NATIONAL CYBER SECURITY STRATEGY OF SRI LANKA 2025 – 2029

Ministry of Digital Economy

SRI LANKA CERT|CC

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT)

The World Bank provided advisory support in preparing the strategy. The support was funded by the Cybersecurity Multi-Donor Trust Fund, administered by the World Bank.

National Cyber Security Strategy of Sri Lanka 2025– 2029

The Cabinet of Ministers has granted the approval for the implementation and enforcement of this Policy effective from 22 July 2025 (25/1198/805/010)

Document Classification: Public

Published by
Research, Policies and Projects Division
Sri Lanka CERT
Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 7
Sri Lanka

Telephone : +94 11 269 1692, Fax: +94 11 269 1064
Email : info@cert.gov.lk
Websites : www.cert.gov.lk | www.onlinesafety.lk

ISBN 978-624-6352-01-1

NATIONAL CYBER SECURITY STRATEGY OF SRI LANKA 2025 – 2029

Ministry of Digital Economy

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
(Sri Lanka CERT)

TABLE OF CONTENTS

Acronyms

AI	-	Artificial Intelligence
AISO	-	Assistant Information Security Officers
APCERT	-	Asia Pacific Computer Security Incident Response Team
CNII	-	Critical National Information Infrastructure
CSIRT	-	Computer Security Incident Response Team
CSP	-	Certification Service Provider
CSA	-	Cyber Security Authority
Cyber4Dev	-	Cyber for Development
DoS/DDoS	-	Denial of Service/ Distributed Denial of Service
EduCSIRT	-	Education Sector Computer Security Incident Response Team
FinCSIRT	-	Financial Sector Computer Security Incident Response Team
FIRST	-	Forum of Incident Response and Security Teams
GCI	-	Global Cybersecurity Index
HOO	-	Head Of Organization
IoT	-	Internet of Things
ISC	-	Information Security Committee
ISO	-	Information Security Officers
ISP	-	Internet Service Providers
ISP CSIRT	-	ISP Computer Security Incident Response Team
JPCERT/CC	-	Japan Computer Emergency Response Team Coordination Center
KPIs	-	Key Performance Indicators
NCA	-	National Certification Authority
NCSI	-	National Cyber Security Index
NCSOC	-	National Cyber Security Operations Center
NCSS	-	National Cyber Security Strategy
NVQ	-	National Vocational Qualification
M&E	-	Monitoring and Evaluation
PII	-	Personally Identifiable Information
RMC	-	Risk Management Committee
Sri Lanka CERT	-	Sri Lanka Computer Emergency Readiness Team
UN	-	United Nations

EXECUTIVE SUMMARY

In an age defined by digital interconnectedness, the reliance on technology enters every facet of modern life, presenting both extraordinary opportunities and complex challenges. As society moves deeper into the 21st century, the digital space has become crucial, yet it is also fraught with vulnerabilities that continuously evolve, giving rise to a dynamic cyber threat landscape.

Malicious actors, ranging from individual hackers to sophisticated cyber crime groups, exploit these vulnerabilities to target individuals, organizations, and even critical sectors such as healthcare, energy, finance, and transportation. This heightened risk emphasizes the urgent need for robust cyber security measures to safeguard against potential disruptions and protect national interests.

Recognizing the importance of ensuring the nation's safety, security, and prosperity in cyber space, the government of Sri Lanka introduced the nation’s first Information and Cyber Security Strategy in 2018. This pioneering strategy set the stage for a resilient and trustworthy cyber security ecosystem, allowing Sri Lankan citizens to embrace digitalization securely.

As the initial five-year period of the first strategy draws to a close, Sri Lanka CERT under the facilitation and the support of the Ministry of Digital Economy embarks on the development of Sri Lanka’s second cyber security strategy for the years 2025 to 2029. Building upon the successes and lessons learned from the previous strategy, this new iteration is tailored to address the evolving cyber threat landscape and align with broader national objectives, including the Sri Lanka Digital Economy Strategy (2030) and DOIT5.0 Digital Policy for Sri Lanka. The National Cyber Security Strategy received the Cabinet of Minister's approval on 22 July 2025 to be implemented from 2025 - 2029.

Crafted with inputs from diverse stakeholders and consultation with experts, the new strategy is a demonstration of Sri Lanka's commitment to continuous improvement and innovation in cyber space. It encompasses four thrust areas, namely enhancing regulatory frameworks, improving knowledge, strengthening preparedness and response capacity, and increasing cooperation.

Specific initiatives of each thrust area includes establishing policies and regulatory framework, increasing the cyber security awareness and education, securing the national critical information infrastructure, strengthening the incident response and recovery capabilities, and leveraging the local international partnerships to cultivate a secure and resilient cyber space for the nation. Each thrust area is underpinned by specific objectives aimed at driving initiatives outlined in the strategy.

Embracing a forward-looking approach, the new strategy incorporates technological advancements to effectively mitigate emerging cyber threats while harnessing the benefits of digitization. Moreover, it underscores the interconnectedness of cyber security with broader national development priorities, ensuring seamless integration into the country's digital transformation efforts.

With the World Bank providing consultancy support for its development, the new strategy represents a collaborative endeavour to fortify Sri Lanka's cyber security posture and propel the nation towards a secure and prosperous digital future. By encouraging collaboration between government, private sectors, and civil society, the strategy aims to create a resilient cyber ecosystem that can withstand the challenges of an increasingly complex digital landscape.

