prevent it from being successful. In a country like Fiji where there is not yet build a strong cybersecurity awareness, this kind of attack is specially dangerous and some measure are needed to avoid to many phishing victims.

Data breaches represent the second most common cybercrime which as stipulated in the graph represents 10% of total cybercrime. These breaches occur when unauthorized parties

gain access to confidential information, leading to financial losses and reputational damage. The following graph represents the evolution of the data breaches per year and people affected by it in the past years at the U.S., this will help to understand the dangers of this cyber-attack.

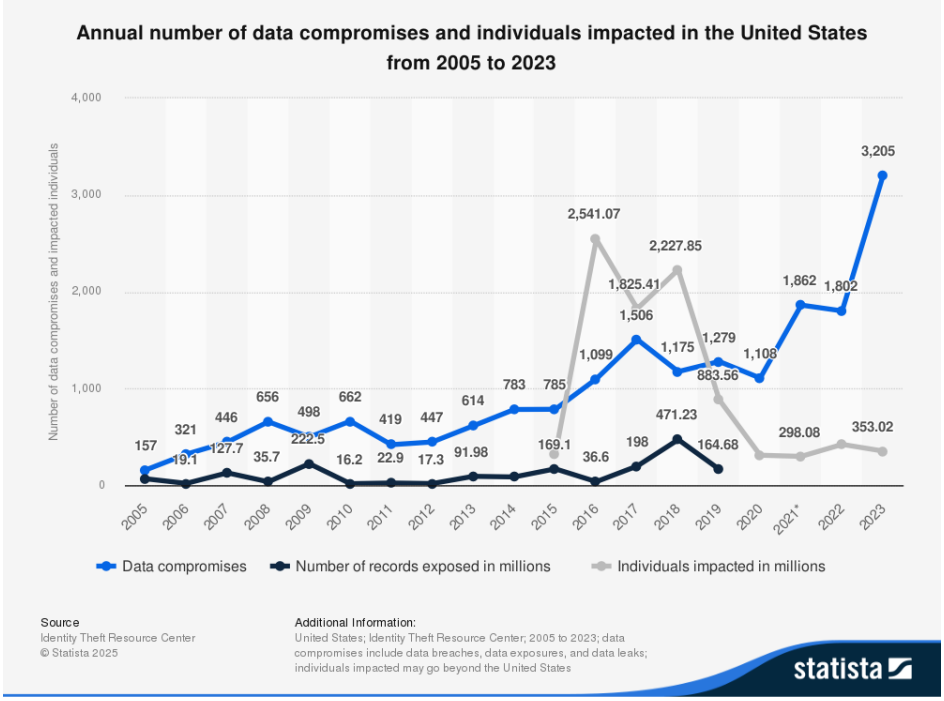

Figure 11. Growth of data breaches by year in the US [17]

The graph indicates that data breaches escalated from 157 in 2005 to 3,205 in 2023. Given that the average cost was approximately 4.45 million dollars in 2023, the overall cost of data breaches in the U.S. for that year amounted to around 14 billion dollars. Recognizing the financial implications of a data breach and its prevalence enables an awareness of the genuine risks these assaults pose to an organization, so underscoring the significance of a well-crafted cybersecurity plan to prevent or mitigate these costs.

The next cybercrime to be examined to comprehend the danger landscape that Fiji will encounter is extortion-based attacks, which, according to Figure 1, constitute 7% of total global cybercrime. Extortion denotes the illegal act wherein perpetrators threaten to disclose critical information, initiate a cyberattack, or disrupt operations unless a certain sum of money is remitted. This category primarily encompasses two types of attacks: Distributed Denial of Service (DDoS) and ransomware. Approximately 43% of all DDoS attacks are directed at U.S. corporations; however, as illustrated in the subsequent graph, the frequency of such attacks escalates annually.

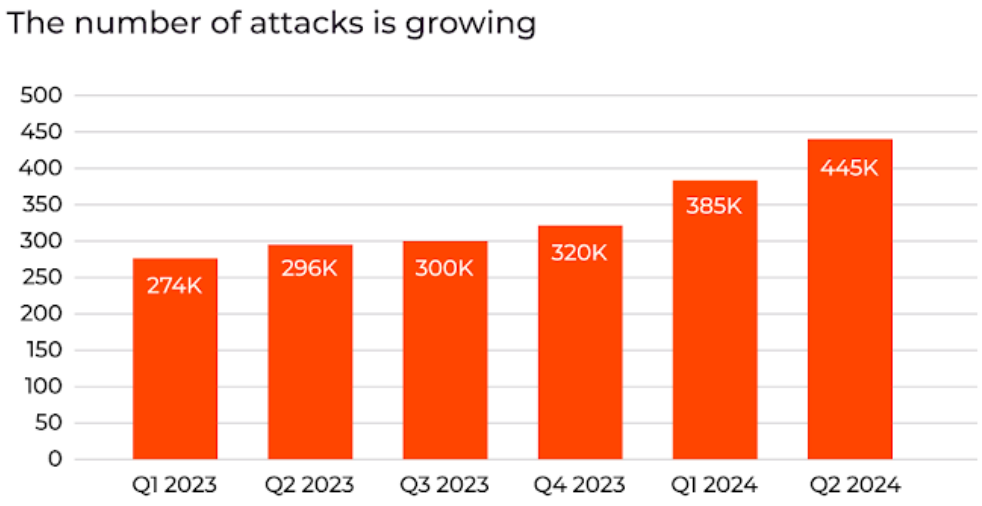

Figure 12. Growth in DDoS attacks from 2021 to 2024 in the US [20]

A Ponemon Institute study [21] estimates the cost of such an attack at an average of $22,000 per hour, resulting in approximately 54 minutes of downtime. A small to medium enterprise will incur approximately $120,000 for service restoration. This expense may appear lower than the average for data breaches; however, the frequency of DDoS attacks is significantly greater. Ransomware incidents have been increasingly prevalent annually, with 55.1% of firms affected in 2018, rising to 72.7% by 2023, as illustrated in this figure.

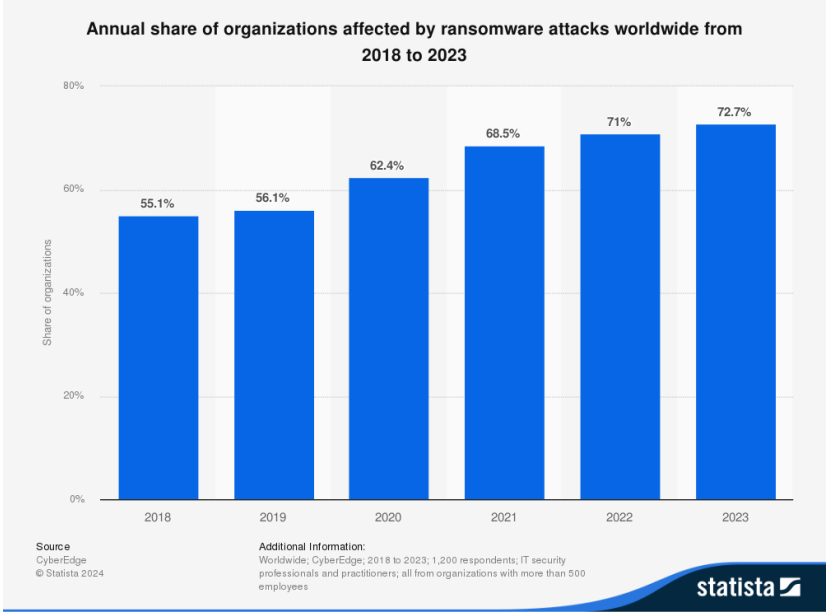

Figure 13. Growth in ransomware attacks worldwide [22]

This type of attack incurs substantial expenditures and prolonged downtime, with an average duration of around 24 days and an expense of $1.85 million per occurrence [19]. Similar to DDoS attacks, over 40% of these incidents targeted U.S. enterprises; nevertheless, organizations must remain prepared for such possibilities even in less typical scenarios, such as in Fiji.

5.3.3 VULNERABILITIES BY SECTOR

After analyzing the most common types of cybercrime, it is essential to determine the sectors that are most commonly attacked by these threats. Because of the sensitive data that specific sectors manage and the possible financial advantages that have the potential to result from successful attacks, specific industries are more frequently targeted by cybercriminals. Because sectors like healthcare, banking, and manufacturing are commonly subjected to many attacks, these sectors should be prioritized for increased investments in cybersecurity

and proactive defense methods. It will be easier to grasp the most vulnerable sectors if you look at the following graphs.

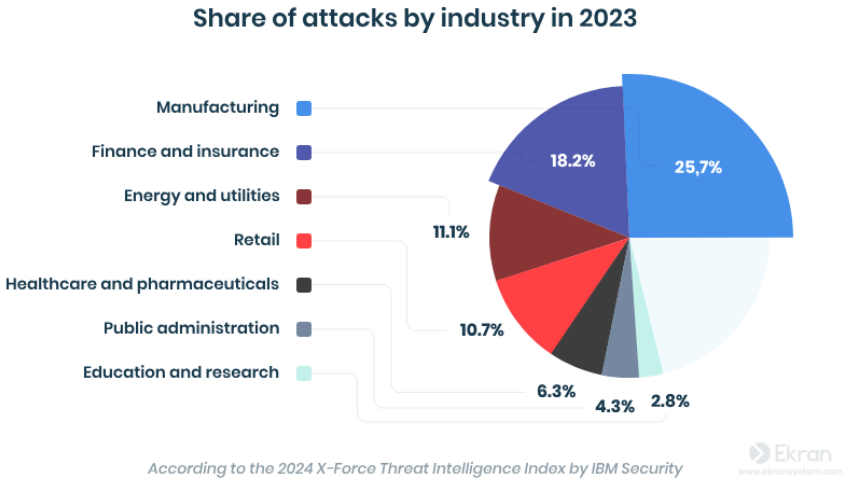

Figure 14. Cyber attacks percentage by industry [23]

5.3.4 CYBERSECURITY THREATS IN FIJI

After reviewing worldwide cyber risks, we now focus on Fiji's unique cybersecurity scenario. Analyzing prior security incidents will assist in identifying the country's most vulnerable systems and developing protection plans.

An important incident occurred in 2023 [24] when a Chinese state-sponsored hacking organization conducted a cyber campaign targeting government, healthcare, technological, and manufacturing entities in Taiwan, Thailand, the Philippines, and Fiji. The attack, carried out by an APT41 organization known as Earth Longzhi, their goal was to gain persistent control over computer systems, most likely for cyber espionage reasons. The attackers used advanced malware techniques, such as a Behinder webshell and bring-your-own-vulnerable-driver (BYOVD) strategies.

Another cyber crisis occurred in Fiji in September 2024 [25], when an unknown attacker hacked the Suva City Council's networks, encrypted all data, and demanded a ransom for its release, a classic ransomware attack. The most recent publicly documented cyberattack in

Fiji targeted the offices of the Pacific Islands Forum [26]. It is unknown when the attacker initially obtained access. The attack intended to collect intelligence about the Secretariat and its operations, and it was also blamed on a Chinese state-sponsored hacking organization. With a better awareness of both global threats and individual cyber occurrences in Fiji, the country can now assess its cybersecurity condition and readiness for future dangers as digital systems grow.

5.3.5 REGIONAL THREATS

Pacific Island states, such as Fiji, are progressively becoming targets for cybercriminals. Prevalent dangers include email fraud, ransomware, card skimming and phishing. Expanding internet access has increased vulnerability to these threats [27]. Advanced Persistent Threat 40 (APT40), a state-sponsored cyber organization with sophisticated capabilities, has been reported to target networks in the Blue Pacific region, including Fiji. APT40 has previously executed nefarious operations against governmental networks and essential infrastructure in various nations.

The geopolitical dynamics of the Pacific area have resulted in heightened cyber activity from multiple state actors. Reports indicate that Chinese hackers have targeted diplomatic entities in the Pacific Islands region, particularly Fiji. Pacific Island nations are vulnerable to becoming targets for international criminal organizations, with escalating illicit activities, including cybercrime [27]. The islands' isolation, economic fragility, elevated corruption, and restricted state capability intensify this threat, rendering them appealing to formidable transnational crime organizations [28-29].

The escalating effects of climate change, including cyclones, earthquakes, and volcanic eruptions, significantly disrupt connectivity infrastructure, encompassing both terrestrial and subsea systems. In many cases, economies may require weeks to reestablish connectivity after such calamities, rendering places like Fiji susceptible to cyber threats during these intervals [28]. Mitigating these dangers necessitates a holistic strategy, encompassing the

fortification of cybersecurity frameworks, the augmentation of international collaboration, and the development of resilience against cyber and environmental adversities.

5.3.6 CONCLUSION

The fast digital revolution that Fiji is undergoing has enormous prospects for the country's economic development and societal advancement. On the other hand, as this chapter has demonstrated, this evolution also puts the country at risk of cyber assaults that are becoming increasingly sophisticated. Phishing, data breaches, and extortion are examples of global trends in cybercrime that underline the issues that Fiji needs to put itself in a position to face.

The vulnerability of Fiji to these ever-evolving dangers is shown by recent cyber events that have targeted government institutions and business entities in the country. Fiji needs to prioritize investments in cybersecurity strategies, awareness programs, and infrastructure resilience to keep up with the increasingly sophisticated tactics used by cybercriminals. Increasing the strength of cybersecurity defenses is necessary to protect the nation's digital future, including enterprises, government agencies, and individuals.

5.4 REGULATORY AND POLICY FRAMEWORKS

5.4.1 INTRODUCTION

In this chapter, the primary objective is to explore the frameworks in Fiji related to cybersecurity and artificial intelligence. By examining these frameworks, we aim to evaluate Fiji's current standing in these fields and identify critical gaps in the existing policies. It is necessary to address these gaps in order to achieve a secure environment for development and adoption of digital technologies, which are a key element to explore opportunities of the country regarding new technologies

.

5.4.2 THE CYBERCRIME ACT OF 2021: FOUNDATION OF FIJI'S CYBERSECURITY FRAMEWORK

The single most influential framework regarding cybersecurity in Fiji is the Cybercrime Act of 2021 [4], a legislative measure designed to safeguard citizens against digital threats and combat cyber offenses and provide to the authorities the necessary tools to prosecute and mitigate cybercrime. The act delineates several categories of cybercrime and their corresponding penalties, including:

- Unauthorized Access: Criminalizing access to computer systems or networks without proper authorization.
- Data Interference: Penalizing actions such as altering, deleting, or suppressing computer data without permission.
- System Interference: Prohibiting acts that disrupt the functionality of computer systems or networks, such as denial-of-service (DoS) attacks.
- Misuse of Devices: Criminalizing the production, distribution, or possession of tools, software, or credentials intended to facilitate cyber offenses.
- Forgery and Fraud: Targeting crimes like creating fake digital documents or committing fraud using computers.

- Identity Theft: Prohibiting the unauthorized use or theft of another person's identity for fraudulent purposes.

These offenses address various aspects of digital criminality, laying a strong foundation for punishing cybercrime in Fiji. However, addressing criminal behavior alone is insufficient without robust procedural measures to investigate and enforce these laws effectively. This is why within the Cybercrime Act of 2021 there are also included tools to prosecute cybercrimes.

5.4.3 STRENGTHENING LAW ENFORCEMENT CAPABILITIES

To facilitate cybercrime detection and prosecution, the Cybercrime Act includes provisions that empower law enforcement agencies with critical investigative tools, such as:

- Data Preservation: Enabling authorities to order the preservation of electronic data relevant to an investigation.
- Search and Seizure: Granting law enforcement the ability to conduct judicially approved searches of digital devices and seize relevant electronic evidence.
- Real-Time Data Collection: Allowing investigators to intercept and monitor traffic or content data in real time for serious cyber offenses.

These procedural capabilities form the backbone of Fiji's ability to combat cybercrime. However, their effective implementation relies on adequate training, resources, and inter-agency coordination which will probably take some time before a successful implementation.

5.4.4 INTERNATIONAL COLLABORATION: ADDRESSING CROSS-BORDER CYBERCRIME

The global character of cyberspace and the pervasiveness of cybercrime has created a demand for international cooperation, which is addressed and highlighted by the Cybercrime Act of 2021. The act provides tools that would enhance cooperation with other countries, including:

- Mutual Legal Assistance: Facilitating requests for support in cybercrime investigations between Fiji and other countries.
- Extradition: Allowing individuals accused of cyber offenses to be transferred to foreign jurisdictions for prosecution.
- Information Sharing: Encouraging the exchange of intelligence on cybercriminal networks, methodologies, and emerging threats.

With cybercrimes crossing borders, this international collaboration is critical to addressing the 21st century challenges of cyber threats assuring that Fiji is an active player in the global impact of cybersecurity. Being aware of methodologies and threats used by cybercriminal organizations in other countries is critical to understanding the potential risks that could impact Fiji in the future.

5.4.5 GAPS IN FIJI'S FRAMEWORK: THE ROLE OF ARTIFICIAL INTELLIGENCE

Despite the strengths of the Cybercrime Act, notable gaps can be found, particularly concerning artificial intelligence. Fiji currently lacks a framework addressing the challenges and opportunities posed by AI. In contrast, other nations, such as the EU with its AI Act, provide comprehensive regulations for the development, deployment, and use of AI technologies. The EU AI Act includes:

- Risk Classification of AI Systems: Identifying acceptable, high-risk, or prohibited AI systems and applying appropriate compliance measures.

- Transparency Obligations: Requiring clear disclosures for systems interacting with humans or generating deep fakes.
- Innovation Support: Providing controlled environments for testing AI systems under regulatory oversight.
- Penalties for Non-Compliance: Enforcing regulations through fines and accountability mechanisms.

Adopting similar guidelines in Fiji could help address AI-related risks and establish an ideal regulatory environment to AI innovation.

5.4.6 ENSURING CYBER SECURITY ADOPTION IN PRIVATE COMPANIES

The 2021 Cybercrime Act does not impose specific cybersecurity guidelines or obligations on private companies, which can lead to the mishandling of sensitive information and data breaches that may harm customers. To address this gap, Fiji could adopt elements from frameworks like the NIS 2 Directive in Europe, which mandates:

- Implementation of technical cybersecurity measures such as encryption, access management, and incident detection.
- Mandatory reporting of cybersecurity incidents within 24 hours.
- Development of structured recovery plans to mitigate the impact of cyberattacks.