INTRODUCTION

In an era where the world is increasingly interconnected, the digital realm has become an essential aspect of the daily lives of individuals. The conveniences of modern technology and the boundless opportunities it offers are accompanied by an intricate web of vulnerabilities, giving rise to an ever-evolving cyber threat landscape. As society ventures deeper into the 21st century, the reliance on digital platforms, data sharing, and online communication has created a complex ecosystem in which both opportunities and risks flourish.

Malicious actors, ranging from individual hackers to organized cyber crime groups, sometimes supported by nation-states, are constantly refining their techniques, exploiting new vulnerabilities, and targeting both individuals and organizations with unprecedented precision. The motivations behind these attacks span a broad spectrum, encompassing financial gain, operational interruption, espionage, political disruption and activism.

Industries critical to the smooth and efficient functioning of society, such as healthcare, energy, finance, and transportation, have become prime targets for cyber attacks due to their potential for widespread disruption if compromised. The arrival of the Internet of Things (IoT) and cloud computing has further expanded the attack surface, creating a vast network that can be exploited if not adequately secured.

According to a research finding [1], global cyber attacks increased by 38% in 2022, compared to 2021 and warned that the maturity of AI technology, such as ChatGPT, have the ability to accelerate the number of cyber attacks in 2023. The report also indicated that the Asia Pacific region had the second highest volume of attacks after the African region and that the top 3 most attacked sectors in 2022 were government, healthcare, education and research.

In this context, recognizing its national responsibility to keep the nation safe, secure and prosperous in cyber space, the government of Sri Lanka introduced the nation's first Information and Cyber Security Strategy in 2018, designed for implementation over the five-year period from 2019 to 2023. As the initial five-year period concludes, it is essential to develop the country's second cyber security strategy, spanning from 2025 to 2029.

Building upon the foundation laid during the implementation of the first strategy, and in support of the Digital Sri Lanka 2030 Strategy and DOIT5.0 Digital Policy for Sri Lanka, this new cyber security strategy aims to drive Sri Lanka forward in achieving its mission and vision to create a secure digital cyber space and represents a dynamic roadmap to support Sri Lanka's growth and success over the next five years. It reflects the country's commitment to continuous improvement and innovation within the ever-changing landscape of cyber space.

CYBER SECURITY LANDSCAPE OF SRI LANKA & PRESENT DEVELOPMENTS

In recent years, Sri Lanka has witnessed a significant rise in cyber security and social media related incidents, with Sri Lanka CERT receiving 21,743 social media and cyber security incidents in the year 2024. Social media-related cases (17,396) dominated, with hacked accounts (7,468) and fake accounts (4,011) being the most reported. Other concerns included online harassment, scams, and copyright violations.

Cyber security incidents totaled 4,347, with financial scams (2,241), phishing (79), ransomware (22), and data breaches (42) posing significant threats. Facebook accounted for 13,617 cases, highlighting social media as a key attack vector.

Category	Number of Incidents	Category	Number of Incidents
Cyber Security Incidents (Total)	4,347	Social Media Incidents (Total)	17,396
Financial Scams	2,241	Hacked Account	7,468
General Scams	926	Fake Account	4,011
Phishing	79	Hateful/Abusive Content	2,883
Ransomware	22	Adults Sexual Harassment/Content	1,411
Data Breach	42		
Website Compromise	11	Harmful & Dangerous Act	673
Database Compromise	4	Child Sexual Harassment	58
Malware Infection	6	Child Non-Sexual Harassment	60
Malicious Software	4	Suicide or Self-Harm	16
Technical Issues	638	False Information	767
Internal Inquiries	198	Copyright Violation/DMCA	49
System Failure	3		
Total Incidents (Social Media + Cyber Security)			**21,743**

Table 1 : Incidents Reported to Sri Lanka CERT

These statistics emphasize the need for stronger cyber security measures, improved digital literacy, and proactive strategies to combat online threats and fraudulent activities. While Sri Lanka CERT compiles statistical data, its comprehensiveness is limited due to the absence of a nationwide data collection methodology and a centralized data repository.

Further multiple organizations, such as the National Child Protection Authority and Sri Lanka Police, also receive incidents, leading to challenges like data duplication and underreporting. The incomplete data hinders an accurate understanding of the cyber security landscape. This new cyber security strategy seeks to address these limitations by implementing measures to improve reporting, enhance data collection, and establish centralized oversight.

Figure 1 on page 10 highlights the findings of a pilot survey conducted by Sri Lanka CERT in collaboration with the Department of Census and Statistics, in 2023, shedding light on citizens' cyber security awareness. The survey reveals concerning trends, including that 55% of citizens install software without considering security implications, 52% fail to keep their operating systems up to date, and 52% do not scan email attachments before downloading. These statistics underscore critical gaps in basic cyber security practices among the public.

CYBER SECURITY ISSUES AND CHALLENGES FOR SRI LANKA

In general, Sri Lanka faces several pressing challenges that undermine its ability to ensure a secure and resilient digital environment. Such challenges include,

1. **Low Public Awareness:** Limited awareness among citizens regarding basic cyber security practices increases exposure to cyber attacks, such as phishing, ransomware, and social engineering. This is depicted clearly in the results shown in Figure 1 and the statistics shown in Table 1.
2. **Shortage of Skilled Cyber Security Professionals:** The insufficient pool of competent cyber security experts poses a major obstacle in combating increasingly sophisticated cyber risks. The shortage of skilled cyber security professionals within the government has resulted in inadequate cyber security preparedness across government organizations.
3. **Unprepared Government Organizations:** Many government organizations are ill-equipped in terms of resources, technology, and expertise to effectively address and respond to cyber security threats. Outdated IT infrastructure further amplifies vulnerabilities, leaving systems exposed to cyber risks. Additionally, the lack of adoption of new technologies limits their ability to implement modern security measures, making them susceptible to evolving cyber threats.
4. **Inadequate Governance and Regulatory Framework:** The absence of a cohesive governance and regulatory structure limits the effective implementation of national-level cyber security initiatives. A dedicated Cyber Security Act is required to establish a strong legal foundation, along with specific legislation for critical infrastructure protection and emerging technologies. Additionally, addressing gaps in existing laws is essential to ensure comprehensive legal coverage against evolving cyber threats, enabling a more resilient and adaptive cyber security framework.

To address the emerging gaps in response to the evolving cyber threat landscape, Sri Lanka introduced its first Information and Cyber Security Strategy (2019–2023) in 2018. This strategy played a vital role in laying the foundation to create a resilient and trusted cyber security ecosystem that realized the benefits of digitization to Sri Lankan citizens. The strategy had a vision to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digitalization and facilitate growth.

CITIZENS' PERCEPTION OF SECURITY AND PRIVACY ASPECTS

(Survey respondents are the users of digital devices such as computers and smart devices.)

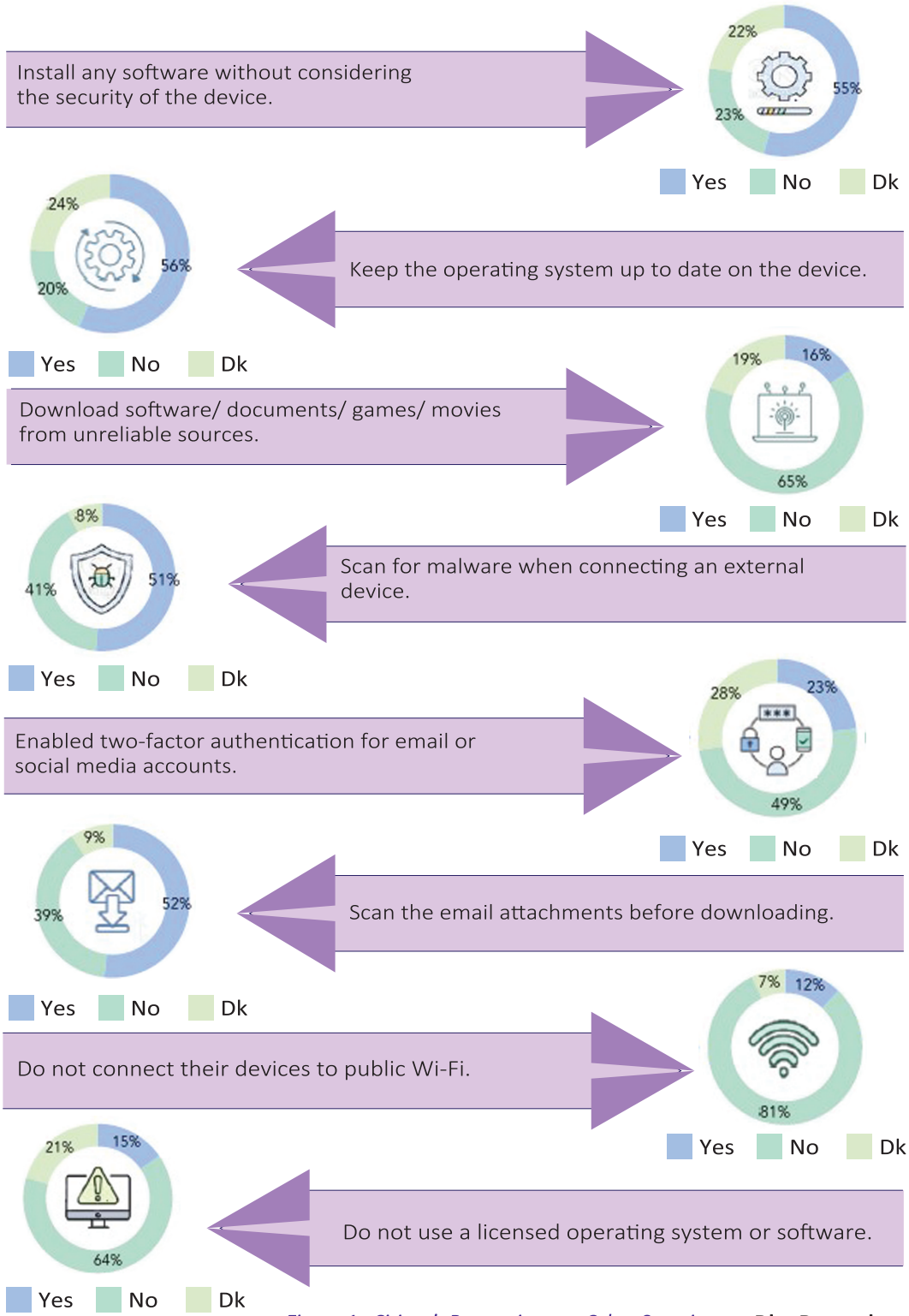


Figure 1 : Citizen's Perceptions on Cyber Security

Dk - Do not know

The nation's first Information and Cyber Security Strategy (2019 – 2023) played a vital role in laying the foundation to create a resilient and trusted cyber security ecosystem that realized the benefits of digitization to Sri Lankan citizens. The strategy had a vision to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digitalization and facilitate growth. Structured around six thrust areas, the strategy encompassed 41 initiatives, all illustrating the Government's dedication to fortify digital infrastructure and establish a robust and trustworthy cyber security ecosystem. Progress attained during the execution of the strategy is outlined below.