Enforcing similar policies in Fijian private companies would create a more secure digital environment, fostering safer business operations and increasing trust in the nation's digital infrastructure.

5.4.7 THE IMPORTANCE OF PRIVACY AND DATA PROTECTION

Another critical area for improvement is privacy and data protection. Safeguarding individual rights and controlling the use of personal data are essential for improving trust in

digital technologies. An example of a framework which addresses these problems is the General Data Protection Regulation (GDPR) in the EU which provides a robust model, with principles such as:

- Lawful, fair, and transparent data processing.
- Collection of data for specified, legitimate purposes only.
- Retention of data for no longer than necessary.
- Security measures to protect against unauthorized access or data breaches.
- Rights for individuals to access, rectify, or delete their data.
- Obligation of companies to notify in case of breach

Incorporating similar principles into Fiji's regulatory framework would lead to a much more transparent environment, therefore a greater trust of the citizens in digital technologies.

5.4.8 CRITICAL INFRASTRUCTURE PROTECTION: AN OVERLOOKED PRIORITY

Critical infrastructure protection is another missing element in Fiji's cybersecurity strategy. Cyberattacks on critical services like transportation, energy and healthcare can have devastating effects. For instance, there have been detected vulnerabilities in hydroelectric systems [30], a successful cyber-attack in this type of power plant will cause catastrophic consequences in the Fiji Islands since 80% of the electricity in the nation comes from hydroelectric systems and because without them, there is not sufficient electricity to supply the entire country. However, there are many other critical sectors as important as energy that in case of a cyberattack would also mean an important impact to the country, such as healthcare, agriculture or water systems.

In order to prevent or mitigate cyberattacks in the critical infrastructure of the islands, frameworks such as the NIST Cybersecurity Framework (CSF) from the USA offers an

interesting approach to protecting this infrastructure. By adopting its risk-based methodology, Fiji could:

- Identify and prioritize risks unique to its infrastructure.
- Implement safeguards to mitigate these risks.
- Establish mechanisms to detect, respond to, and recover from cyber incidents.

The framework's emphasis on public-private collaboration and its adaptability to diverse contexts make it well-suited for Fiji's needs.

5.4.9 CONCLUSION: BUILDING A RESILIENT DIGITAL FUTURE

As discussed in this chapter, Fiji's current cybersecurity and AI frameworks provide a foundation for addressing cybercrime providing essential tools to achieve a secure environment for digital innovation. However, this framework leaves significant gaps unaddressed that need to be mentioned somewhere else. There are no laws governing the use of AI, there is no proper protection of data and the right amount of attention is not given to the critical infrastructure which presents a risk to the nation's digital progress and the security of the citizens' data and infrastructure.

Following other examples such as the EU AI Act, GDPR, NIS 2, or NIST CSF, Fiji can create a complete set of regulations for the AI that would increase security, support innovation, and build people's trust. All these frameworks can be used as a guide to identify the gaps and to place Fiji at the forefront of the safe and prudent use of digital technologies. However, even these examples do not provide a complete guarantee, as they also reveal gaps, as explained in [37]. It is essential to continuously refine and evolve the frameworks over time to address these shortcomings effectively.

5.5 CYBER SECURITY EDUCATION AND WORKFORCE DEVELOPMENT

5.5.1 INTRODUCTION

As was mentioned earlier, the digital transformation that Fiji is going through will result in an increase in the relevancy of cybersecurity for the country. As a consequence of this, there has been an increase in the demand for experts with expertise in that field. However, currently Fiji's cybersecurity education and workforce development are still relatively underdeveloped.

Courses in computer science and information technology are offered at a few universities in Fiji, including the University of the South Pacific, the Fiji National University, and the University of Fiji. However, specialist cybersecurity courses are just beginning to emerge in the country. Recently a new postgraduate degree in the field of cybersecurity was launched at both the University of the South Pacific and the Fiji National University.

The spread of cybersecurity education in Fiji has been delayed by a number of obstacles, including limited access to training materials, a scarcity of qualified professors in the field of cybersecurity, and only a few of opportunities for training. The resolution of these concerns is absolutely necessary in order to construct a resilient and secure digital ecosystem for the country.

5.5.2 CYBERSECURITY EDUCATION SITUATION IN FIJI

For the purpose of gaining a comprehensive understanding of the level of cybersecurity education in the country, we will conduct an analysis of the statistics regarding the number of students enrolled in undergraduate degrees connected to technology at the three most prestigious universities in the country. Having this information will make it easier to visualize the degree to which the school system and society of Fiji are equipped to deal with the cybersecurity concerns that will emerge in the future.

Before delving into the many educational institutions that are located in Fiji, it is essential to first examine the statistics of a fully developed and contemporary nation that is located on the same continent as Australia. This will allow us to determine which data is the most appropriate. When we look at the percentage of undergraduate students enrolled in STEM fields in Australia, we find that they make up to 21 percent of the total number of students enrolled in institutions in Australia. On the other hand, this number is far higher in some nations, such as Germany and India, where it is greater than thirty percent.

The Fiji National University is the university that has the highest number of students enrolled in it. According to the data that was posted by this university, Figure 15 illustrates the progression of the number of STEM students who have enrolled in the university over the course of the past five years. Once we have established what a typical percentage of students in STEM fields is, we should begin to examine the university that has the most students attend.

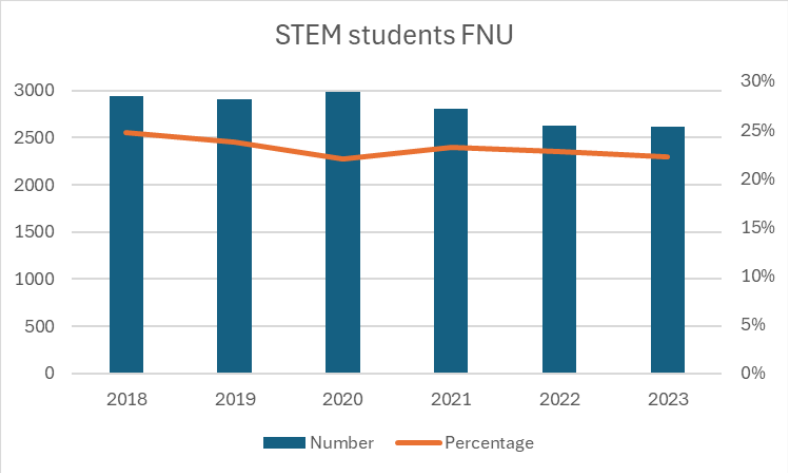

Figure 15. Enrolled STEM students in FNU 2018-2023 [46-50]

The figure above shows that while maintaining a good STEM undergraduate degree percentage the number of students, both the number of students and the percentage of STEM students have been slightly decreasing in the past years. The next university which should be observed is the University of the South Pacific which is the second largest university in

Fiji, this university also gives degrees in other pacific islands but focus will remain in Fijian statistics. Figure 16 shows the equivalent statistics to the Fiji National University.

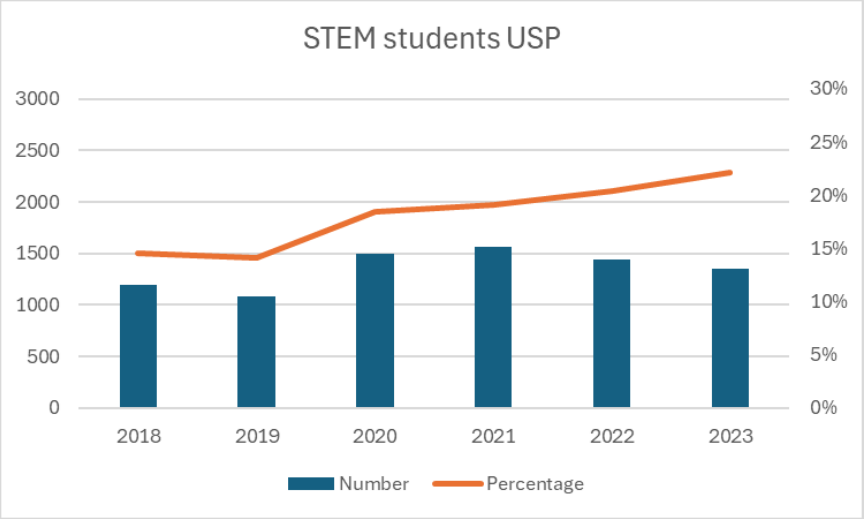

Figure 16. Enrolled STEM students in USP 2018-2023 [51-55]

In the case of the University of the South Pacific in Fiji, it can be observed that while the percentage of STEM students is increasing, the number of STEM students is not, which reveals a decreasing number of students each year. Lastly, below are the statistics of the smallest university of Fiji, the University of Fiji.

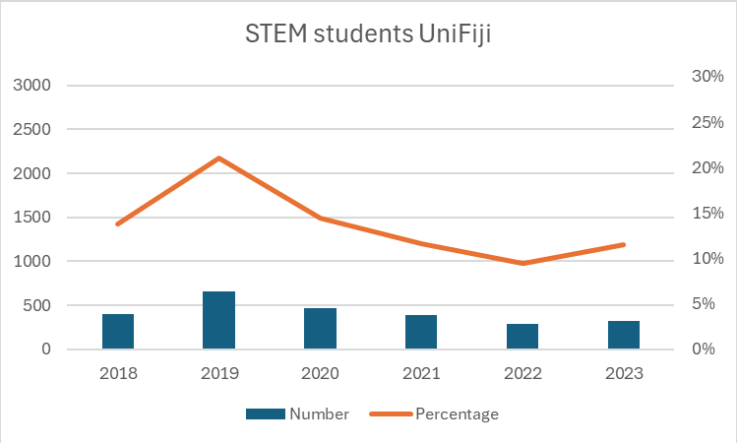

Figure 17. Enrolled STEM students in UniFiji 2018-2023 [41-45]

In this graph it can be observed a lower number of students and percentage of STEM students compared to the other universities, this is probably due to the fact that the University of Fiji is the only university mentioned that is not located in the capital of the country, but in a much more rural area.

Once the three universities in Fiji have been explored we can look at the global values. In 2023 Fiji had around 21% of STEM students out of the total number of students which was not as high as top STEM countries like Germany, China or India. However, it is similar to fully developed countries like USA or Australia. This reveals an interest of the students to start a career in a STEM field which is necessary to acquire the necessary skills to start a career in cybersecurity. However, the percentage of people attending university has been reduced after COVID from 84 to 60% in 2023, this value is way higher in other countries like Australia where we can find a value of 106% because of adult learners or international students. All these values reveal an interest to initiate a STEM career but a lack of resources to do so, further in this chapter we will focus on measures that could be taken to facilitate and provide help for these studies.

5.5.3 CURRENT CYBERSECURITY SKILL GAP IN FIJI

As of today, Fiji does not count with a fully prepared workforce of cybersecurity professionals, there are various skills lacking today in the nation that would be essential to correctly develop the mentioned workforce. Most of the skills that are needed in the country are technical skills which are needed to avoid cyber attacks and therefore protect sensitive information and maintain important services operating. The most important skills are:

- Cloud Security: Since more organizations are migrating to cloud solutions, there is emerging a need for professionals who are able to secure these environments correctly.
- Incident Response and Threat Intelligence: One of the most important skills in cybersecurity professionals is the ability to identify, analyze, and mitigate cyberthreats. This skill is crucial to minimize the damage of an attack and prevent future ones.
- Network security: The lack of monitorization and security in an organization network can be the cause of devastating consequences in the company. Being able to provide these characteristics to the network allows the organization to detect an intrusion, isolate it and eliminate it effectively.
- Penetration Testing: The ability to measure how strong or weak the security of an organization's digital system is, represents a crucial task to acknowledge which systems are currently vulnerable to potential attacks and should be securitized.
- Application Security: Just as network security, if an application is not correctly secured an attacker could intrude the organization systems which could lead to a huge loss in money and reputation for the company.

The skills just mentioned are some of the most essential and necessary skills a cybersecurity workforce must have to be able to secure most systems that require it.

5.5.4 INITIATIVES FOR WORKFORCE DEVELOPMENT

To close the cybersecurity skills gap in Fiji, some initiatives have been established, and many others could be as well. These initiatives include national strategies, scholarship programs, and industry collaborations that aim to equip Fijians with the necessary skills to pursue a career in the cybersecurity sector.

Regarding national strategies, Fiji has already launched their National Development plan [2]. Which outlines the nation's vision for economic growth via digital transformation. As part of the strategy, Fiji has committed to invest in the needed infrastructure and more importantly in enhancing STEM programs including cybersecurity. Currently there are already scholarships for STEM degrees to encourage students to pursue careers like cybersecurity given by The Tertiary Scholarship and Loans Board, even some private companies like Samsung are collaborating with the Ministry of education to promote STEM careers across the country [71].

Some universities like Fiji National University have already started collaborating with organizations to improve their cybersecurity program. The mentioned university is already collaborating with the EC Council in Fiji, which will grant students the opportunity to work under the National Training and Productivity Centre with cutting-edge cybersecurity training and certifications, enhancing their training to prevent and mitigate cyber threats effectively [57].

There are also signs of organizations with strong commitment with cybersecurity and workforce development in the area. For example, Outsource Fiji in January 2024 concluded a cybersecurity training program for 30 professionals to provide them with the needed skills to secure the clients data [58].

5.5.5 CONCLUSION

As Fiji continues its digital transformation, the importance of cybersecurity will only grow, making workforce development in this field a critical priority. Despite the increasing interest in STEM education, the nation faces significant challenges in preparing a skilled cybersecurity workforce, including limited specialized training programs, a shortage of experienced educators, and restricted access to resources. While the country's top universities have begun offering cybersecurity-related programs, enrollment trends indicate a need for greater support to encourage more students to pursue careers in this essential field.

Addressing the current cybersecurity skills gap requires a multifaceted approach, combining national strategies, industry partnerships, and scholarship programs to enhance education and training opportunities. Ongoing initiatives, such as Fiji's National Development Plan, collaborations with organizations like the EC Council, and training programs led by institutions such as Outsource Fiji, are promising steps toward strengthening the nation's cybersecurity capabilities. However, sustained investment and innovation in education and workforce development will be necessary to ensure Fiji can meet future cybersecurity challenges and safeguard its digital infrastructure.

By continuing to expand educational opportunities, fostering industry collaboration, and equipping professionals with essential cybersecurity skills, Fiji can build a more secure and resilient digital ecosystem, ensuring the nation is well prepared for the evolving threats of the digital age.

5.6 AI IN ENHANCING CYBER SECURITY: USE CASES IN FIJI

5.6.1 INTRODUCTION

Cyber threats are evolving at a tremendous rate, and traditional defensive methods often have a hard time keeping up with these attacks. In response, countries such as Australia and New Zealand are using artificial intelligence to improve their cybersecurity measures. All around the world, AI has shown great results in strengthening cybersecurity, providing rapid threat detection, improving incident response, and enhancing overall resilience against cyberattacks.

Fiji, while still advancing its digital transformation, has already taken important initial steps in this direction. A notable example is Vodafone Fiji's implementation of an AI-based fraud detection system, which shows the country's commitment to integrating emerging technologies into its cybersecurity environment [76]. These early initiatives can help understand how AI can serve as an invaluable tool in protecting digital infrastructure.

This chapter examines key international use cases from Australia and New Zealand and considers their relevance to Fiji's context. By reflecting on these experiences, the chapter aims to outline a path for adapting AI-driven approaches to enhance cybersecurity in Fiji, acknowledging the nation's unique challenges and opportunities in the digital era.

5.6.2 AI IN CYBERSECURITY OVERVIEW

As previously explained, some of the current cyber threats require sophisticated solutions to detect and prevent them, these solutions often include artificial intelligence to enhance their results. AI has been deployed in various cybersecurity areas successfully such as red teaming, breach management, threat detection and incident response between others.

To illustrate the impact of how artificial intelligence can improve cybersecurity solutions, it is convenient to observe some statistics in relation to the topic. According to the IBM data

breach report of 2024 [19], organizations which used AI and automation extensively for prevention, had an average breach cost of USD 3.76 million. Meanwhile, organizations that didn't use these tools in prevention saw USD 5.98 million in costs, a 45.6% difference, for AI in detection organizations saved an average of 1.88 million dollars, 1.74 million in investigation and 1.68 million in response. This report also mentions that breaches were 100 days faster in companies that extensively used AI security and automation compared with those that did not.

These results clearly demonstrate that integrating AI into cybersecurity measures can lead to significant cost savings and faster incident resolution. At the same time, as cyber attackers continue to use AI to refine their tactics such as crafting more sophisticated phishing or ransomware attacks, the case for increasing AI adoption in cybersecurity becomes even more necessary.

5.6.3 INTERNATIONAL CASE STUDIES

In this section of the chapter case studies from Australia and New Zealand will be explained to demonstrate how AI techniques have been applied to enhance cybersecurity in developed countries.

5.6.3.1 Case Studies in Australia

The first case that should be analyzed is related to one of the most harmful and common attacks in the current world, phishing. The initiative is called Smart Shield [59], and it uses advanced machine learning algorithms to examine and learn from phishing emails and malicious websites, enabling greater detection of advanced phishing attempts. Developed through a collaboration between the Cyber Security Cooperative Research Centre, CSIRO's Data61, and the Government of Western Australia. By employing advanced machine learning algorithms, Smart Shield not only analyzes and learns from phishing emails and

malicious websites but also provides real-time, color-coded alerts (using a “traffic light” system) to warn users of potential threats. This proactive mechanism has enhanced threat detection accuracy and significantly reduced false positives, enabling organizations to better protect their email communications from sophisticated phishing attempts.

The implementation of Smart Shield involves several key components:

- Data Collection and Training: The system was trained using approximately 38,000 employee-reported emails and 20 million phishing and benign URLs relevant to Australia. The emails were primarily sourced from CSIRO, representing over five years of phishing and spam data, with additional samples from the Western Australian Government. This extensive dataset ensures that the algorithms learn from data pertinent to the target environment.
- Advanced Detection Algorithms: Smart Shield utilizes both contemporary and novel ML algorithms to detect phishing. These algorithms analyze linguistic patterns, structural features, and deceptive tactics used in phishing content, allowing for the identification of sophisticated phishing attempts that might bypass traditional filters.
- User-Centric Interface: The system features a real-time "traffic light" warning mechanism that provides users with immediate visual cues about the safety of incoming emails. This approach not only enhances security but also educates users, which helps to create a more security-conscious culture within organizations.

Smart Shield has demonstrated significant success in enhancing phishing detection and prevention. This initiative was recognized as really effective and successful as it won the Technology Platform Solution category at the NSW iAwards in 2022 [60]. Especially mentioning its innovative approach to cybersecurity.

However, implementing an AI anti-phishing system like Smart Shield involves several challenges:

- Data Relevance: Ensuring that the training data is relevant to the target environment is crucial for the system's effectiveness. Smart Shield addresses this by using data primarily sourced from CSIRO and the Western Australian Government.
- Algorithm Complexity: Developing and fine-tuning advanced ML algorithms to accurately detect sophisticated phishing attempts requires significant expertise and resources.

Another case study of Australia that should be mentioned is called Cyber Deception as a Service [61] which is an innovative initiative developed by the Cyber Security Cooperative Research Centre in collaboration with industry partners. This project leverages advanced machine learning and artificial intelligence techniques to create realistic decoy assets that imitate real IT assets, by deploying these decoys strategically within a network, the system aims to mislead attackers, guiding them away from "real" assets and into controlled environments where their activities can be monitored and analyzed. This approach not only helps in early threat detection but also provides valuable insights into attacker tactics and techniques.

The implementation of this initiative involves several key components:

- Automated Decoy Generation: Utilizing ML algorithms to simulate a wide range of IT assets, ensuring that decoys are really similar to real systems.
- Dynamic Adaptation: Continuously updating and modifying decoys to reflect changes in the actual IT environment to maintain the illusion of authenticity.
- Intrusion Detection: Monitoring interactions with decoys to identify unauthorized access attempts and trigger alerts for security teams.
- Data Collection and Analysis: Gathering data on attacker interactions with decoys to enhance understanding of threat vectors and inform future security strategies.

While the success of the project has not been publicly disclosed, it is a great idea that not only enhances the security of an organization but also reduces the alert fatigue produced by false positives, because all the alerts produced by this system should be true positives since employees will not enter the fake IT assets.

5.6.3.2 Case Studies in New Zealand

The first case that will be explored in New Zealand is about a company called NEC which has been at the forefront of integrating artificial intelligence and machine learning into cybersecurity solutions, aiming to enhance threat detection, response, and overall security posture for other organizations [62]. The service developed by NEC implements "detection" of unknown attacks over the entire attack process from malware intrusion and the spread of infection inside a system to the achievement of an attacker's aim such as theft of data.

While AI and ML offer substantial advancements in cybersecurity, NEC acknowledges the challenges associated with their implementation:

- Adversarial AI: Cybercriminals are also leveraging AI to develop more sophisticated attacks, creating a continuous battle between attackers and defenders.
- Data Quality and Privacy: The effectiveness of AI models depends on the quality and quantity of data. Ensuring data privacy while collecting and processing information for AI analysis is crucial.
- Integration with Existing Systems: Seamless integration of AI solutions into existing cybersecurity infrastructures requires careful planning and execution to avoid potential disruptions.

Another case study in New Zealand that could be really beneficial to Fiji, is the application of artificial intelligence to overcome the cybersecurity skill shortage, thereby enabling a smaller team of experts to manage a much larger set of security events. IBM New Zealand, made a solution in 2019 which uses advanced machine learning algorithms to automate many routine tasks that traditionally needed cybersecurity analysts [77]. The key components of IBM's approach include:

- Automated Data Analysis and Threat Detection: The system continuously monitors large quantities of security data, ranging from network logs to user activity reports, and uses ML algorithms to establish a baseline of normal behavior. Any deviations

from this norm are flagged as potential threats. By automating this process, the solution is able to process millions of events and highlight those that require further investigation.

- Alert Prioritization and Incident Triage: One of the most critical functions of the system is its ability to prioritize alerts. Instead of overwhelming security teams with thousands of low-level alerts, the AI solution classifies incidents based on severity and context. This prioritization ensures that human analysts focus their efforts on the most critical issues first, therefore reducing response times and improving overall incident management.

However, this project revealed some interesting challenges along the implementation, such as the difficulty of integrating AI systems within the existing cybersecurity infrastructure and the initial investment required to develop these ML algorithms.

5.6.4 APPLICABILITY TO FIJI

The international case studies from Australia and New Zealand offer actionable insights for Fiji's ongoing digital transformation. Fiji can draw on the successes of projects like Smart Shield and Cyber Deception as a Service to enhance its cybersecurity posture. For example, Smart Shield's real-time, AI-assisted anti-phishing approach demonstrated by its ability to analyze extensive local data and provide immediate user warnings, illustrates how AI can mitigate phishing threats even in resource limited environments. Similarly, the Cyber Deception as a Service project provides a model for early threat detection by deceive attackers into decoy environments. Moreover, the IBM ANZ case study on addressing the cybersecurity skills shortage shows that AI can serve as a "force multiplier" by automating routine monitoring tasks, thereby enabling a shorter cybersecurity workforce to focus on complex threat analysis. By adapting these solutions to local contexts, such as integrating them into Fiji's existing IT infrastructure and investing in workforce training, Fiji can develop a scalable and resilient cybersecurity framework that meets both its immediate and future needs. However, the initial cost of the solution and the need of highly skilled

professionals to develop the solutions can be difficult challenges to surpass in order to use these great AI ideas.

5.6.5 CONCLUSION

This chapter has explored how advanced AI-driven cybersecurity initiatives have been successfully deployed in Australia and New Zealand. The Smart Shield anti-phishing system demonstrates the power of machine learning to detect sophisticated phishing attempts, while the Cyber Deception as a Service project shows how automated decoy environments can proactively trap attackers and yield valuable intelligence. In addition, leveraging AI to alleviate the cybersecurity skills shortage as highlighted in the IBM ANZ case study underscores the potential of these technologies to augment limited human resources. Together, these international case studies illustrate a shift from traditional reactive defenses toward proactive, adaptive, and intelligence-driven cybersecurity strategies. For Fiji, these examples provide a roadmap for integrating AI into its cybersecurity environment, giving the country a possibility to enhance threat detection, reduce false positives, and build a more resilient digital ecosystem. Adopting these advanced strategies will be immensely helpful for Fiji as it works to protect its digital infrastructure in an increasingly complex threat landscape.

5.7 COLLABORATION AND PARTNERSHIPS

5.7.1 INTRODUCTION

In an increasingly digital world, the rapid advancement of artificial intelligence and the growing complexity of cybersecurity threats demand strong collaboration between key sectors. In Fiji, where digital transformation at its peak, partnerships between the government, academic institutions, and the private sector play a crucial role in ensuring a secure and innovative technological environment. These collaborations will provide research, develop policies, and create the infrastructure needed to support AI adoption and robust cybersecurity measures.

Fiji's strategic position as a regional hub in the Pacific makes it both an emerging digital economy and a target for cyber threats. The government has started taking proactive steps to establish national cybersecurity frameworks and AI development strategies. However, effective implementation requires support from universities, which provide research and workforce development, and private sector companies, which bring expertise, funding, and cutting-edge technology. Without these synergies, Fiji risks facing harder challenges in AI adoption and remaining vulnerable to cyber threats.

Collaboration between sectors has already shown promising results, including government-backed cybersecurity policies, university-led training programs, and private sector investments in digital infrastructure such as 5G infrastructure programs. The growing participation of international organizations further strengthens Fiji's position in global AI and cybersecurity efforts. By establishing strong partnerships, Fiji can accelerate innovation, build a highly skilled workforce, and ensure a safer digital future for its citizens.

This chapter explores the role of collaboration and partnerships in advancing AI and cybersecurity in Fiji. It highlights how government, academia, and the private sector could work together, the challenges they face, and the opportunities that can be created for a digitally resilient nation.

5.7.2 GOVERNMENT – ACADEMIA COLLABORATION

The first collaboration that should be explored is between government and academy sectors, these two have already been collaborating in the past years. For example, the University of the South Pacific has been actively engaging with government officials to address Fiji's unique cybersecurity needs. For instance, Maurice Dawson, an associate professor at Illinois Institute of Technology, collaborated with USP to discuss cybersecurity challenges with government officials, students, and the media [73]. This collaboration aimed to enhance awareness and develop strategies to strengthen Fiji's cybersecurity framework.

Another collaboration between the government and academia was already mentioned in chapter 5. Because of the Fiji National Development Plan [2], which focuses on the importance of digital evolution and cybersecurity for the future of the nation, the country is supporting scholarships to STEM education including cybersecurity and IT related degrees.

The collaborations mentioned should be just the beginning of this kind of partnership. Looking at other countries, there are several collaborative opportunities that helped them develop a much more advanced cybersecurity and artificial intelligence environment for developing a skilled workforce and enhancing innovation. For instance, the Australian government funds the Cybersecurity Collaborative Research Centre where they bring collaboration between government, industry and academia to create real-world solutions for cyber threats [63], this initiative not only enhance the cybersecurity of the country but also helps fostering the next generation of cybersecurity talent, an initiative like this one would be really helpful for Fiji in developing the local workforce.

As has been explained, the collaboration between government and academia in Fiji has already been helpful specifically for the cybersecurity area in the country, however, continuing investing in this collaboration could bring even greater results for developing both artificial intelligence and cybersecurity which will bring a bright future for the nation.

5.7.3 GOVERNMENT – PRIVATE COLLABORATION

The next collaboration that should be explored is between the government and the private sector, as both have a significant role in strengthening Fiji's AI and cybersecurity landscape. These two sectors have already collaborated in various initiatives aimed at enhancing digital security and innovation.

For example, the Fijian government has partnered with private tech companies to improve cybersecurity awareness and digital infrastructure. A notable initiative is Samsung's collaboration with the Ministry of Education, which focuses on digital transformation in schools [71]. By integrating digital learning tools, this partnership indirectly supports the development of AI and cybersecurity skills among Fiji's youth.

Another key collaboration is between the Fijian government and local telecommunications companies, which have worked together to strengthen the country's cybersecurity infrastructure [69]. An example of this is Telecom Fiji which worked with the Fiji Police force to boost their cybersecurity, systems and data resiliency.

Another example of a government-private sector collaboration is the World Bank's KoDi initiative, which is assisting Fiji in implementing its National Digital Strategy [70]. This initiative focuses on strengthening digital infrastructure and cybersecurity adoption through partnerships between the government and international technology providers. By providing global expertise and funding, the KoDi initiative ensures that Fiji can develop secure digital services, expand internet accessibility, and build a resilient cybersecurity framework aligned with global standards.

The collaborations mentioned should only be the beginning of a deeper engagement between the government and private sector. Looking at other countries, several initiatives demonstrate the impact of public-private partnerships in advancing AI and cybersecurity:

A non-profit organization in New Zealand has developed an AI Forum [64], which brings together government policymakers, private tech companies, and researchers to develop ethical AI applications and cybersecurity policies which bring a collaborative environment

to develop AI in the country. This initiative could really make a change in Fiji since AI has not yet been used as much as it can be.

Many countries, including Australia and Singapore, provide government-backed grants to encourage private companies to invest in AI and cybersecurity research, introducing this innovation programs will deeply enhance the AI and cybersecurity of Fijian companies.

Strengthening the government-private sector partnership is critical to advancing Fiji's cybersecurity resilience and AI capabilities. By adopting successful models from other nations, Fiji can expand cybersecurity infrastructure, enhance innovation, and prepare the workforce for a digital future.

5.7.4 ACADEMIA – PRIVATE SECTOR COLLABORATION

The last collaboration that will be explored is between the academic sector and private companies, as both play a key role in developing Fiji's AI and cybersecurity capabilities. While universities provide research, training, and skilled graduates, private sector companies contribute to technology, funding, and real-world implementation of innovative solutions.

One example of this collaboration is the partnership between the University of the South Pacific, Cisco, and Telecom Fiji [67]. In 2023, these organizations signed an agreement to establish a Digital Skills Hub, which includes a cybersecurity lab, design-thinking workshop, collaboration workspaces, and other digitally enabled platforms to provide the students of USP with increased access to digital skills training. This initiative allows the private sector to invest in Fiji's digital workforce, ensuring that graduates are equipped with industry relevant skills.

While academia and private companies in Fiji have started working together, there are more opportunities to strengthen these partnerships by learning from successful international models:

Some universities in New Zealand are collaborating with Google, Microsoft, and local cybersecurity firms to create AI research labs that develop smart cybersecurity defenses and AI-driven security monitoring [68]. Encouraging these opportunities would help the country to bring innovation to AI and cybersecurity.

In countries like Singapore and Canada, big tech firms fund university cybersecurity internships to train the next generation experts. This implemented in Fiji would help students to work with AI security teams, conduct hacking training, etc…

Collaboration between academia and the private sector is crucial for building a skilled workforce, accelerating innovation, and strengthening Fiji's digital defenses. While initiatives like the USP-Cisco-Telecom Fiji partnership are steps in the right direction, expanding industry-funded AI and cybersecurity research, establishing innovation hubs, and creating specialized internships will further position Fiji as a leader in AI-driven cybersecurity solutions in the Pacific region.

5.7.5 CONCLUSION

The future of AI and cybersecurity in Fiji depends on strong collaboration between government, academia, and the private sector. Existing partnerships such as USP's cybersecurity initiatives, Telecom Fiji's digital infrastructure projects, and the World Bank's KoDi initiative have already made a significant impact.

However, there are more opportunities to strengthen these collaborations by adopting successful models from Australia, New Zealand, and other global leaders. Initiatives such as government-funded cybersecurity research centers, AI innovation hubs, and industry sponsored university programs can accelerate Fiji's progress in AI-driven security solutions. Encouraging more public-private-academic partnerships will enable innovative research, a skilled cybersecurity workforce, and the development of national AI policies.

As Fiji continues its digital transformation journey, it is crucial to encourage an environment of cooperation and innovation. Strengthening existing partnerships, exploring new collaborations, and learning from global best practices will be essential for the country's evolution regarding AI and cybersecurity. By working together, the government, academia, and the private sector can build a secure, digital future for Fiji.

5.8 CHALLENGES IN CYBER SECURITY IMPLEMENTATION

5.8.1 INTRODUCTION

In the global fight against cyber threats, each country brings its own set of opportunities and challenges. For Fiji, these challenges are particularly pronounced.

As Fiji goes through its digital transformation, organizations face many challenges when implementing cybersecurity measures. The challenges come in all shapes, from a lack of access to trained professionals to the absence of proper technological infrastructure. In addition to these issues there is the high cost of sophisticated solutions and regulatory frameworks that often struggle to keep pace with technological change.

By analyzing the challenges that cybersecurity measures implementation will bring to the country and how these barriers will impact organizations we aim to highlight the key areas where intervention and innovation are most needed.

Understanding these difficulties is essential to create a secure digital environment, not only in Fiji but also in other nations with similar socioeconomic and technological profiles. By addressing these issues, Fiji has the potential to emerge as a model for resilient and adaptable cybersecurity in other developing regions.

5.8.2 CHALLENGES

Let's start talking about the specific challenges that Fiji will face when implementing cybersecurity measures. The first obstacle that we should mention is the lack of trained professionals in the country. Similar to what was previously stated in Chapter 2 AI Adoption in Fiji: Opportunities and Challenges, at this moment the country does not count with a highly skilled workforce to implement cybersecurity measures in all the needed industries, however in the case of cybersecurity, the Fijian government has defined in the National Development Plan the mentioned field as high priority so is expected that in the following

years the cybersecurity skilled professionals number will increase significantly. Having that in mind, the measures that should be implemented before the workforce is developed should be simpler and using easier technologies as the workforce continues to evolve in the following years, the organizations will be able to switch to more sophisticated solutions.

Currently, security solutions are exponentially increasing their cost especially when looking at sophisticated or advanced solutions. To make an analysis of the pricing for the different solutions, the focus will be in small to medium business since as said by the Asian Development Bank the 82.4% [60] of business in Fiji belongs to that category and those are the ones that will have more difficulties to use this solutions. Basic antivirus software ranges from 30 to 50$ per user per year, assuming there are on average around 30 people in those companies, the total cost increases up to 900 to 15000 $ per year. Regarding intrusion detection and prevention systems, there are open-source solutions, but they require skilled professionals to use them, on the other hand there are commercial solutions which are easier to work with but cost around 5000$.

Regarding intrusion detection and prevention systems, while open-source solutions like Snort or Zeek are available at no direct licensing cost, they require skilled professionals for setup, monitoring, and maintenance. For small businesses with limited IT expertise, these hidden labor costs can be prohibitive. Alternatively, commercial solutions, which offer user-friendly interfaces and integrated support, typically start at $5,000 for small-scale deployments. These commercial solutions, while easier to adopt, represent a substantial upfront investment for SMBs in Fiji.

Network security tools such as Virtual Private Networks are also critical for protecting business communications. Business-grade VPN services cost $5 to $15 per user monthly. For a company of 30 employees, this translates to an annual cost of $1,800 to $5,400. Implementing a hardware VPN solution, which provides enhanced security for on-premises networks, requires an additional investment of $1,000 to $5,000.

Backup and recovery systems, essential for data protection, cost between $1,000 and $5,000 annually for SMBs, depending on the volume of data and required features like cloud

redundancy. Enterprise-grade options with advanced capabilities can exceed $10,000 annually, which is often beyond the financial capacity of many Fijian SMBs.

Endpoint detection and response solutions, which provide advanced threat protection at the device level, cost $20 to $50 per endpoint monthly. For 30 devices, this amounts to $7,200 to $18,000 annually. Such tools are critical in modern cybersecurity but present a significant expense.

For SMBs in Fiji, advanced tools like AI-powered threat detection systems are largely inaccessible due to their high costs, which start at $100,000 annually for small-scale setups. Managed Security Services, which outsource cybersecurity needs to third-party providers, may offer a more affordable option, costing $1,000 to $10,000 per month depending on the services included.

In conclusion, while basic solutions like antivirus software and VPNs are more financially feasible for Fijian SMBs, advanced cybersecurity tools remain cost-prohibitive for most. Strategic investments, or regional collaborations may be necessary to make these technologies accessible to the majority of businesses.