01 Establishment of the Governance Framework

Efforts toward cyber security governance in Sri Lanka entails creating an apex institution overseeing all cyber security matters. The establishment of this apex cyber security institution is reliant upon legislative approval, which has encountered delays. Nevertheless, Sri Lanka CERT has achieved notable advancements by establishing and overseeing a incident response call center (101 hotline) during this period. Additionally, endeavours are underway to establish the National Cyber Security Operations Center (NCSOC), while the National Certification Authority (NCA) is presently operational, with plans to enlist a Certification Service Provider (CSP).

Figure 2 : Thrust Areas of the Strategy (2019-2023)

02 Development of Legislation, Policies and Standards

As previously mentioned, the passing of a new Cyber Security Act to establish an apex cyber security institution did not materialize during the period. However, the CERT successfully drafted legislation defining the role of the Cyber Security Authority (CSA) as the apex institution for civilian cyber security matters. The Sri Lanka CERT continues to assist the Ministry of Digital Economy in advancing this act. Other notable developments include the enactment of the Personal Data Protection Act, No. 9 of 2022, which sets guidelines for personal data processing, strengthens data subject rights, and lays the groundwork for a Data Protection Authority. Additionally, the Information and Cyber Security Policy for Government Organizations (2022-2026) was formulated and received Cabinet of Ministers approval in August 2022, slated for implementation across all government bodies. Furthermore, baseline security standards, and web application security guidelines, have been established and publicly disclosed as part of these initiatives.

03 Resilient Digital Government Systems and Infrastructure

During the strategy period, successful efforts aimed at strengthening the resilience of critical information infrastructure and government organizations in Sri Lanka included completing a Critical Infrastructure Readiness Survey, which identified Critical National Information Infrastructure (CNII) Providers while assessing their cyber security preparedness. Several other initiatives that are currently ongoing include IT General Control (ITGC) Reviews and Risk Assessments for the identified CNII organizations as well as the appointment of Information Security Officers (ISO) and Assistant Information Security Officers (AISO) across all government entities, with comprehensive training programs in place to enhance their expertise in cyber security.

04 Development of Competent Workforce

The 2019-2023 Cyber Security Strategic Plan also included a diverse range of activities to cultivate a skilled workforce specializing in information and cyber security in Sri Lanka.

The initiatives include a Supply and Demand Survey conducted to identify the gap between the availability of cyber security professionals and industry demand, an Information and Cyber Security Readiness Survey to assess the preparedness of public sector employees, and ongoing collaborative work on a Cyber Security Skills Framework with international partners.

The 2019-2023 Cyber Security Strategic Plan also included a diverse range of activities to cultivate a skilled workforce specializing in information and cyber security in Sri Lanka. The initiatives include a Supply and Demand Survey conducted to identify the gap between the availability of cyber security professionals and industry demand, an Information and Cyber Security Readiness Survey to assess the preparedness of public sector employees, and ongoing collaborative work on a Cyber Security Skills Framework with international partners.

Additionally, National Vocational Qualification (NVQ) Standards at Levels 5 and 6 have been established in the Information and Cyber Security domain, and a project to train 10,000 government officers in cyber security was initiated and is currently underway.

05 Raising Awareness and Empowerment of Citizens

Efforts to raise awareness and empower citizens in Sri Lanka regarding cyber security during the strategic plan period include the development of the trilingual web portal https://www.onlinesafty.lk/, which serves as a platform to enhance cyber security awareness among the population.

Additionally, annual awareness programs and training sessions were conducted, with a focus on diverse demographics such as school children, university students, government officials, members of the tri-forces, law enforcement personnel, and private sector employees, contributing to the dissemination of education on information and cyber security. Furthermore, the Annual National Conferences on Cyber Security were conducted accompanied by multiple workshops providing further opportunities for knowledge dissemination and skill development in the field of cyber security.

06 Development of Public-Private and Local-International Partnerships

During the strategic plan period, the CERT continued to develop public-private and local-international partnerships in support of Sri Lanka's cyber security endeavors. These involved collaborations with private organizations and the establishment of international partnerships with entities like FIRST, APCERT, Cyber4Dev, the World Bank, and JPCERT/CC. These partnerships serve as key pillars in fostering cooperation and sharing knowledge and resources in the realm of cyber security. Sri Lanka CERT's contribution to the Asia Pacific CERT community was acknowledged by APCERT, resulting in Sri Lanka being awarded the APCERT Best Contributor Award for 2022.

PRESENT STATUS AND THE OUTCOME OF THE STRATEGY IMPLEMENTATION

Effectiveness of the strategy implementation was reflected in the latest Global Cybersecurity Index (GCI) report published by the International Telecommunication Union (ITU). Sri Lanka has made significant strides in strengthening its cyber security landscape, positioning itself as a leader in the region. This progress is reflected in its recognition as an "Advancing" country in the Global Cybersecurity Index, which highlights its commitment to enhancing cyber security practices across multiple pillars.

The Global Cybersecurity Index serves as a trusted benchmark for assessing countries' commitment to cyber security on a global scale. The fifth edition of the Global Cybersecurity Index (GCI) 2024 provides a comprehensive assessment of countries' commitment to cyber security across five key pillars namely (a) Legal, (b) Technical, (c) Organizational, (d) Capacity Development, and (e) Cooperation. The Legal pillar evaluates the strength of laws related to cyber crime and cyber security, while the Technical pillar focuses on the capabilities of national and sector-specific agencies. The Organizational pillar examines national strategies and organizations dedicated to cyber security governance, and the Capacity Development pillar looks at efforts to build cyber security knowledge through training, education, and awareness campaigns. Lastly, the Cooperation pillar measures partnerships between government, private sector, and international organizations.

In the 2024 report, 193 countries have been categorized into 5 tiers as Tier 1 (T1) – Role-modelling, Tier 2 (T2) – Advancing, Tier 3 (T3) – Establishing, Tier 4 (T4) – Evolving, and Tier 5 (T5) – Building based on their efforts to safeguard the cyber space. Sri Lanka has been classified as a Tier 2- Advancing country, achieving a score of 85-95 out of 100. A "T2 Advancing" country shows a strong commitment to cyber security through coordinated, government-led actions. This includes assessing, setting up, or implementing widely recognized cyber security measures across at least four pillars or many key indicators. This result demonstrates the effectiveness of the implementation of National Cyber Security Strategy by Sri Lanka CERT during the past several years. Sri Lanka was ranked 83rd in the 2020 GCI report and in 84th in the 2018 report prior to the implementation of the nation's first cyber security strategy.

The report further highlights that Sri Lanka's strength lies in its Legal Measures, Technical Measures, and Capacity Development, where it scored highest. However, the Organizational and Cooperation Measures are identified as areas for potential growth.

Notably, Sri Lanka's performance surpasses the average score for the Asia-Pacific region, indicating a robust commitment to advancing cyber security initiatives. The report encourages continued efforts in enhancing organizational frameworks and fostering international cooperation to further strengthen the country's cyber security landscape.

Sri Lanka CERT is actively working to enhance the country's cyber security standing and position itself to a T1: Role Modelling in the future.

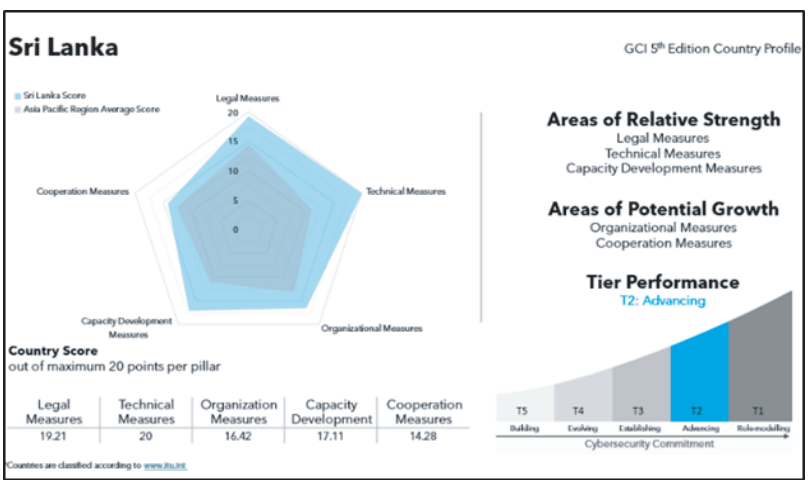


Figure 3 : Result of GCI (2024)

TOWARDS A NEW CYBER SECURITY STRATEGY

The nation's first Information and Cyber Security Strategy played a vital role in laying the foundation to create a resilient and trustworthy cyber security ecosystem, allowing Sri Lankan citizens to reap the benefits of digitization securely. However, the evolving nature of cyber threats necessitates a continuous and adaptive approach. The new strategy was developed with a comprehensive understanding of the achievements and challenges of the previous strategy, signifying a seamless continuation and evolution of the previous initiatives. The new strategy is designed considering the dynamic cyber threat landscape and recognizing the constantly changing tactics employed by cyber adversaries. By staying attuned to emerging threats, the new strategy aims to proactively strengthen defenses and mitigate potential risks.

Learning from past experiences and identifying vulnerabilities or shortcomings allows for targeted improvements. This ensures that the new strategy is not only responsive to current threats but also builds upon the lessons learned from the implementation of the initial cyber security framework.

Aligning with the national context, particularly the Digital Economy Blueprint, underscores the interconnectedness of cyber security with broader national objectives. The Digital Economy Blueprint presented in Figure 4, aims to accelerate economic growth through digital transformation, focusing on key areas such as innovation, e-commerce, fintech, digital governance, and smart infrastructure. It outlines core components, including digital infrastructure, Digital Public Infrastructure (DPI) encompassing digital payments, digital identity, and data exchange, Industry 4.0 digital services covering both government and industry applications, and multiple service delivery channels for diverse stakeholders.