The final challenge Fiji faces when implementing cybersecurity measures is not just about deployment but also about ensuring that these measures are properly used. This relates to the lack of cybersecurity awareness among the general population, employees, and even decision-makers within organizations. Without sufficient understanding of cyber risks and best practices, even the most sophisticated security measures can be ineffective.

A significant portion of cybersecurity breaches occur because of human error whether through weak passwords, falling victim to phishing scams, or mishandling sensitive data. In Fiji, the level of cybersecurity awareness remains low, with many individuals and businesses underestimating the risks posed by cyber threats. Many small to medium enterprises lack formal cybersecurity policies, and employees may not be trained to recognize or respond to threats appropriately.

Additionally, there is often a perception that cybersecurity is solely an IT department concern rather than an organizational-wide responsibility. This mindset leads to poor security practices across various industries, increasing the risk of cyber incidents. Even in sectors handling sensitive data, such as finance and healthcare, cybersecurity protocols are sometimes seen as secondary priorities.

5.8.3 CONCLUSION

The implementation of cybersecurity measures in Fiji is met with a range of challenges, each requiring attention to overcome. The shortage of skilled professionals, high costs of security solutions, infrastructure limitations, regulatory gaps, and low cybersecurity awareness all contribute to the complexity of securing Fiji's digital landscape.

The current gaps in knowledge, awareness and workforce skill make it difficult for organizations to maintain secure systems, leaving them vulnerable to cyber threats. Without widespread understanding and adoption of cybersecurity best practices, the risks associated with cyber incidents will continue to grow, affecting businesses, government institutions, and individuals.

For Fiji to successfully and securely continue with its digital transformation, these challenges must be fully recognized and addressed. Only through a clear understanding of these barriers can effective strategies be developed to protect the country's digital infrastructure and data integrity.

5.9 FUTURE DIRECTIONS FOR AI AND CYBER SECURITY IN FIJI

5.9.1 INTRODUCTION

While Fiji has made significant progress towards developing a mature cybersecurity and artificial intelligence environment, much remains to be done to fully utilize its potential. As technology continues to evolve, the country must proactively address emerging threats, capitalize on new opportunities, and establish robust frameworks for AI and cybersecurity solutions.

This chapter explores the future directions for cybersecurity and AI in Fiji, focusing on key opportunities, and strategic approaches that can help the nation to stay ahead of new challenges. By examining global trends, policy considerations, and workforce development needs, a roadmap will be designed for Fiji's digital resilience and innovation for the following years.

5.9.2 AI AND CYBERSECURITY POLICIES

To prepare for future challenges, Fiji must enhance its regulatory frameworks by developing AI governance policies that ensure ethical and responsible AI use. Strengthening cybersecurity laws will help the nation keep pace with emerging threats and evolving technologies, while enhanced data protection measures can protect personal and corporate information. Collaboration between government, private industries, and academic institutions will be crucial in shaping robust cybersecurity policies. Ethical considerations must be central to AI governance, with transparency requirements that ensure AI-driven processes are clear and transparent.

Fiji must also establish guidelines for AI in cybersecurity that define acceptable uses, and privacy safeguards. Legal frameworks should be adapted to cover AI-specific risks, including algorithmic bias, automated decision-making, and the implications of AI-driven cyber threats. A national AI ethics board could oversee AI deployment in critical sectors,

ensuring compliance with established best practices. Furthermore, Fiji should align its AI policies with global regulations to facilitate international cooperation and attract technology investments. Learning from other frameworks such those in Europe or the US can be of great help to improve their own in a rapid manner.

5.9.3 CYBERSECURITY ECOSYSTEM

For Fiji to remain secured against cyber threats, it must invest in its national cybersecurity infrastructure and response mechanisms. Public awareness campaigns should be done to promote good cyber practices among citizens and businesses, specially since the global problem of phishing. Developing incident response teams (CERT) and emergency response plans will help mitigate the impact of cyber incidents. AI-driven predictive analytics can also be used to anticipate and prevent cyber threats before they materialize, enhancing the nation's proactive defense strategies.

Cybersecurity capacity-building efforts should work on a risk management perspective to start securing those areas that are more dangerous such as critical infrastructure, banking, healthcare, and government services. AI-powered cybersecurity tools, such as automated threat detection and response systems, should be integrated into national cybersecurity strategies. Furthermore, initiatives should be launched to increase cybersecurity awareness at all levels of society, from basic digital literacy for individuals to advanced security training for IT professionals. Establishing dedicated cybersecurity research centers will allow for ongoing innovation and exploration of security solutions.

5.9.4 WORKFORCE DEVELOPMENT

A strong cybersecurity and AI workforce is essential for Fiji's digital future. Expanding cybersecurity education programs in universities and technical institutions will help for the future cybersecurity workforce. Training programs and professional certifications should be

encouraged to upskill the current workforce, equipping professionals with expertise in AI and cybersecurity. Research and innovation must be prioritized by supporting projects that address Fiji's specific challenges in these fields.

Collaboration between industries, government bodies, and academia can drive the development of cutting-edge cybersecurity solutions. Additionally, offering scholarships and financial incentives will encourage students to pursue careers in AI and cybersecurity. Establishing AI and cybersecurity bootcamps can provide intensive, hands-on training to accelerate workforce readiness.

Fiji should consider forming cybersecurity research hubs within universities to encourage security innovation. Encouraging startups to explore AI applications in cybersecurity could create employment opportunities and local innovation. Furthermore, government-funded research initiatives should support AI-based cybersecurity projects that address local cybersecurity vulnerabilities. Research collaboration with international institutions can provide opportunities to share knowledge and would give Fiji the opportunity to work with global AI and security advancements.

5.9.5 INTERNATIONAL COLLABORATION

Fiji can enhance its cybersecurity and AI capabilities by actively engaging with international organizations and adopting global best practices. Strengthening regional cybersecurity alliances with Pacific Island nations will allow for shared resources and knowledge exchange. Partnering with global cybersecurity institutions such as INTERPOL, ITU, and international CERTs can provide valuable expertise and threat intelligence. Securing international funding and investment opportunities can help finance the development of advanced security infrastructure.

Participation in global cybersecurity simulation exercises will ensure that Fiji remains prepared for evolving cyber threats. Aligning local policies with internationally recognized AI governance frameworks can facilitate seamless integration into the global AI and

cybersecurity ecosystem. Furthermore, joining AI research communities and engaging in international cybersecurity agreements can enable collaborative security initiatives with other nations, enhancing Fiji's resilience against cyber threats.

To build stronger international partnerships, Fiji should actively participate in AI and cybersecurity forums, conferences, and diplomatic initiatives. It should also become part of bilateral agreements with technology-leading nations to receive technical assistance and training. By international cooperation, Fiji can benefit from shared threat intelligence, best practices, and technological innovations that can significantly enhance its cybersecurity and AI capabilities.

5.9.6 RECOMMENDATIONS FOR THE FUTURE

To ensure a secure and AI-driven future, Fiji must develop a national AI and cybersecurity strategy that aligns technology adoption with regulatory frameworks. Strengthening digital infrastructure and implementing secure systems will be critical in preventing cyberattacks. Raising public awareness about cybersecurity risks and best practices should be a nationwide initiative to ensure businesses and citizens are well-prepared.

Encouraging local innovation and supporting startups in the AI-driven cybersecurity space will boost economic and technological growth. A culture of cyber resilience should be included within governmental and corporate structures, ensuring cybersecurity remains a priority across all sectors. AI-driven fraud prevention mechanisms should be incorporated into financial and government institutions to enhance security. Additionally, AI integration within Fiji's national cybersecurity frameworks will ensure that emerging technologies are effectively utilized to safeguard digital assets.

Further strategic initiatives should include the development of a cybersecurity command center to oversee national cyber defense measures. Additionally, Fiji should promote public-private partnerships to enhance cybersecurity capabilities through shared investments and

research. Finally, investment in cloud security measures should be prioritized as cloud computing continues to be a cornerstone of digital transformation.

5.9.7 CONCLUSION

The future of AI and cybersecurity in Fiji has an immense potential, but it requires planning and strategic investments. By strengthening regulatory policies, and creating a skilled workforce, Fiji can establish a secure and innovative digital ecosystem. Strong collaboration at national and international levels will be key to successfully navigating the evolving cybersecurity landscape.

As Fiji continues on its path of digital transformation, ensuring AI and cybersecurity initiatives align with long-term national objectives will be crucial. Through the combined efforts of government institutions, private sector stakeholders, academic researchers, and global partners, Fiji can position itself as a leader in AI-driven cybersecurity within the Pacific region. Investing in secure digital infrastructure, workforce development, and research collaboration will be fundamental in building a resilient and forward-looking digital future.

5.10 CONCLUSION AND RECOMMENDATIONS

5.10.1 SUMMARY OF KEY FINDINGS

Throughout this section, we have explored the transformative potential of artificial intelligence and the evolving cybersecurity landscape in Fiji. AI has emerged as a great tool for growth, capable of greatly enhancing industries such as agriculture, manufacturing, tourism, or public services. By leveraging AI-driven solutions, Fiji can enhance economic resilience and technological advancement.

However, the rapid digitalization of the nation also exposes it to increasing cyber threats, including phishing, ransomware, and data breaches. Critical infrastructure sectors, such as energy, healthcare, and finance, remain particularly vulnerable. Compounding these challenges are gaps in regulatory frameworks and workforce readiness. Fiji faces a shortage of highly skilled professionals and lacks enough regulations, which is slowing sustainable digital growth. Addressing these issues requires substantial investment in digital infrastructure and policy reforms.

Collaboration between government, academia, and the private sector has already begun to strengthen AI and cybersecurity capabilities. These partnerships will be crucial to fully harnessing global best practices. Lessons from Australia and New Zealand can be helpful to understand the effectiveness of AI-driven security measures, and investment in cybersecurity education as essential components for national security.

5.10.2 ACTIONABLE RECOMMENDATIONS FOR STAKEHOLDERS

To ensure a secure and AI-driven future, stakeholders must prioritize some strategic initiatives. The government should develop and implement a comprehensive AI strategy, aligning with long-term digital transformation goals. Establishing an AI governance framework will ensure responsible adoption while addressing issues such as bias,

transparency, and ethical AI use. Enhancing data protection laws by incorporating global best practices, such as the EU's GDPR, will safeguard citizens' privacy and digital rights.

Investment in digital infrastructure is necessary, including upgrades to national cybersecurity frameworks, cloud security enhancements, and AI-driven threat monitoring. The creation of a national AI-driven cybersecurity command center would centralize security operations and coordinate responses to cyber threats. Small and medium sized enterprises should receive financial incentives to adopt secure digital technologies.

Education and workforce development must also be strengthened. Universities and technical institutions should enhance AI and cybersecurity programs to close the existing skills gap. Government-sponsored cybersecurity boot camps and certification programs, in collaboration with international tech companies and universities, can provide hands-on training.

Public-private partnerships should be promoted to develop AI-driven cybersecurity solutions tailored to Fiji's specific challenges. Establishing innovation hubs and research centers will develop local talent and entrepreneurship. The private sector should be incentivized to invest in cybersecurity infrastructure through tax benefits and grants.

International collaboration is another essential aspect of Fiji's cybersecurity and AI strategy. Strengthening ties with global organizations, such as INTERPOL and ITU, will facilitate intelligence-sharing. Participation in global cybersecurity simulation exercises will enhance national preparedness against evolving threats. Moreover, establishing bilateral agreements with technology-leading nations will support knowledge-sharing, technical assistance, and workforce training.

5.10.3 STRENGTHENING AI AND CYBERSECURITY LEGISLATION

In addition to strategic investments, Fiji must refine its legal and regulatory framework to ensure responsible AI deployment and effective cybersecurity policies. The country should

introduce AI ethics guidelines to ensure transparency and accountability in decision-making processes. Additionally, strengthening cybercrime laws will enable authorities to respond swiftly to emerging digital threats.

Fiji's regulatory bodies must establish a structured certification process for AI-driven solutions to ensure compliance with security and ethical standards. Developing a standardized AI risk assessment framework similar to the one presented by the EU AI act will help organizations evaluate the safety and reliability of AI applications. These steps will foster public trust in AI while ensuring that cybersecurity policies evolve alongside technological advancements.

The country also lacks a specific legislative framework for critical infrastructure, this kind of regulation is essential for the country's security since an attack of this kind can have fatal consequences for the country. Designing a framework similar to the NIST CSF, would be helpful for Fiji's resilience against cyber threats.

Fiji also lacks regulation and guidelines for cybersecurity in private companies which leaves citizen unprotected in most companies right now. Developing a regulation similar to the European NIS 2 is the key to face this problem.

5.10.4 EXPANDING DIGITAL LITERACY AND PUBLIC AWARENESS

Public education initiatives must play a central role in building a resilient digital society. Fiji should implement nationwide digital literacy programs to educate citizens about cybersecurity best practices and AI's potential impact. Awareness campaigns targeting businesses and government agencies can help reinforce security measures and mitigate risks posed by cyber threats.

Moreover, introducing AI and cybersecurity topics into primary and secondary school will prepare future generations to navigate an increasingly digital world. Providing online

resources and workshops will empower individuals and organizations to adopt AI and cybersecurity solutions effectively.

5.10.5 CONCLUSION

Fiji stands at an important moment in its digital journey, presenting both immense opportunities and significant challenges. Proactively investing in AI adoption, strengthening cybersecurity measures, and creating a culture of innovation will enable Fiji to lead in AI-driven cybersecurity within the Pacific region.

A collaborative approach involving government agencies, private sector stakeholders, academic institutions, and international partners is essential to achieving this vision. Through strategic planning, policy reforms, and workforce development, Fiji can build a secure and innovative digital ecosystem.

The path ahead demands continuous adaptation and commitment, but with the right initiatives in place, Fiji is poised to harness the power of AI and cybersecurity for national prosperity.

SECTION 6 DASHBOARDS

To enhance the visualization of the Fiji cybersecurity and AI current state comparing it to other countries and giving actionable recommendations. Some dashboards have been developed. These Dashboards are divided into 6 different tabs, each tab shows information about some specific topic, these are the selected topics:

- AI Adoption
- Threat Landscape
- Workforce Development
- Policy Comparison
- Cybersecurity Solutions Costs
- Challenges and Recommendations

6.1 AI ADOPTION TAB

This tab includes dashboards that show the impact that AI can have in the most important sectors in Fiji, and it also includes some success stories of AI already implemented in the country.

6.1.1 DATA BY SECTOR

In this section there is a dashboard that allows the user to select one of the following industries: Tourism, manufacturing, agriculture or public sector. In figures [15-18], there are presented all the different outputs for each industry, here it can be seen the use cases for what AI can be used, the challenges for AI in that industry and the productivity estimated

gain when it can be estimated. In the tourism and public sector industries there is difficult to give an estimation of productivity gain, so it has been avoided.