A synchronized approach ensures that cyber security efforts are seamlessly integrated into Sri Lanka's Digital Economy Blueprint, supporting the country's vision for a secure, resilient, and thriving digital economy. By embedding robust cyber security measures into every aspect of the digital blueprint including digital infrastructure, Digital Public Infrastructure (DPI), government and industry applications, and service delivery channels Sri Lanka aims to foster trust, resilience, and sustainable growth through the effective implementation of its Cyber Security Strategy (2025-2029).

Signifying a smooth continuation from the previous strategy, the new framework reinforces the government's commitment to sustaining successful initiatives. This continuity ensures that the positive outcomes achieved in the past five years serve as a foundation for further progress, providing a sense of stability and reliability in the nation's cyber security efforts.

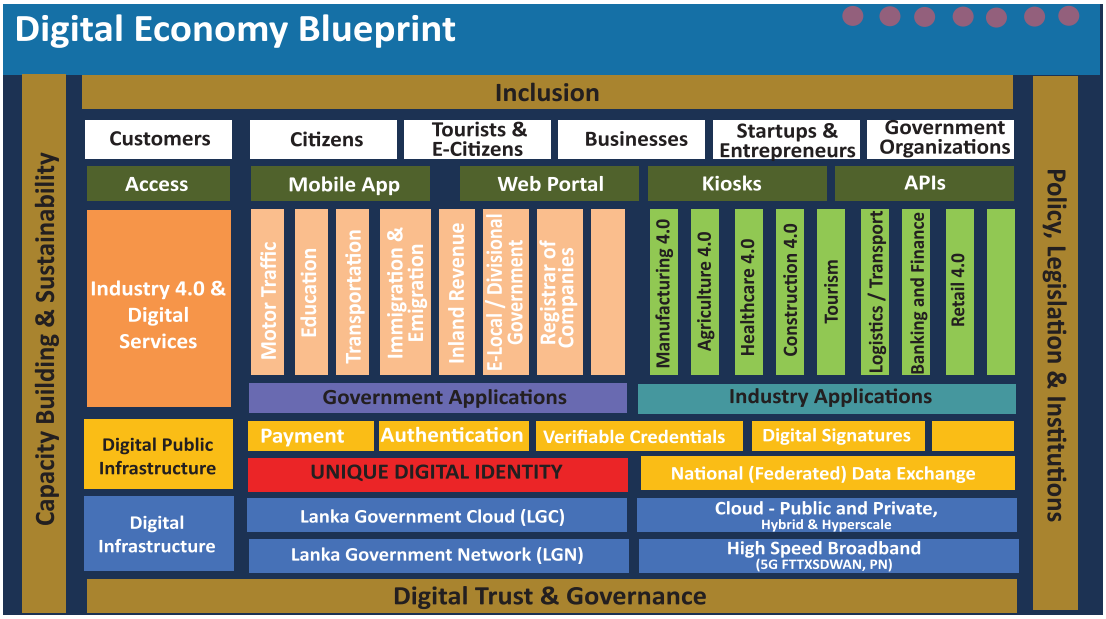


Figure 4 : Digital Economy Blueprint

Digital Trust and Sri Lanka's National Cyber Security Strategy (2025-2029)

Digital trust is built upon individuals' expectation that digital technologies and services and the organizations providing them will safeguard all stakeholders' interests while upholding societal values and expectations. To support this, the World Economic Forum has proposed a Digital Trust Framework for establishing principles and best practices that enhance security, reliability, privacy, and accountability in the digital ecosystem.

Through the various initiatives outlined in the National Cyber Security Strategy (2025-2029), Sri Lanka aims to establish digital trust by strengthening cyber security measures, thereby reinforcing the cyber security dimension under the Security and Reliability goal of the Digital Trust Framework.

Sri Lanka's National Cyber Security Strategy (2025–2029) aims to create an enabling environment for individuals, government, and private entities to safeguard their digital assets, including infrastructure, systems, applications, and data. The strategy establishes a strong legal and regulatory framework for data protection, cyber crime prevention, and critical infrastructure security. It also focuses on advancing knowledge and capacity through cyber security education, workforce development, and awareness initiatives. Preparedness and response capabilities are strengthened through enhanced incident management, threat intelligence sharing, and crisis response. Finally, the strategy promotes cooperation among local and international stakeholders, including public–private partnerships, to support policy alignment, collaborative defense, and capacity building.

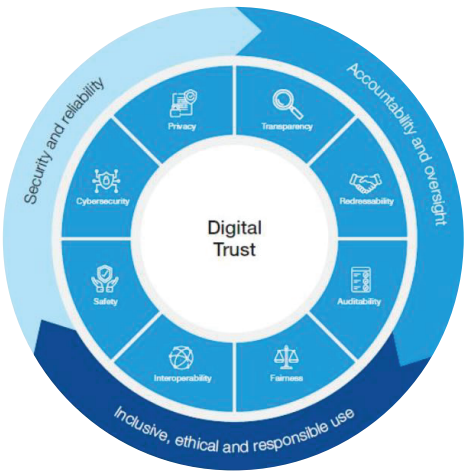


Figure 5 : Digital Trust Framework

CYBER SECURITY STRATEGY (2025-2029)

VISION

Ensure a secure, trusted, and inclusive digital ecosystem for Sri Lanka to fully realize the benefits of the evolving digital economy.

MISSION

To strengthen Sri Lanka's cyber security resilience by fostering a secure, trusted, and inclusive digital ecosystem through risk-based, standards-driven, and future-oriented initiatives. This strategy aims to safeguard national digital infrastructure, protect privacy and civil liberties, enhance cyber security capacity, and ensure alignment across all sectors, enabling the country to fully realize the benefits of the evolving digital economy.

DESIRED STATE

Sri Lanka is currently in the T2: Advancing state in the Global Cybersecurity Index and aims to achieve Tier 1: Role-Modeling status through the successful implementation of the second version of the National Cyber Security Strategy. This strategy is designed to enhance the country's overall cyber security readiness by strengthening legal frameworks, technical capabilities, institutional structures, and capacity development while fostering collaboration among key stakeholders to create a robust cyber security ecosystem.

By adopting global best practices, enhancing national capabilities, and ensuring cross-sector alignment, Sri Lanka seeks to build a secure, resilient, and inclusive digital environment that safeguards privacy, fosters trust, and maximizes the benefits of the digital economy.

CORE VALUES

The contours of the strategy and the initiatives to achieve the country's strategic goals emerge from guiding values that frame decisions about how to identify, manage, and mitigate cyber security threats in a way that balances many considerations including, inter alia, risks, civil rights and costs. Therefore, the strategy implementation will be guided by the following principles:

- Digital Trust. This strategy aims to create an enabling environment to build user confidence in the integrity, reliability, and security of digital technologies, fostering a secure and thriving digital ecosystem. Aligned with the World Economic Forum's Digital Trust Framework, which emphasizes transparency, interoperability, auditability, fairness, and privacy, this strategy facilitates the adoption of these principles to enhance user trust and support the growth of the digital economy.
- Prioritized. Recognizing the ambition of the strategy to achieve as much as possible within the resources available, the strategy will utilize a risk-based approach to support priorities.
- Standards-Based. Sri Lanka will strive to adhere to global best practices by adopting international cyber security standards to the maximum extent possible.
- Future-Oriented Capacity Development. The strategy strives to align capacity development initiatives with the future needs of the industry, utilizing a “train for tomorrow” approach that understands the evolving requirements of government and non-government organizations, both in the present and in the years to come.
- Alignment Across All Sectors. The strategy will align with initiatives across the government to avoid duplication and ensure integration with government priorities.

STRATEGIC ALIGNMENT

The new cyber security strategy is in alignment with the cabinet approved Digital Sri Lanka 2030 Strategy, DOIT5.0 Digital Policy for Sri Lanka and the Digital Economy Blueprint.

THRUST AREAS

Since cyber security plays a fundamental role in supporting the core operations of the Sri Lankan economy, the nation's cyber security strategy must align with national development priorities and build upon previous initiatives. After consultations with a broad range of stakeholders, and in alignment with the Digital Sri Lanka 2030 Strategy, the objectives of the National Cyber Security Strategy 2025 - 2029 fall into four categories, called Thrust Areas. They are, Enhance Regulatory Frameworks, Improve Knowledge, Strengthen Preparedness and Response Capacity and Increase Cooperation. Each Thrust Area contains several objectives which drive the initiatives contained in the Strategy Implementation Plan. The scope of this strategy confined to the civilian aspects of cyber security which encompase government and private sectors and civil societies.

Legal and Regulatory Frameworks

- Review and Implement Governance Frameworks
- Establish Policies for Current and Future Technology
- Align and Enhance Regulatory Frameworks

Increase Cooperation

- Enhance International Interaction and Fulfill International Obligations
- Leverage Local Partnerships

Strengthen Preparedness and Response Capacity

- Strengthen Incident Response and Recovery Capabilities
- Increase the Technical Capabilities of National Cyber Security Operations
- Secure Critical Information Infrastructure
- Support the Broader Stakeholder Community

Improve Knowledge

- Increase Awareness
- Enhance the Expertise Pipeline

THRUST AREA I - ENHANCE LEGAL AND REGULATORY FRAMEWORKS

Addressing the threats and disruptions that can result from malicious attacks to computer systems begins with establishing and maintaining robust legal frameworks that guide effective policies and governance structures.

The establishment of the Sri Lanka CERT, the creation of the information and cyber security policy for government organizations and the legislative acts related to information and cyber security have substantially improved the cyber security environment within Sri Lanka. The passing of the Personal Data Protection Act, which includes the establishment of the Data Protection Authority, along with initiatives to create an apex institution that oversees all national cyber security activities represent some of the initiatives that support the country's ability to monitor and respond to an increasing number and sophistication of cyber threats that risk destabilizing the country's economic and social fabric. However, since the cyber landscape is always rapidly evolving, Sri Lanka must also continually review and adjust its regulatory environment to address emerging threats.

Strategic Approach

Ensure that the cyber security legislative foundations provide the basis for the establishment of an effective governance framework and allow for the establishment and enforcement of regulations and policies that align with current and forthcoming technological advancements while adhering to core values.

To achieve the goal of a comprehensive regulatory environment, the strategy includes objectives in three key areas: regulation, policy and governance.

OBJECTIVE A
REVIEW AND IMPLEMENT GOVERNANCE FRAMEWORKS

As the country navigates an increasingly interconnected and digitally dependent world, the effectiveness of the national cyber security strategy hinges on the robustness of governance frameworks. Therefore, it becomes essential to implement governance frameworks that are agile, resilient, and aligned with the ever-changing landscape of cyber threats and technological advancements.