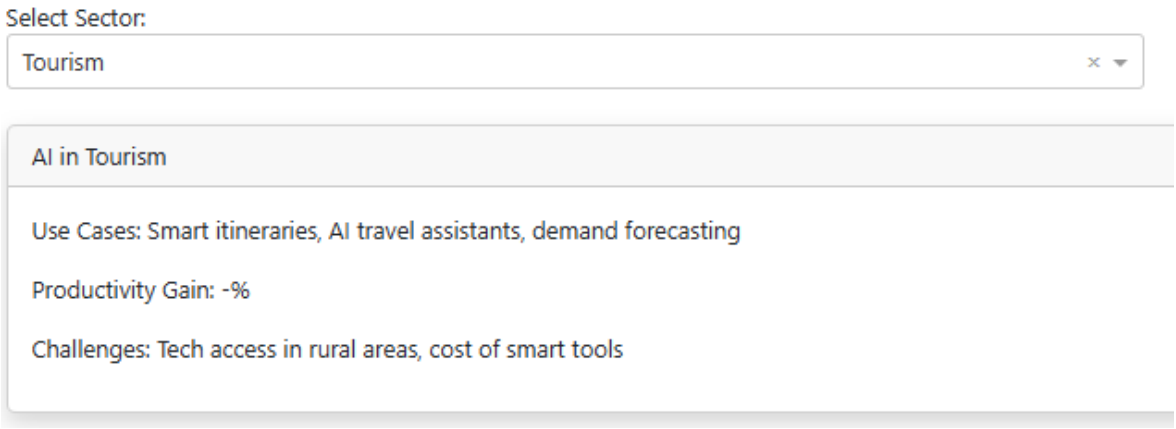

Figure 18. AI in Tourism Dashboard

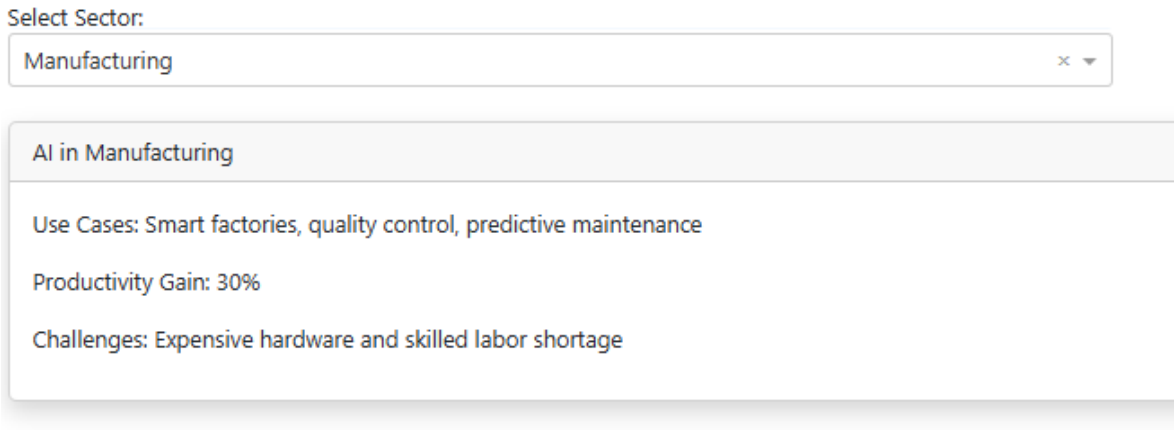

Figure 19. AI in Manufacturing Dashboard

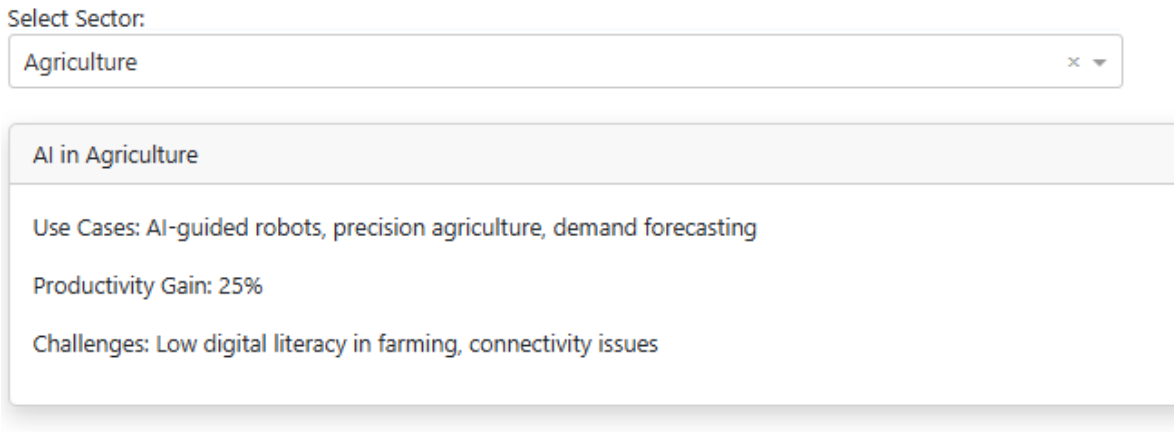

Figure 20. AI in Agriculture Dashboard

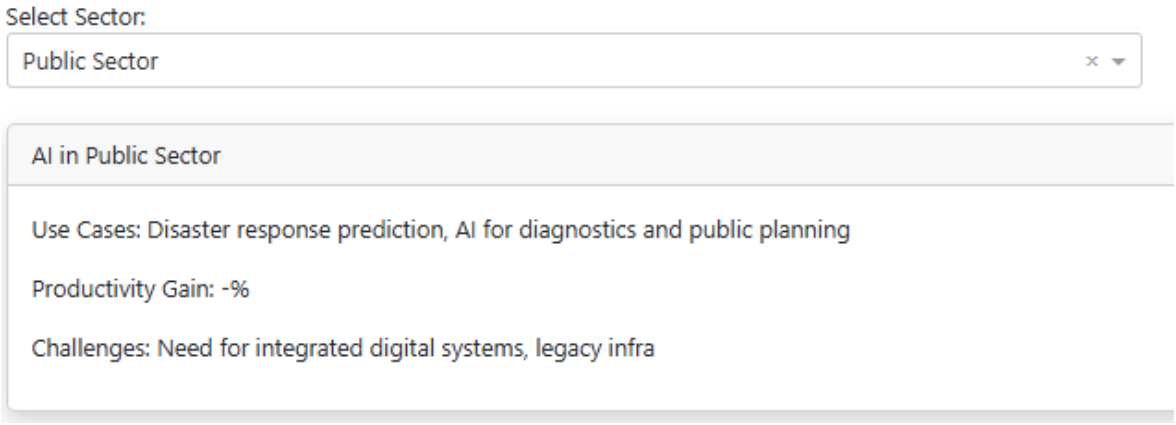

Figure 21. AI in the Public Sector Dashboard

6.1.2 SUCCESS STORIES IN FIJI

This is the last section regarding AI adoption in Fiji, in Figure 22, it is shown some success stories of AI been implemented in Fiji in a card format.

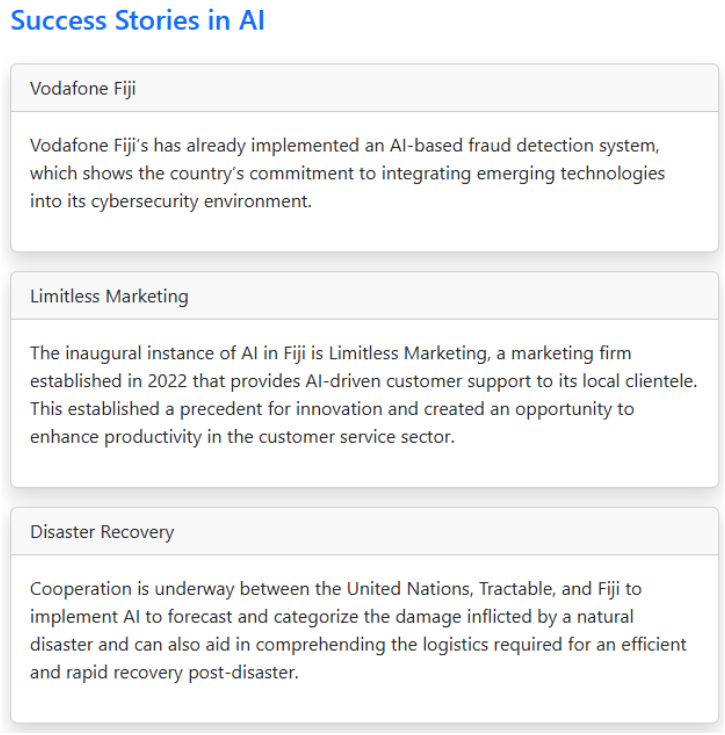

Figure 22. Success Stories of AI in Fiji

6.2 THREAT LANDSCAPE

This tab contains information regarding the threat landscape of Fiji, since currently there are no official statistics about Fiji specific situation some of the dashboard find here will refer to other countries or worldwide. However, this will help the understanding of the most important threats globally and therefore the most important threats for the islands.

6.2.1 MOST COMMON CYBERATTACKS GLOBALLY

This section presents a dashboard (Figure 23) displaying the most common cybercrimes worldwide. The dashboard includes interactive features that allow users to selectively hide specific cybercrimes via the legend, enabling focused comparisons among selected

categories. Additionally, clicking on a section of the graph reveals a brief description of the corresponding cybercrime.

Figure 23. Most Common Cybercrimes Globally Dashboard

6.2.2 SHARE OF ATTACKS BY INDUSTRY

This section shows a dashboard similar to the one shown in Figure 23, however as shown in Figure 24, in this case the pie graph is form by different industries and how many attacks target those industries. Similar to the most common cybercrime dashboard, you can hide some industries by selecting them in the legend. When clicking on a section of the graph extra information is also revealed, here you can find a description of the industry in Fiji and the most common types of attacks that target that industry.

Figure 24. Share of Attacks by Industry Dashboard

6.2.3 CYBERATTACKS GROWTH

Here there are three different dashboards ,Figure 25, Figure 26, Figure 27. These dashboards show how different attacks are growing in the US and worldwide in the past years. These graphs do an excellent job showing how year by year every attack is affecting more companies, which means as well an increasing importance in cybersecurity each year.

Figure 25. US Data Breaches Growth over the years

Figure 26. Share of Companies Affected by Ransomware Worldwide

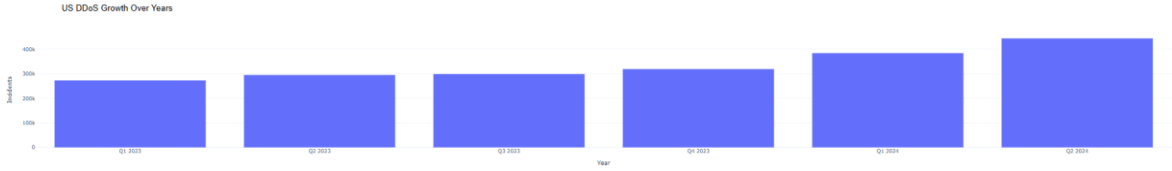

Figure 27. US DDoS Incidents over the years

6.2.4 CYBERATTACKS IN FIJI

This small section, show the most relevant cyberattacks that occurred in Fiji area in the last years. This can show the most dangerous threats currently for the islands. This attacks as shown in Figure 28, are the Suva Ransomware attack, the Pacific area cyber espionage and the pacific forum breach.

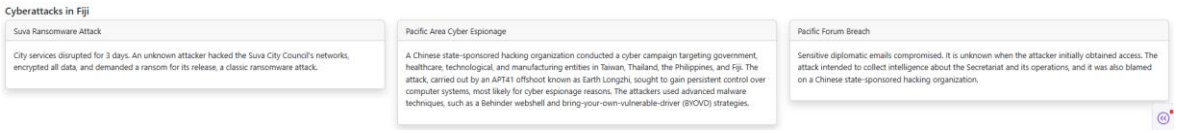

Figure 28. Most Relevant Cyberattacks in Fiji

6.3 WORKFORCE DEVELOPMENT

This tab focuses on how the current workforce is prepared for the cybersecurity challenge that the country is facing and how the country is trying to close the cybersecurity skill gap in order to be better prepared for future challenges.

6.3.1 STEM STUDENTS IN FIJI AND OTHER COUNTRIES

Figure 29 and Figure 30 show the situation regarding STEM students in Fiji. Figure 29 compares the percentage of STEM graduates in the Fiji with other countries which can be a way of measuring how well is the workforce prepared to face technical challenges. Figure 30 represents the number and percentage (according to other degrees) of STEM students in Fiji, which is used to visualize the tendency of growth for the following years.

Figure 29. Comparison of STEM students %

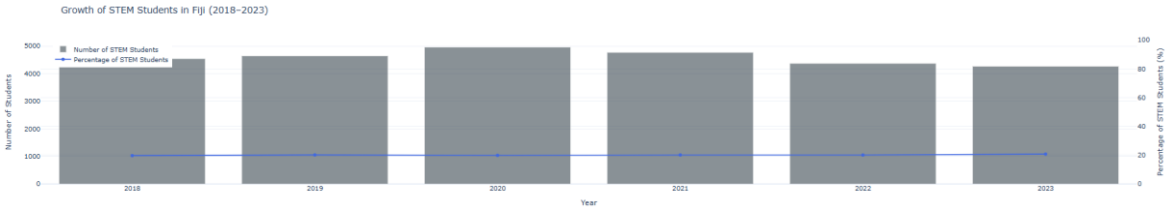

Figure 30. Growth of STEM students in Fiji

6.3.2 INITIATIVES TO CLOSE SKILL GAP

The last section of the tab showed in Figure 31, shows the different current initiatives in Fiji to close the skill gap in cybersecurity. These are divided into national strategies, scholarship programs and industry collaborations, this section allows to click in each one of these categories and read the different strategies on each one.

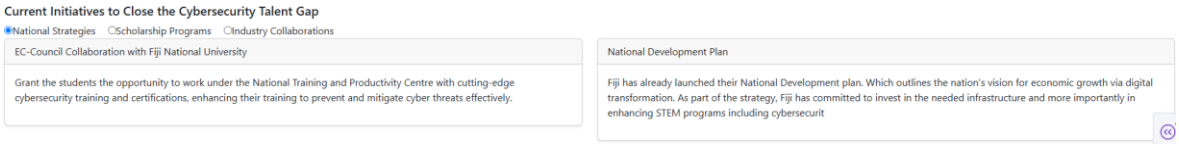

Figure 31. Current Fiji Initiatives to close skill gap

6.4 POLICY COMPARISON

This tab contains only one dashboard (Figure 32), which shows a comparison regarding policies in different regions, this dashboard allows the user to select a topic between AI, data privacy, critical infrastructure and cybercrime prosecution, and different regions. Once those are selected, it shows a comparison between those region and Fiji regarding the selected topic.

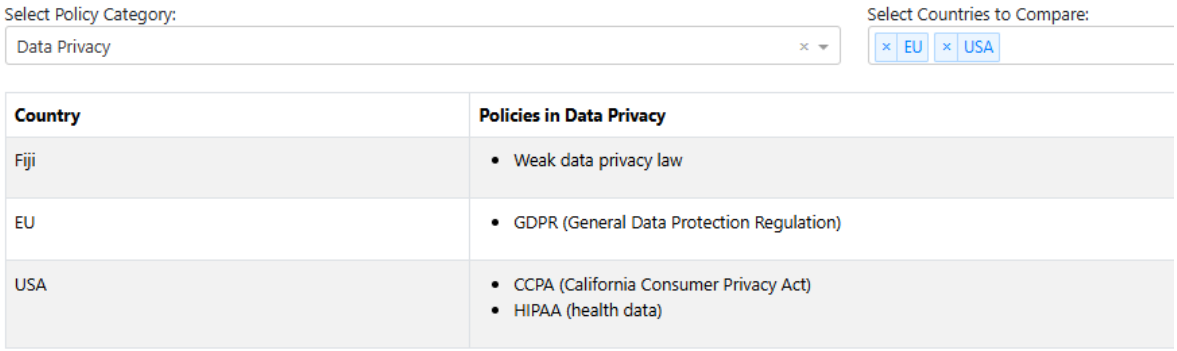

Figure 32. Policy Comparison

6.5 CYBERSECURITY IMPLEMENTATION COSTS

This tab shown in Figure 33, contains information about cybersecurity implementation costs for small to medium-sized companies which are the most likely to have problems when facing these implementation costs. It also shows the rate of SMEs (small to medium enterprises) in Fiji.

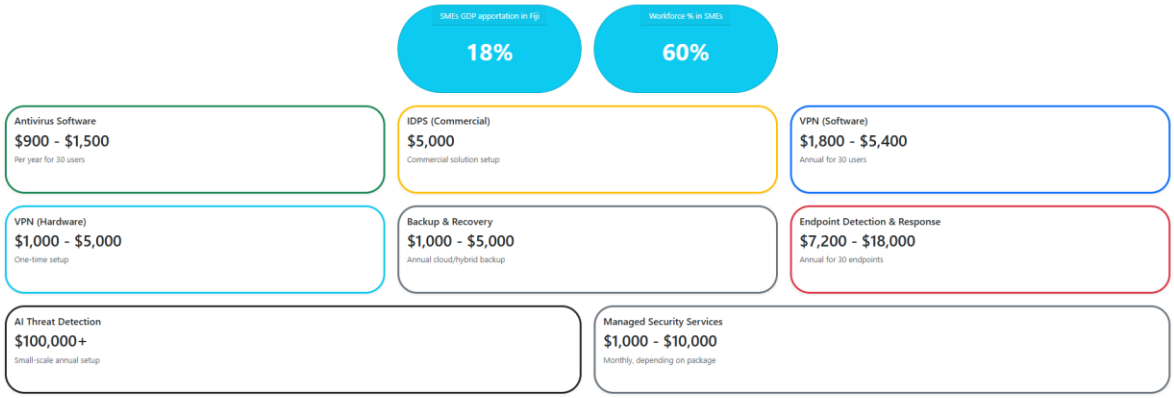

Figure 33. Cybersecurity implementation costs

6.6 CHALLENGES AND RECOMMENDATIONS

The last tab in the developed site, is shown in Figure 34, here there are explained the main challenges found in cybersecurity for Fiji. This tab also allows the user to see recommendations to face each one of these challenges by clicking in the view recommendations button.

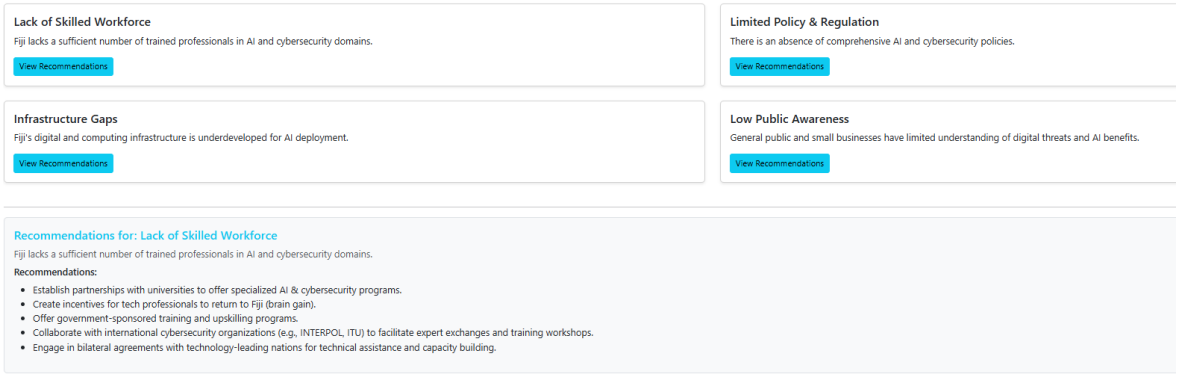

Figure 34. Challenges and Recomendations Tab

SECTION 7 CONCLUSIONS

This project has been considered a success, as it has effectively utilized ten comprehensive chapters to analyze the current state of artificial intelligence and cybersecurity in Fiji. Through detailed analysis and comparison with regional and international counterparts, it has identified key gaps in Fiji's digital landscape, from the absence of AI-specific legislation to the limited development of a cybersecurity workforce. Understanding these challenges has been essential for giving recommendations with the goal of supporting the country's secure digital transformation.

This comparative approach has helped identifying structural and policy-level weaknesses while also highlighting areas of opportunity, particularly in regional collaboration, capacity building, and creating new regulatory frameworks.

A central feature of this project has been the development of interactive dashboards that present the research findings in an accessible way. These tools offer a clear visualization of the challenges and proposed solutions, making it easier for policymakers, educators, and stakeholders to engage with the data and prioritize next steps.

Beyond its technical contributions, this work highlights the importance of safeguards, inclusive governance and closing the skill gap for keeping the current rapid infrastructure development potential of Fiji.

Looking ahead, there is a clear need for continued research and collaboration. As technologies such as AI continue to evolve, digital threats will evolve as well. This project serves as both a foundation and a call to action inviting stakeholders in Fiji to build on this work, deepen regional cooperation, and ensure that technological advancement supports Fijian well-being, economic resilience, and long-term security.

SECTION 8 CITATIONS

[1] USAID. (2022). Pacific Islands Digital Ecosystem Country Assessment. U.S. Agency for International Development. https://www.usaid.gov/digital-development/pacific-islands-deca

[2] Fiji Ministry of Finance. (2017). Fiji National Development Plan [Report]. Government of Fiji. Retrieved September 2024, from http://www.finance.gov.fj/NDP2017.pdf

[3] Fiji Village. (n.d.). *Local company loses $500,000 to an online scam*. Fiji Village. Retrieved November 13, 2024, from https://www.fijivillage.com/news/Local-company-loses-500000-to-an-online-scam--f8rx45/

[4] Fiji Government. (2021). *Fiji Cybercrime Act 2021* [Statutory instrument]. Retrieved September 8, 2025, from https://www.fiji.gov.fj

[5] Fiji Times. (2024, November 1). *Artificial intelligence to be a cornerstone of NDP*. The Fiji Times. https://www.fijitimes.com.fj/artificial-intelligence-to-be-a-cornerstone-of-ndp/

[6] Azeemah, A. (2024, May 27). *Fijian in AI platform*. The Fiji Times. Retrieved from https://www.fijitimes.com.fj/fijian-in-ai-platform/

[7] Javaid, M., Haleem, A., Khan, I. H., & Suman, R. (2023). Understanding the potential applications of Artificial Intelligence in Agriculture Sector. Advanced Agrochem, 2(1), 15-30. https://doi.org/10.1016/j.aac.2022.10.001

[8] Elufioye, Oluwafunmi & Ike, Chinedu & Odeyemi, Olubusola & Usman, Favour & Mhlongo, Noluthando. (2024). AI-DRIVEN PREDICTIVE ANALYTICS IN AGRICULTURAL SUPPLY CHAINS: A REVIEW: ASSESSING THE BENEFITS AND CHALLENGES OF AI IN FORECASTING DEMAND AND OPTIMIZING SUPPLY IN AGRICULTURE. Computer Science & IT Research Journal. X. 1-10. 10.51594/csitrj.v5i.

[9] Pokotylo, P. (2024, December 4). *AI in Agriculture: Revolutionizing Crop Management and Yield Prediction*. Keymakr. Retrieved from https://keymakr.com/blog/ai-in-agriculture-revolutionizing-crop-management-and-yield-prediction/

[10] Padhiary, M., Saha, D., Kumar, R., Sethi, L. N., & Kumar, A. (2024). Enhancing precision agriculture: A comprehensive review of machine learning and AI vision applications in all-

terrain vehicle for farm automation. *Smart Agricultural Technology*, 8, 100483. https://doi.org/10.1016/j.atech.2024.100483

[11] Deloitte. (2024). *2024 Manufacturing Industry Outlook*. Retrieved from https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook-2024.html

[12] globalEDGE. (n.d.). *Fiji: Economy*. Michigan State University. Retrieved February 12, 2025, from https://globaledge.msu.edu/countries/fiji/economy

[13] Knoema – Contribution of travel and tourism to GDP (% of GDP) – Fiji Knoema. (n.d.). *Contribution of travel and tourism to GDP (% of GDP) – Fiji*. Retrieved February 12, 2025, from https://knoema.com/atlas/Fiji/topics/Tourism/Travel-and-Tourism-Total-Contribution-to-GDP/Contribution-of-travel-and-tourism-to-GDP-percent-of-GDP

[14] Fiji Bureau of Statistics. (2025, January 15). Professional, scientific and technical activities – 2022 [Report]. Fiji Bureau of Statistics. Retrieved February 12, 2025, from https://www.statsfiji.gov.fj/professional-scientific-and-technical-activities-2022/

[15] World Economic Forum. (2020, January). *Natural disasters, resilience and relief: Artificial intelligence & McKinsey*. Retrieved September 10, 2024, from https://www.weforum.org/stories/2020/01/natural-disasters-resilience-relief-artificial-intelligence-ai-mckinsey/

[16] Tractable. (2022, October 31). *Tractable and United Nations team up to bring the power of artificial intelligence to natural disaster recovery in Fiji*. Retrieved Septermber 10, 2024, from https://tractable.ai/tractable-and-united-nations-team-up-to-bring-the-power-of-artificial-intelligence-to-natural-disaster-recovery-in-fiji/

[17] Statista. (2024, December 10). *Data breaches recorded in the United States by number of breaches and records exposed*. Statista. Retrieved October 1, 2024, from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[18] Statista. (2023, September 20). *Share of worldwide cyber attacks by type* [Chart]. Statista. Retrieved October 1, 2024, from https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/

[19] IBM. (2024). *Data breach reports*. IBM. Retrieved October 2, 2024, from https://www.ibm.com/reports/data-breach

[20] The Hacker News. (2024, August). *DDoS attacks surge 46% in first half of 2024*. The Hacker News. Retrieved October 3, 2024, from https://thehackernews.com/2024/08/ddos-attacks-surge-46-in-first-half-of.html

[21] Cloudbric. (2021, January 14.). *How much will a DDoS attack cost your business?* Retrieved October 3, 2024, from https://www.cloudbric.com/how-much-will-a-ddos-attack-cost-your-business/#:~:text=According%20to%20Ponemon%20Institute%20study,minute%20of%20downtime%20it%20causes

[22] Statista. (2024, November 9). *Businesses ransomware attack rate* [Data]. Retrieved October 2, 2024, from https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

[23] Syteca. (2024, March 25). *5 industries most at risk of data breaches* [Blog post]. Retrieved October 6, 2024, from https://www.syteca.com/en/blog/5-industries-most-risk-of-data-breaches

[24] Lakshmanan, R. (2023, May 3). Chinese hacker group Earth Longzhi resurfaces with advanced malware tactics. The Hacker News. Retrieved from https://thehackernews.com/2023/05/chinese-hacker-group-earth-longzhi.html

[25] Waqairadovu, A. (2024, September 23). SCC hit by major cyber breach. FBC News. Retrieved from https://www.fbcnews.com.fj/news/scc-hit-by-major-cyber-breach/

[26] Doran, M. (2024, September 12). Australia sends expert teams to Fiji as Chinese state-backed hackers attack Pacific Islands Forum. ABC News. Retrieved from https://www.abc.net.au/news/2024-09-12/chinese-state-backed-hackers-attack-pacific-islands-forum/104341412

[27] Reuters. (2024). Pacific Island nations at risk of becoming footholds for global crime gangs, says UN. Retrieved February 27, 2025, from https://www.reuters.com/world/asia-pacific/pacific-island-nations-risk-becoming-footholds-global-crime-gangs-says-un-2024-10-11/

[28] New York Post. (2025). US and allies must get tough on Russia, China's deep-sea cable sabotage. Retrieved February 27, 2025, from https://nypost.com/2025/02/26/opinion/us-must-get-tough-on-russia-chinas-deep-sea-cable-sabotage/

[29] The Wall Street Journal. How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons. Retrieved February 27, 2025, from https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95

[30] Water Power Magazine. (March, 2019). *Under cyber attack*. Retrieved February 13, 2025, from https://www.waterpowermagazine.com/analysis/under-cyber-attack-7051600/?cf-view

[31] National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[32] AI policy in Europe: From principles to practices - IBM policy. Accessed September 27, 2024. https://www.ibm.com/policy/ai-act/.

[33] Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors (Basel, Switzerland)*, *22*(14), 5105. https://doi.org/10.3390/s22145105

[34] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[35] European Data Protection Supervisor. (2022). EU-wide cybersecurity requirements to protect privacy and personal data. European Data Protection Supervisor. https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/eu-wide-cybersecurity-requirements-protect-privacy-and-personal-data_en

[36] Sandra Schmitz-Berndt, Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyad009, https://doi.org/10.1093/cybsec/tyad009

[37] Cezary Banasiński, Marcin Rojszczak, Cybersecurity of consumer products against the background of the EU model of cyberspace protection, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab011, https://doi.org/10.1093/cybsec/tyab011

[38] "Artificial Intelligence Act: Parliament to Adopt Landmark Law: 11-03-2024: News: European Parliament." Artificial Intelligence Act: Parliament to adopt landmark law | 11-03-2024 | News | European Parliament. Accessed September 26, 2024. https://www.europarl.europa.eu/news/en/agenda/briefing/2024-03-11/0/artificial-intelligence-act-parliament-to-adopt-landmark-law.

[39] European Parliament & Council. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on the security of network and

information systems (NIS2). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[40] World Bank. (n.d.). School enrollment, tertiary (% gross) [Data set]. World Bank. Retrieved November 23, 2024, from https://data.worldbank.org/indicator/SE.TER.ENRR?end=2023&locations=FJ-AU-NZ&start=1970&view=chart

[41] University of Fiji. (2018). University of Fiji annual report 2018 [Annual report]. University of Fiji. Retrieved November 23, 2024, from https://www.unifiji.ac.fj/annual-report/2018/

[42] University of Fiji. (2019). University of Fiji annual report 2019 [Annual report]. University of Fiji. Retrieved November 23, 2024, from https://www.unifiji.ac.fj/annual-report/2019/

[43] University of Fiji. (2020). University of Fiji annual report 2020 [Annual report]. University of Fiji. Retrieved November 23, 2024,, from https://www.unifiji.ac.fj/annual-report/2020/

[44] University of Fiji. (2021). University of Fiji annual report 2021 [Annual report]. University of Fiji. Retrieved November 23, 2024,, from https://www.unifiji.ac.fj/annual-report/2021/

[45] University of Fiji. (2022). University of Fiji annual report 2022 [Annual report]. University of Fiji. Retrieved November 23, 2024,, from https://www.unifiji.ac.fj/annual-report/2022/

[46] Fiji National University. (2018). Fiji National University annual report 2018 [Annual report]. Fiji National University. Retrieved November 26, 2024, from https://www.fnu.ac.fj/about-fnu/publications/annual-report-2018/

[47] Fiji National University. (2019). Fiji National University annual report 2019 [Annual report]. Fiji National University. Retrieved November 26, 2024, from https://www.fnu.ac.fj/about-fnu/publications/annual-report-2019/

[48] Fiji National University. (2020). Fiji National University annual report 2020 [Annual report]. Fiji National University. Retrieved November 26, 2024, from https://www.fnu.ac.fj/about-fnu/publications/annual-report-2020/

[49] Fiji National University. (2021). Fiji National University annual report 2021 [Annual report]. Fiji National University. Retrieved November 26, 2024, from https://www.fnu.ac.fj/about-fnu/publications/annual-report-2021/

[50] Fiji National University. (2022). Fiji National University annual report 2022 [Annual report]. Fiji National University. Retrieved November 26, 2024, from https://www.fnu.ac.fj/about-fnu/publications/annual-report-2022/

[51] University of the South Pacific. (2018). University of the South Pacific annual report 2018 [Annual report]. University of the South Pacific. Retrieved November 26, 2024, from https://www.usp.ac.fj/publications/archived-publications/usp-annual-report-2018/

[52] University of the South Pacific. (2019). University of the South Pacific annual report 2019 [Annual report]. University of the South Pacific. Retrieved November 26, 2024, from https://www.usp.ac.fj/publications/archived-publications/usp-annual-report-2019/

[53] University of the South Pacific. (2020). University of the South Pacific annual report 2020 [Annual report]. University of the South Pacific. Retrieved November 26, 2024, from https://www.usp.ac.fj/publications/archived-publications/usp-annual-report-2020/

[54] University of the South Pacific. (2021). University of the South Pacific annual report 2021 [Annual report]. University of the South Pacific. Retrieved November 26, 2024, from https://www.usp.ac.fj/publications/archived-publications/usp-annual-report-2021/

[55] University of the South Pacific. (2022). University of the South Pacific annual report 2022 [Annual report]. University of the South Pacific. Retrieved November 26, 2024, from https://www.usp.ac.fj/publications/archived-publications/usp-annual-report-2022/

[56] Australian Government, Department of Industry. (n.d.). University enrolment and completion: STEM and other fields [Data set]. Retrieved February 13, 2025, from https://www.industry.gov.au/publications/stem-equity-monitor/higher-education-data/university-enrolment-and-completion-stem-and-other-fields

[57] Fiji National University. (June 14, 2024). FNU partners with EC-Council to bolster cybersecurity workforce [Blog post]. Fiji National University. Retrieved February 13, 2025, from https://www.fnu.ac.fj/blog/news/fnu-partners-with-ec-council-to-bolster-cybersecurity-workforce/

[58] Outsource Fiji. (January 23, 2024). Outsource Fiji strengthens cybersecurity measures with training for 30 industry professionals. Outsource Fiji. Retrieved February 13, 2025, from https://outsourcefiji.com/outsource-fiji-strengthens-cybersecurity-measures-with-training-for-30-industry-professionals/

[59] Cyber Security CRC. (n.d.). Smart Shield: Artificial Intelligence Anti-Phishing System. Retrieved November 26, 2024, from https://cybersecuritycrc.org.au/smart-shield-artificial-intelligence-anti-phishing-system

[60] Cyber Security CRC and CSIRO Projects Named Winners at NSW iAwards CSIRO. (2022, July). Cyber Security CRC and CSIRO projects named winners at NSW iAwards. Retrieved

November 26, 2024, from https://www.csiro.au/en/news/all/news/2022/july/cyber-security-crc-and-csiro-projects-named-winners-at-nsw-iawards

[61] Cyber Security CRC. (n.d.). DECAAS: Cyber Deception Service. Retrieved November 26, 2024, from https://cybersecuritycrc.org.au/decaas-cyber-deception-service

[62] NEC Corporation. (2017, February 15). NEC AI in cybersecurity. Retrieved November 26, 2024, from https://dr.nec.com.onenec.net/en/global/techrep/journal/g17/n02/170215.html#top

[63] Cyber Security CRC. (n.d.). Who we are. Retrieved December 12, 2024, from https://cybersecuritycrc.org.au/who-we-are

[64] AI Forum NZ. (n.d.). AI Forum NZ. Retrieved December 13, 2024, from https://aiforum.org.nz/

[65] National Research Foundation Singapore. (n.d.). Snde FIS. Retrieved November 26, 2024, from https://www.nrf.gov.sg/rie-ecosystem/ecosystem-wide-fis/snde-fis/

[66] Asia Pacific Defence Reporter. (n.d.). Government grants awarded for AI research. Retrieved November 26, 2024, from https://asiapacificdefencereporter.com/government-grants-awarded-for-ai-research/

[67] Cisco. (2023, November 30). USP Telecom Fiji Cisco. Retrieved November 26, 2024, from https://news-blogs.cisco.com/apjc/2023/11/30/usp-telecom-fiji-cisco/

[68] University of Wellington. (n.d.). Artificial intelligence. Retrieved November 26, 2024, from https://www.wgtn.ac.nz/research/strengths/research-focus/artificial-intelligence

[69] Telecom Fiji. (2024, April 4). Fiji police engages Telecom for ICT services management. Retrieved November 26, 2024, from https://www.telecom.com.fj/telecom-fiji-knowledge/fiji-police-engages-telecom-for-ict-services-management/

[70] World Bank. (n.d.). World Bank's KODI supports Fiji in strengthening cybersecurity. Retrieved November 26, 2024, from https://www.worldbank.org/en/programs/kodi/brief/world-bank-s-kodi-supports-fiji-in-strengthening-cybersecurity

[71] St. Vincent Times. (2023, February 3). Fiji: Samsung will assist in the digitization school system. Retrieved November 26, 2024, from https://www.stvincenttimes.com/fiji-samsung-will-assist-in-the-digitization-school-system/

[72] Cyber Security CRC. (n.d.). Retrieved November 26, 2024, from https://cybersecuritycrc.org.au/

[73] IIT. (2024, May 22). Dawson collaborates with South Pacific nations on cybersecurity, AI issues. Retrieved November 26, 2024, from https://www.iit.edu/news/dawson-collaborates-south-pacific-nations-cybersecurity-ai-issues

[74] Asian Development Bank. (2023, October 25). *Job creation remains a challenge for micro, small, and medium-sized enterprises in Fiji*. Retrieved January 22, 2025, from https://www.adb.org/news/job-creation-remains-challenge-micro-small-and-medium-sized-enterprises-fiji

[75] World Bank. (2021). *Fiji Digital Government Transformation Project*. https://projects.worldbank.org/en/projects-operations/project-detail/P176203

[76] Hawk AI. (2024, November 5). *Hawk helps Vodafone Fiji fight financial crime*. https://hawk.ai/news-press/hawk-helps-vodafone-fiji-fight-financial-crime

[77] IBM. (2019, March 28). *IBM launches P-TECH in New Zealand to address digital skills shortage*. https://au.newsroom.ibm.com/2019-03-28-IBM-Launches-P-TECH-in-New-Zealand-to-Address-Digital-Skills-Shortage

ANEXO 1 SDGs

This project, focused on strengthening the cybersecurity and artificial intelligence (AI) landscape in Fiji, directly supports several of the United Nations Sustainable Development Goals (SDGs). As digital transformation accelerates, particularly in small island developing states like Fiji, addressing cybersecurity and AI development through a responsible and inclusive lens is essential for achieving sustainable development.

SDG 4 - Quality Education:

By emphasizing workforce development in cybersecurity and AI, this project promotes inclusive quality education and lifelong learning opportunities. It advocates for the upskilling and reskilling of Fijians, ensuring the local workforce is prepared for digital challenges and opportunities.

SDG 8 - Decent Work and Economic Growth:

Cybersecurity and AI sectors are rapidly growing fields. Investing in these areas enables job creation, supports innovation, and fosters economic resilience. For Fiji, building local capacity in these domains is essential to ensure sustainable economic growth, especially in a digitally driven global economy.

SDG 9 - Industry, Innovation and Infrastructure:

The project contributes to building resilient digital infrastructure and promotes inclusive and sustainable industrialization. Supporting AI and cybersecurity innovation ensures Fiji can participate in the global digital economy while safeguarding its critical systems.

SDG 16 - Peace, Justice and Strong Institutions:

Cybersecurity underpins national security, data privacy, and the integrity of institutions. By identifying regulatory gaps and promoting sound governance frameworks, this project

contributes to the development of effective, accountable, and transparent institutions at all levels.

SDG 17 - Partnerships for the Goals:

The project encourages national and international collaborations, among governments, academia, private sector, and civil society, which are essential for knowledge exchange, resource mobilization, and fostering innovation in cybersecurity and AI.

ANEXO 2 – DASHBOARD CODE

```
import dash
from dash import html, dcc, Input, Output
import dash_bootstrap_components as dbc
import pandas as pd
import plotly.express as px
import plotly.graph_objects as go
import numpy as np
from scipy import stats
from dash.dependencies import Input, Output, State, MATCH, ALL
from dash import callback_context
import plotly.graph_objects as go
from plotly.subplots import make_subplots


def create_cost_card(title, cost, description, color="primary"):
    return dbc.Card(
        dbc.CardBody([
            html.H5(title, className="card-title"),
            html.H2(cost, className="card-text"),
            html.P(description, className="text-muted"),
        ]),
        className=f"shadow-sm border-start border-4 border-{color} mb-4",
        style={"minWidth": "250px", "height": "180px","borderRadius":"40px"}
    )

# Sample AI sector data
sector_data = pd.DataFrame({
    'Sector': ['Tourism', 'Manufacturing', 'Agriculture', 'Public Sector'],
    'AI_Use_Case': [
        'Smart itineraries, AI travel assistants, demand forecasting',
        'Smart factories, quality control, predictive maintenance',
        'AI-guided robots, precision agriculture, demand forecasting',
        'Disaster response prediction, AI for diagnostics and public planning'
    ],
    'Productivity_Gain_%': ['-', 30, 25,'-' ],
    'Challenges': [
        'Tech access in rural areas, cost of smart tools',
        'Expensive hardware and skilled labor shortage',
        'Low digital literacy in farming, connectivity issues',
```

```
        'Need for integrated digital systems, legacy infra'
    ]
})

# Success stories
success_stories = [
    {"title": "Vodafone Fiji", "content": "Vodafone Fiji's has already implemented an
AI-based fraud detection system, which shows the country's commitment to integrating
emerging technologies into its cybersecurity environment."},
    {"title": "Limitless Marketing", "content": "The inaugural instance of AI in Fiji is
Limitless Marketing, a marketing firm established in 2022 that provides AI-driven
customer support to its local clientele.  This established a precedent for innovation
and created an opportunity to enhance productivity in the customer service sector."},
    {"title": "Disaster Recovery", "content": "Cooperation is underway between the
United Nations, Tractable, and Fiji to implement AI to forecast and categorize the
damage inflicted by a natural disaster and can also aid in comprehending the logistics
required for an efficient and rapid recovery post-disaster."}
]

# Threat types
threats = ['Phishing', 'Ransomware', 'Data Breach', 'DDoS']


# Policy comparison
policy_frameworks = {
    'Fiji': {
        'AI': ["No AI-specific laws"],
        'Critical Infrastructure': ["No dedicated law"],
        'Data Privacy': ["Weak data privacy law"],
        'Prosecuting cybercrimes': ["Cybercrime Act of 2021"]
    },
    'USA': {
        'AI': ["NIST AI Risk Management Framework"],
        'Critical Infrastructure': ["NIST Cybersecurity Framework (CSF)"],
        'Data Privacy': ["CCPA (California Consumer Privacy Act)", "HIPAA (health
data)"],
        'Prosecuting cybercrimes': ["Computer Fraud and Abuse Act (CFAA)", "Electronic
Communications Privacy Act (ECPA)"]
    },
    'EU': {
        'AI': ["EU AI Act (in progress)", "GDPR (data protection)"],
        'Critical Infrastructure': ["NIS2 Directive (Network and Information
Security)"],
        'Data Privacy': ["GDPR (General Data Protection Regulation)"],
```

```
        'Prosecuting cybercrimes': ["Directive on Attacks Against Information Systems",
"Budapest Convention on Cybercrime"]
    }
}

# Available categories for dropdown
policy_categories = ['AI', 'Critical Infrastructure', 'Data Privacy','Prosecuting
cybercrimes']

#Challenges and recommendations
fiji_challenges = {
    "Lack of Skilled Workforce": {
        "details": "Fiji lacks a sufficient number of trained professionals in AI and
cybersecurity domains.",
        "recommendations": [
            "Establish partnerships with universities to offer specialized AI &
cybersecurity programs.",
            "Create incentives for tech professionals to return to Fiji (brain gain).",
            "Offer government-sponsored training and upskilling programs.",
            "Collaborate with international cybersecurity organizations (e.g., INTERPOL,
ITU) to facilitate expert exchanges and training workshops.",
            "Engage in bilateral agreements with technology-leading nations for
technical assistance and capacity building."
        ]
    },
    "Limited Policy & Regulation": {
        "details": "There is an absence of comprehensive AI and cybersecurity
policies.",
        "recommendations": [
            "Develop a national AI strategy aligned with ethical principles.",
            "Draft and pass legislation on cybersecurity standards.",
            "Engage stakeholders across sectors to co-develop guidelines.",
            "Align local AI and cybersecurity policies with internationally recognized
governance frameworks (e.g., OECD AI Principles, GDPR).",
        ]
    },
    "Infrastructure Gaps": {
        "details": "Fiji's digital and computing infrastructure is underdeveloped for AI
deployment.",
        "recommendations": [
            "Invest in cloud and edge computing infrastructure.",
            "Upgrade internet connectivity in rural areas.",
            "Create public-private partnerships for infrastructure development."
```

```
        ]
    },
    "Low Public Awareness": {
        "details": "General public and small businesses have limited understanding of
digital threats and AI benefits.",
        "recommendations": [
            "Run nationwide awareness campaigns about cybersecurity hygiene.",
            "Promote responsible AI literacy in schools and media.",
            "Establish a national helpdesk for cybersecurity incidents."
        ]
    }
}
# App setup
app = dash.Dash(__name__, external_stylesheets=[dbc.themes.BOOTSTRAP])
app.title = "Fiji AI & Cybersecurity Dashboard"

# Layout
app.layout = dbc.Container([
    html.H2("Fiji AI & Cybersecurity Dashboard", className='text-center my-4'),

    dcc.Tabs(id='tabs', value='tab-ai', children=[
        dcc.Tab(label='AI Adoption', value='tab-ai'),
        dcc.Tab(label='Threat Landscape', value='tab-threats'),
        dcc.Tab(label='Workforce Development', value='tab-workforce'),
        dcc.Tab(label='Policy Comparison', value='tab-policy'),
        dcc.Tab(label='Challenges and Recommendations', value='tab-config'),
        dcc.Tab(label='Cybersecurity Solutions Costs', value='tab-costs')
    ]),

    html.Div(id='tabs-content')
], fluid=True)


@app.callback(Output('tabs-content', 'children'), Input('tabs', 'value'))
def render_tab(tab):
    if tab == 'tab-ai':
        return html.Div([
            dbc.Row([dbc.Col([
                html.Label("Select Sector:"),
                dcc.Dropdown(
                    id='sector-dropdown',
                    options=[{'label': s, 'value': s} for s in sector_data['Sector']],
                    value='Tourism'
                )
```

```
            ], width=4)]),
            html.Br(),
            html.Div(id='sector-info'),
            dcc.Graph(id='ai-productivity-graph'),
            html.H4("Success Stories in AI", className='my-4 text-primary'),
            dbc.Row([dbc.Col([
                dbc.Card([
                    dbc.CardHeader(story["title"]),
                    dbc.CardBody(html.P(story["content"]))
                ], className="mb-3 shadow") for story in success_stories
            ], width=4)])
        ])

    elif tab == 'tab-threats':
        common_attacks = pd.DataFrame({
            'Attack Type': ['Phishing', 'Data Breach', 'Delivery Scam', 'Extortion',
'Identity Theft','Others'],
            'Percentage': [53.2, 10.4, 9.2, 7, 5, 15.2]
        })
        fig_common_attacks = px.pie(
            common_attacks,
            names='Attack Type',
            values='Percentage',
            title='Most Common Cyberattacks Globally',
            hole=0.4,  # Donut style
            color_discrete_sequence=px.colors.sequential.RdBu
        )

        fig_common_attacks.update_traces(
            textinfo='label',
            hoverinfo='label+percent',
            hovertemplate='<b>%{label}</b><br>Share: %{percent}',
            pull=[0]*len(common_attacks),
            marker=dict(line=dict(color='#000000', width=1.5)),
            selector=dict(type='pie')
        )

        fig_common_attacks.update_layout(
            showlegend=True,
            legend_title_text='Cyberattack Type',
            legend=dict(orientation='h', y=-0.1),
            transition_duration=500
        )
```

```
        industry_attacks = pd.DataFrame({
            'Industry': ['Finance', 'Healthcare', 'Energy', 'Manufacturing',
'Retail','Public Administration','Education','Others'],
            'Percentages': [18.2, 6.3, 11.1, 25.7, 10.7, 4.3, 2.8, 20.9]
        })
        fig_industry_attacks = px.pie(
            industry_attacks,
            names='Industry',
            values='Percentages',
            title='Share of Attacks by Industry',
            hole=0.4,  # Donut style
            color_discrete_sequence=px.colors.sequential.RdBu
        )

        fig_industry_attacks.update_traces(
            textinfo='label',
            hoverinfo='label+percent',
            hovertemplate='<b>%{label}</b><br>Share: %{percent}',
            pull=[0]*len(common_attacks),
            marker=dict(line=dict(color='#000000', width=1.5)),
            selector=dict(type='pie')
        )

        fig_industry_attacks.update_layout(
            showlegend=True,
            legend_title_text='Industry',
            legend=dict(orientation='h', y=-0.1),
            transition_duration=500
        )

        # Example data for yearly growth
        data_breaches_growth = pd.DataFrame({
            'Year':
[2005,2006,2007,2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018,2019,2020, 2021,
2022, 2023],
            'Incidents': [157, 321, 446,
656,498,662,419,447,614,783,785,1099,1506,1175,1279,1108,1862,1802,3205]
        })
        years = data_breaches_growth['Year']
        incidents = data_breaches_growth['Incidents']

        # Perform linear regression
```

```
        slope, intercept, r_value, p_value, std_err = stats.linregress(years, incidents)

        # Calculate predicted values (trendline)
        trendline_values = intercept + slope * years

        # Create figure with the original line plot
        fig_breaches_growth = px.line(
            data_breaches_growth,
            x='Year', y='Incidents',
            title='US Data Breaches Growth Over Years',
            markers=True
        )

        # Add the linear regression trendline
        fig_breaches_growth.add_trace(
            go.Scatter(
                x=years,
                y=trendline_values,
                mode='lines',
                name='Trendline',
                line=dict(color='lightgray', width=2, dash='dash')
            )
        )

        # Optional: update layout to a light theme style
        fig_breaches_growth.update_layout(
            template='plotly_white',  # Light background theme
            title_font=dict(size=20, family='Arial', color='black'),
            xaxis_title='Year',
            yaxis_title='Incidents',
            legend=dict(x=0.7, y=1.1, bgcolor='rgba(255,255,255,0)',
bordercolor='rgba(0,0,0,0)'),
            hovermode='x unified'
        )
        #Ransomware growth
        ransom_growth = pd.DataFrame({
            'Year': [2018,2019,2020,2021,2022,2023],
            'Anual Share': [55.1, 56.1, 62.4, 68.5,71,72.7]
        })
        years = ransom_growth['Year']
        anual_share = ransom_growth['Anual Share']

        # Perform linear regression
```

```
        slope, intercept, r_value, p_value, std_err = stats.linregress(years,
anual_share)

        # Calculate predicted values (trendline)
        trendline_values = intercept + slope * years

        # Create figure with the original line plot
        fig_ransom_growth = px.line(
            ransom_growth,
            x='Year', y='Anual Share',
            title='Anual share of organizations affected by ransomware worldwide',
            markers=True
        )

        # Add the linear regression trendline
        fig_ransom_growth.add_trace(
            go.Scatter(
                x=years,
                y=trendline_values,
                mode='lines',
                name='Trendline',
                line=dict(color='lightgray', width=2, dash='dash')
            )
        )

        # Optional: update layout to a light theme style
        fig_ransom_growth.update_layout(
            template='plotly_white',  # Light background theme
            title_font=dict(size=20, family='Arial', color='black'),
            xaxis_title='Year',
            yaxis_title='Incidents',
            yaxis=dict(range=[0, 100]),
            legend=dict(x=0.7, y=1.1, bgcolor='rgba(255,255,255,0)',
bordercolor='rgba(0,0,0,0)'),
            hovermode='x unified'
        )

        #DDoS Growth
        DDoS_growth = pd.DataFrame({
            'Year': ['Q1 2023','Q2 2023','Q3 2023','Q4 2023','Q1 2024','Q2 2024'],
            'Incidents': [274000, 296000, 300000,320000, 385000,445000]
        })
        years = DDoS_growth['Year']
```

```
        incidents = DDoS_growth['Incidents']

        # Create figure with the original line plot
        fig_DDoS_growth = px.bar(
            DDoS_growth,
            x='Year', y='Incidents',
            title='US DDoS Growth Over Years'
        )

        # Optional: update layout to a light theme style
        fig_DDoS_growth.update_layout(
            template='plotly_white',  # Light background theme
            title_font=dict(size=20, family='Arial', color='black'),
            xaxis_title='Year',
            yaxis_title='Incidents',
            legend=dict(x=0.7, y=1.1, bgcolor='rgba(255,255,255,0)',
bordercolor='rgba(0,0,0,0)'),
            hovermode='x unified'
        )


        # Sample stories
        fiji_stories = [
            {"title": "Suva Ransomware Attack", "desc": "City services disrupted for 3
days. An unknown attacker hacked the Suva City Council's networks, encrypted all data,
and demanded a ransom for its release, a classic ransomware attack."},
            {"title": "Pacific Area Cyber Espionage", "desc": "A Chinese state-sponsored
hacking organization conducted a cyber campaign targeting government, healthcare,
technological, and manufacturing entities in Taiwan, Thailand, the Philippines, and
Fiji.  The attack, carried out by an APT41 offshoot known as Earth Longzhi, sought to
gain persistent control over computer systems, most likely for cyber espionage
reasons.  The attackers used advanced malware techniques, such as a Behinder webshell
and bring-your-own-vulnerable-driver (BYOVD) strategies."},
            {"title": "Pacific Forum Breach", "desc": "Sensitive diplomatic emails
compromised. It is unknown when the attacker initially obtained access. The attack
intended to collect intelligence about the Secretariat and its operations, and it was
also blamed on a Chinese state-sponsored hacking organization."}
        ]

        return html.Div([
            html.H4("Threat Landscape in Fiji and Beyond", className='text-primary'),

            dbc.Row([
                dbc.Col(
```

```
                    dcc.Graph(id='common-attacks-pie', figure=fig_common_attacks),
                    width=9
                ),
                dbc.Col(
                    html.Div(id='selected-attack-output', style={'marginTop': '10px',
'fontWeight': 'bold'}),
                    width=3,
                    style={'paddingLeft': '30px', 'borderLeft': '1px solid #ddd'}
                )
            ]),

            dbc.Row([
                dbc.Col(
                    dcc.Graph(id='industry-attacks-pie', figure=fig_industry_attacks),
                    width=9
                ),
                dbc.Col(
                    html.Div(id='selected-industry-output', style={'marginTop': '10px',
'fontWeight': 'bold'}),
                    width=3,
                    style={'paddingLeft': '30px', 'borderLeft': '1px solid #ddd'}
                )
            ]),

            dcc.Graph(figure=fig_breaches_growth),
            dcc.Graph(figure=fig_ransom_growth),
            dcc.Graph(figure=fig_DDoS_growth),
            html.H5("Cyberattacks in Fiji", className='mt-4'),
            dbc.Row([
                dbc.Col([
                    dbc.Card([
                        dbc.CardHeader(story["title"]),
                        dbc.CardBody(html.P(story["desc"]))
                    ], className='mb-3 shadow')
                ]) for story in fiji_stories
            ])
        ])

    elif tab == 'tab-workforce':
        fiji_stem_growth = pd.DataFrame({
            'Year': [2018, 2019, 2020, 2021, 2022, 2023],
            'Students': [1500, 1800, 2000, 2400, 2800, 3200],
            'Percentage': [30, 32, 35, 38, 40, 43]  # Example % values
```

```
})

# Create a figure with secondary y-axis
fig_stem_growth = make_subplots(specs=[[{"secondary_y": True}]])

# Add bar graph (number of students)
fig_stem_growth.add_trace(
    go.Bar(
        x=fiji_stem_growth['Year'],
        y=fiji_stem_growth['Students'],
        name='Number of STEM Students',
        marker_color='rgba(58, 71, 80, 0.6)'
    ),
    secondary_y=False
)

# Add line graph (percentage)
fig_stem_growth.add_trace(
    go.Scatter(
        x=fiji_stem_growth['Year'],
        y=fiji_stem_growth['Percentage'],
        name='Percentage of STEM Students',
        mode='lines+markers',
        line=dict(color='royalblue', width=2)
    ),
    secondary_y=True
)

# Update layout
fig_stem_growth.update_layout(
    title='Growth of STEM Students in Fiji (2018-2023)',
    template='plotly_white',
    xaxis_title='Year',
    yaxis_title='Number of Students',
    legend=dict(x=0.01, y=0.99),
)

# Set secondary y-axis title (right side)
fig_stem_growth.update_yaxes(
    title_text="Percentage of STEM Students (%)",
    secondary_y=True,
    range=[0, 100]
)
```

```
        # 2. STEM students % by country
        stem_comparison = pd.DataFrame({
            'Country': ['Fiji', 'Australia', 'India', 'China', 'USA'],
            'STEM_Percent': [21, 32, 34, 46, 20]
        })

        fig_stem_percent = px.bar(
            stem_comparison,
            x='Country', y='STEM_Percent',
            title='STEM Students as % of Total Tertiary Enrollment',
            text='STEM_Percent',
            color='Country'
        )
        fig_stem_percent.update_traces(textposition='outside')
        fig_stem_percent.update_layout(template='plotly_white')
        initiatives = {
            'National Strategies': [
                {"title": "EC-Council Collaboration with Fiji National University",
"desc": " Grant the students the opportunity to work under the National Training and
Productivity Centre with cutting-edge cybersecurity training and certifications,
enhancing their training to prevent and mitigate cyber threats effectively."},
                {"title": "National Development Plan", "desc": "Fiji has already
launched their National Development plan. Which outlines the nation's vision for
economic growth via digital transformation. As part of the strategy, Fiji has committed
to invest in the needed infrastructure and more importantly in enhancing STEM programs
including cybersecurit"}
            ],
            'Scholarship Programs': [
                {"title": "Scholarships for STEM", "desc": "Scholarships for STEM
degrees to encourage students to pursue careers like cybersecurity given by The Tertiary
Scholarship and Loans Board, even some private companies like Samsung are collaborating
with the Ministry of education to promote STEM careers across the country."}
            ],
            'Industry Collaborations': [
                {"title": "Cybersecurity Trainning", "desc": "There are also signs of
organisations with strong commitment with cybersecurity and workforce development in the
area. For example, Outsource Fiji in January 2024 concluded a cybersecurity training
program for 30 professionals to provide them with the needed skills to secure the
clients data."}
            ]
        }
```

```
        return html.Div([
            html.H4("Cybersecurity Workforce Development in Fiji", className='text-
primary'),

            dcc.Graph(figure=fig_stem_growth),
            dcc.Graph(figure=fig_stem_percent),

            html.H5("Current Initiatives to Close the Cybersecurity Talent Gap",
className='mt-4'),
            dcc.RadioItems(
                id='initiative-category',
                options=[{'label': k, 'value': k} for k in initiatives.keys()],
                value='National Strategies',
                labelStyle={'display': 'inline-block', 'marginRight': '20px'}
            ),
            html.Div(id='initiative-cards')
        ])

    elif tab == 'tab-policy':
        return html.Div([
            html.H4("Policy Frameworks Comparison", className='text-primary mb-3'),

            dbc.Row([
                dbc.Col([
                    html.Label("Select Policy Category:"),
                    dcc.Dropdown(
                        id='policy-category-dropdown',
                        options=[{'label': cat, 'value': cat} for cat in
policy_categories],
                        value='AI'
                    )
                ], width=4),

                dbc.Col([
                    html.Label("Select Countries to Compare:"),
                    dcc.Dropdown(
                        id='policy-country-dropdown',
                        options=[{'label': c, 'value': c} for c in
policy_frameworks.keys() if c != 'Fiji'],
                        value=['EU'],
                        multi=True
                    )
                ], width=8),
```

```
            ], className='mb-4'),

            html.Div(id='policy-comparison-output')
        ])

    elif tab == 'tab-config':
        return html.Div([
            html.H4("Key Challenges for AI & Cybersecurity in Fiji", className='text-
primary mb-4'),

            dbc.Row([
                dbc.Col(
                    dbc.Card([
                        dbc.CardBody([
                            html.H5(challenge, className='card-title'),
                            html.P(data["details"], className='card-text'),
                            dbc.Button("View Recommendations", id={'type': 'challenge-
button', 'index': challenge}, color='info', size='sm')
                        ])
                    ], className='mb-4 shadow-sm'),
                width=6)  # Two cards per row
                for challenge, data in fiji_challenges.items()
            ]),

            html.Hr(),
            html.Div(id='challenge-details-output')
        ])
    elif tab == 'tab-costs':
        return html.Div([
            html.H4("Cybersecurity Solutions Costs", className='text-primary mb-4'),

            dbc.Row([
                dbc.Col(
                    dbc.Card([
                        dbc.CardHeader("SMEs GDP apportation in Fiji"),
                        dbc.CardBody([
                            html.P("18%",className="card-text", style={"fontWeight":
"bold", "fontSize": "3rem"}),
                        ])
                    ],className="d-flex flex-column justify-content-center align-items-
center", color="info", inverse=True ,style = {"height":
"180px","borderRadius":"120px"}),
                width={"size": 2, "offset": 4},),
```

```
                dbc.Col(
                    dbc.Card([
                        dbc.CardHeader(r"Workforce % in SMEs"),
                        dbc.CardBody([
                            html.P("60%",className="card-text", style={"fontWeight":
"bold", "fontSize": "3rem"}),
                        ])
                    ],className="d-flex flex-column justify-content-center align-items-
center", color="info", inverse=True ,style = {"height":
"180px","borderRadius":"120px"}),
                width={"size": 2, "offset": 0.1})
            ],className="mb-4"),

            dbc.Row([
                dbc.Col(create_cost_card("Antivirus Software", "$900 - $1,500", "Per
year for 30 users", "success"), width=4),
                dbc.Col(create_cost_card("IDPS (Commercial)", "$5,000", "Commercial
solution setup", "warning"), width=4),
                dbc.Col(create_cost_card("VPN (Software)", "$1,800 - $5,400", "Annual
for 30 users", "primary"), width=4),
            ]),

            dbc.Row([
                dbc.Col(create_cost_card("VPN (Hardware)", "$1,000 - $5,000", "One-time
setup", "info"), width=4),
                dbc.Col(create_cost_card("Backup & Recovery", "$1,000 - $5,000", "Annual
cloud/hybrid backup", "secondary"), width=4),
                dbc.Col(create_cost_card("Endpoint Detection & Response", "$7,200 -
$18,000", "Annual for 30 endpoints", "danger"), width=4),
            ]),

            dbc.Row([
                dbc.Col(create_cost_card("AI Threat Detection", "$100,000+", "Small-
scale annual setup", "dark"), width=6),
                dbc.Col(create_cost_card("Managed Security Services", "$1,000 -
$10,000", "Monthly, depending on package", "secondary"), width=6),
            ])
        ])


@app.callback(
    Output('sector-info', 'children'),
    Input('sector-dropdown', 'value')
```

```
)
def update_sector_info(sector):
    row = sector_data[sector_data['Sector'] == sector].iloc[0]
    return dbc.Card([
        dbc.CardHeader(f"AI in {sector}"),
        dbc.CardBody([
            html.P(f"Use Cases: {row['AI_Use_Case']}"),
            html.P(f"Productivity Gain: {row['Productivity_Gain_%']}%"),
            html.P(f"Challenges: {row['Challenges']}")
        ])
    ], className='mb-4 shadow')

@app.callback(
    Output('common-attacks-pie', 'figure'),
    Input('common-attacks-pie', 'clickData')
)
def update_pie_attack_pull(clickData):
    # Recreate the dataframe here or keep it global if you prefer
    common_attacks = pd.DataFrame({
        'Attack Type': ['Phishing', 'Data Breach', 'Delivery Scam', 'Extortion',
'Identity Theft','Others'],
        'Percentage': [53.2, 10.4, 9.2, 7, 5, 15.2]
    })

    fig = px.pie(
        common_attacks,
        names='Attack Type',
        values='Percentage',
        title='Most Common Cyberattacks Globally',
        hole=0.4,
        color_discrete_sequence=px.colors.sequential.RdBu
    )
    # Default all pull to zero
    pull_values = [0] * len(common_attacks)

    # If a slice is clicked, find its index and pull it out
    if clickData and 'points' in clickData:
        clicked_label = clickData['points'][0]['label']
        if clicked_label in common_attacks['Attack Type'].values:
            idx = common_attacks.index[common_attacks['Attack Type'] ==
clicked_label][0]
            pull_values[idx] = 0.1
```

```
    fig.update_traces(
        textinfo='label',
        hoverinfo='label+percent',
        hovertemplate='<b>%{label}</b><br>Share: %{percent}',
        pull=pull_values,
        marker=dict(line=dict(color='#000000', width=1.5)),
    )
    fig.update_layout(
        showlegend=True,
        legend_title_text='Cyberattack Type',
        legend=dict(orientation='h', y=-0.1),
        transition_duration=500
    )
    return fig

@app.callback(
    Output('selected-attack-output', 'children'),
    Input('common-attacks-pie', 'clickData')
)
def display_selected_attack_info(clickData):
    if not clickData:
        return "Click a slice to see more information."

    clicked_label = clickData['points'][0]['label']

    # Example detailed info for each attack type
    details = {
        'Phishing': "Phishing attacks trick users into giving sensitive information
(like passwords or credit card numbers) by posing as trustworthy entities through fake
emails, messages, or websites.",
        'Data Breach': "A data breach occurs when unauthorized individuals gain access
to confidential or sensitive information, often due to poor security measures or system
vulnerabilities.",
        'Delivery Scam': "A delivery scam involves either the buyer paying for goods or
services that are never delivered, or a seller shipping items but never receiving
payment.",
        'Extortion': "Cyber extortion involves threats to release, delete, or withhold
access to sensitive data unless a ransom is paid – often carried out using ransomware or
stolen data.",
        'Identity Theft': "Identity theft happens when cybercriminals steal personal
information to impersonate someone and commit fraud, such as opening bank accounts or
making purchases.",
```

```
        'Others': "Other cyber crimes which don't represent a significant portion of the
global cyber crime"
    }

    info = details.get(clicked_label, "No details available for this attack.")

    return html.Div([
        html.H5(f"Details on {clicked_label}"),
        html.P(info)
    ])

@app.callback(
    Output('industry-attacks-pie', 'figure'),
    Input('industry-attacks-pie', 'clickData')
)
def update_pie_industry_pull(clickData):
    # Recreate the dataframe here or keep it global if you prefer
    industry_attacks = pd.DataFrame({
        'Industry': ['Finance', 'Healthcare', 'Energy', 'Manufacturing',
'Retail','Public Administration','Education','Others'],
        'Percentages': [18.2, 6.3, 11.1, 25.7, 10.7, 4.3, 2.8, 20.9]
    })

    fig = px.pie(
        industry_attacks,
        names='Industry',
        values='Percentages',
        title='Share of Attacks by Industry',
        hole=0.4,
        color_discrete_sequence=px.colors.sequential.RdBu
    )
    # Default all pull to zero
    pull_values = [0] * len(industry_attacks)

    # If a slice is clicked, find its index and pull it out
    if clickData and 'points' in clickData:
        clicked_label = clickData['points'][0]['label']
        if clicked_label in industry_attacks['Industry'].values:
            idx = industry_attacks.index[industry_attacks['Industry'] ==
clicked_label][0]
            pull_values[idx] = 0.1

    fig.update_traces(
```

```
        textinfo='label',
        hoverinfo='label+percent',
        hovertemplate='<b>%{label}</b>}<br>Share: %{percent}',
        pull=pull_values,
        marker=dict(line=dict(color='#000000', width=1.5)),
    )
    fig.update_layout(
        showlegend=True,
        legend_title_text='Industry',
        legend=dict(orientation='h', y=-0.1),
        transition_duration=500
    )
    return fig

@app.callback(
    Output('selected-industry-output', 'children'),
    Input('industry-attacks-pie', 'clickData')
)
def display_selected_industry_info(clickData):
    if not clickData:
        return "Click a slice to see more information."

    clicked_label = clickData['points'][0]['label']

    # Example detailed info for each attack type
    details = {
        'Finance': (
            "Description: The finance sector is one of the most developed and vital
parts of Fiji's economy, comprising commercial banks, insurance companies, credit
institutions, and the Reserve Bank of Fiji. It plays a key role in economic growth and
digital transformation.",
            "Cyber Threats: This sector is highly targeted by phishing, ransomware, and
banking trojans aiming to steal customer data, access accounts, or disrupt operations.
Insider threats and fraud are also common risks."
        ),
        'Healthcare': (
            "Description: Fiji's healthcare sector includes a mix of public and private
providers. While it faces challenges in infrastructure and workforce, digital health
initiatives and investments are slowly improving services, especially in urban areas.",
            "Cyber Threats: Ransomware is a major threat, as it can cripple access to
critical patient records. Other risks include data breaches, phishing attacks on staff,
and compromised medical devices."
        ),
```

```
        'Energy': (
            "Description: Fiji's energy sector is moderately developed, with a strong
emphasis on renewable energy. Hydropower, solar, and biomass are increasingly used to
reduce reliance on imported fossil fuels.",
            "Cyber Threats: The sector is vulnerable to Distributed Denial of Service
(DDoS) attacks, SCADA system intrusions, and malware that can disrupt energy production
or grid stability."
        ),
        'Manufacturing': (
            "Description: Fiji's manufacturing sector contributes significantly to
exports and employment, particularly in food processing, textiles, and beverages.
However, it is still developing and faces infrastructure and technology challenges.",
            "Cyber Threats: Cyberattacks can include ransomware, supply chain attacks,
and industrial espionage targeting proprietary designs or disrupting production lines."
        ),
        'Retail': (
            "Description: The retail sector in Fiji is diverse and growing, driven by
tourism and domestic consumption. E-commerce is emerging but remains in the early stages
due to limited digital infrastructure and logistical constraints.",
            "Cyber Threats: Threats include point-of-sale malware, data breaches of
customer payment info, phishing scams, and fake e-commerce sites used for fraud."
        ),
        'Public Administration': (
            "Description: Public administration in Fiji includes central and local
government functions. It is undergoing modernization, with growing efforts toward e-
government services and digital public infrastructure.",
            "Cyber Threats: Governments face ransomware, website defacements, and
attacks aiming to access or leak sensitive citizen data. Nation-state actors or
hacktivists may also target public systems."
        ),
        'Education': (
            "Description: Fiji's education sector is government-funded and includes both
public and private institutions. While urban areas have better facilities, rural
education access and digital learning tools are still developing.",
            "Cyber Threats: Common attacks include data breaches, ransomware, phishing
targeting students and staff, and disruptions to online learning platforms."
        ),
        'Others': (
            "Description: Other sectors, including tourism, agriculture, and
transportation, are key contributors to Fiji's economy. Tourism is especially
significant, though vulnerable to global events and natural disasters.",
```

```
            "Cyber Threats: Tourism platforms face booking scams, fake websites, and
data theft. Agriculture and transport may experience IoT-related attacks or disruptions
in logistics through ransomware or system breaches."
        )
    }

    description, threats = details.get(clicked_label, ("No details available for this
sector.", ""))

    return html.Div([
        html.H5(f"Details on {clicked_label}"),
        html.P(description),
        html.P(threats)
    ])


@app.callback(
    Output('initiative-cards', 'children'),
    Input('initiative-category', 'value')
)
def update_initiatives(category):
    initiatives = {
        'National Strategies': [
            {"title": "EC-Council Collaboration with Fiji National University", "desc":
" Grant the students the opportunity to work under the National Training and
Productivity Centre with cutting-edge cybersecurity training and certifications,
enhancing their training to prevent and mitigate cyber threats effectively."},
            {"title": "National Development Plan", "desc": "Fiji has already launched
their National Development plan. Which outlines the nation's vision for economic growth
via digital transformation. As part of the strategy, Fiji has committed to invest in the
needed infrastructure and more importantly in enhancing STEM programs including
cybersecurit"}
        ],
        'Scholarship Programs': [
            {"title": "Scholarships for STEM", "desc": "Scholarships for STEM degrees to
encourage students to pursue careers like cybersecurity given by The Tertiary
Scholarship and Loans Board, even some private companies like Samsung are collaborating
with the Ministry of education to promote STEM careers across the country."}
        ],
        'Industry Collaborations': [
            {"title": "Cybersecurity Trainning", "desc": "There are also signs of
organisations with strong commitment with cybersecurity and workforce development in the
area. For example, Outsource Fiji in January 2024 concluded a cybersecurity training
```

```
program for 30 professionals to provide them with the needed skills to secure the
clients data."}
        ]
    }
    selected_inits = initiatives.get(category, [])
    return dbc.Row([
        dbc.Col([
            dbc.Card([
                dbc.CardHeader(init['title']),
                dbc.CardBody(html.P(init['desc']))
            ], className='mb-3 shadow-sm')
        ], width=6) for init in selected_inits
    ])

@app.callback(
    Output('policy-comparison-output', 'children'),
    Input('policy-category-dropdown', 'value'),
    Input('policy-country-dropdown', 'value')
)
def update_policy_comparison(category, selected_countries):
    if not selected_countries:
        return html.P("Please select at least one country to compare.", className='text-
danger')

    # Build comparison table data: Fiji + selected countries
    countries_to_show = ['Fiji'] + selected_countries
    table_header = ['Country', 'Policies in ' + category]

    rows = []
    for country in countries_to_show:
        policies = policy_frameworks.get(country, {}).get(category, ["No data
available"])
        # Join policies in bullet points
        policies_list = html.Ul([html.Li(policy) for policy in policies])
        rows.append({'Country': country, 'Policies in ' + category: policies_list})

    # Use Dash DataTable or simple html.Table for display:
    table = dbc.Table(
        # Create table header
        [html.Thead(html.Tr([html.Th(col) for col in table_header]))] +
        # Create table body with rows
        [html.Tbody([
            html.Tr([html.Td(row['Country']), html.Td(row['Policies in ' + category])])
```

```
            for row in rows
        ])],
        bordered=True,
        striped=True,
        hover=True,
        responsive=True
    )

    return table

@app.callback(
    Output('challenge-details-output', 'children'),
    Input({'type': 'challenge-button', 'index': ALL}, 'n_clicks'),
    State({'type': 'challenge-button', 'index': ALL}, 'id')
)
def display_challenge_details(n_clicks_list, ids):
    ctx = callback_context
    if not ctx.triggered:
        return html.P("Click on any challenge to view detailed recommendations.",
className='text-muted')

    triggered_id = ctx.triggered[0]['prop_id'].split('.')[0]
    triggered_index = eval(triggered_id)['index']

    challenge_data = fiji_challenges[triggered_index]

    return html.Div([
        html.H5(f"Recommendations for: {triggered_index}", className='text-info'),
        html.P(challenge_data["details"], className='mb-2 text-muted'),

        html.H6("Recommendations:"),
        html.Ul([html.Li(rec) for rec in challenge_data["recommendations"]])
    ], className='p-3 bg-light border rounded')

@app.callback(
    Output('ai-productivity-graph', 'figure'),
    Input('sector-dropdown', 'value')
)
def update_productivity_chart(selected_sector):
    fig = px.bar(
        sector_data,
        x='Sector',
        y='Productivity_Gain_%',
```

```
        color='Sector',
        title='Estimated Productivity Gains with AI by Sector',
        text='Productivity_Gain_%'
    )
    fig.update_traces(textposition='outside')
    fig.update_layout(transition_duration=500)
    return fig

@app.callback(
    Output('config-output', 'children'),
    Input('config-threat', 'value'),
    Input('config-sector', 'value')
)
def generate_config_output(threat, sector):
    return dbc.Card([
        dbc.CardHeader(f"{threat} Threat in {sector}"),
        dbc.CardBody([
            html.P("Estimated Risk: High" if threat == 'Ransomware' else "Moderate"),
            html.P("Suggested Actions: Update systems, train staff, use AI monitoring.")
        ])
    ], className='shadow')

# Run app
if __name__ == '__main__':
    app.run(debug=True)
```