The initiatives listed reinforces Sri Lanka's commitment to cyber security governance that is well-prepared to address existing and emerging challenges.

A.1. Establishment of an Apex Cyber Security Institution

The current draft of the Cyber Security Act establishes the foundation for the creation of a Cyber Security Authority of Sri Lanka, which will serve as the institution entrusted with comprehensive oversight of all matters pertaining to the civilian aspects of cyber security.
The Cyber Security Act outlines the powers, duties, and functions vested in this authoritative body, positioning it to play a pivotal role in shaping and enforcing policies, regulations, and standards essential for safeguarding the nation's cyber landscape.

A.2. Implement Cyber Security Institutional Frameworks at the Organizational Level (organizational structures/committees, appointment of ISOs, security committees)

The cabinet-endorsed Information and Cyber Security Policy establishes institutional frameworks essential for implementing cyber security at the organizational level. Under the leadership of the Head of Organization (HOO), the policy mandates creating key roles such as the Chief Information Security officer(CISO)/Information Security Officer (ISO), Chief Innovation Officer, and Chief Internal Auditor as well as the establishment of an Information Security Committee (ISC) and a Risk Management Committee (RMC). These functions promote an information security culture that aligns with organizational goals.

A.3. Establishment of an Implementation Plan for the National Cyber Security Strategy

Develop a comprehensive implementation plan that outlines the specific actions, timelines, responsibilities, and resources required to execute the National Cyber Security Strategy. This plan will provide a clear roadmap for achieving the defined objectives and ensure coordinated efforts across government entities.

A.4. Monitoring and Evaluation (M&E) Framework - National Perspective

Establish a comprehensive Monitoring and Evaluation (M&E) framework with a national perspective to assess the progress and impact of the National Cyber Security Strategy and the Information and Cyber Security Policy for Government Organizations. This framework will include Key Performance Indicators (KPIs) and metrics to gauge the effectiveness of governance frameworks, policy implementation, and incident response. It will enable ongoing monitoring and reporting to ensure that the strategy remains adaptive and responsive to emerging threats and challenges.

A.5. Policy Implementation Assessment

Regularly assess the implementation of existing cyber security policies, especially the Information and Cyber Security Policy for Government, as well as other governance frameworks, to identify gaps, weaknesses, or areas in need of improvement. This includes evaluating the alignment of policies with emerging threats and technology trends. Further, these policies shall be promoted for various sectors (government and private) to effectively secure digital assets.

A.6. Enhance the Role of the National Audit Office

With the collaborative support of the institutions responsible for the subject of cyber security, the National Audit Office assumes the responsibility of conducting annual compliance audits to assess the adherence and progress in implementing the Information and Cyber Security Policy within government organizations.

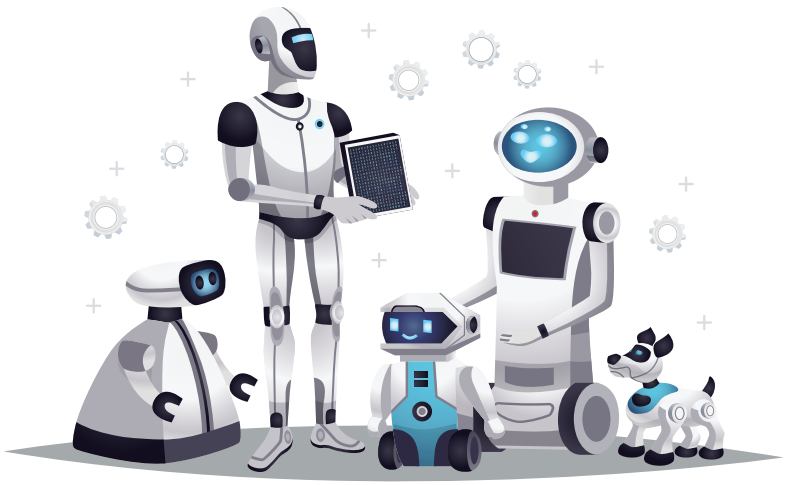
A.7. International Standards Compliance

Ensure that information and cyber security frameworks align with international standards and best practices to facilitate global cooperation and enhance the nation's cyber security posture on the international stage.

OBJECTIVE B
ESTABLISH POLICIES FOR CURRENT AND FUTURE TECHNOLOGY

In an era marked by rapid technological advancements, Sri Lanka's national cyber security strategy recognizes the imperative to establish robust policies that encompass both current and future technology landscapes. As the country navigates the dynamic digital environment, it is essential to address cyber security challenges and opportunities proactively. To this end, a series of applicable activities have been identified to guide our approach, ensuring that our policies remain agile, effective, and aligned with the ever-evolving technology landscape. These activities span various domains, from legal frameworks to data protection and emerging technology governance, collectively bolstering our national commitment to cyber security.

The following initiatives contribute to the establishment of policies that are not only relevant to current technology but also adaptable to the dynamic landscape of emerging technologies, reinforcing the foundation of the national cyber security strategy.



B.1. Address Security Implications of Emerging Technologies

Establish mechanisms, including processes, policies and standards, to identify and mitigate risks associated with relatively new technologies, such as Internet of Things (IoT) and blockchain, as well as emerging technologies, such as machine learning and Artificial Intelligence (AI). Apply the mechanisms developed to any existing technologies, such as cloud services, to ensure that the appropriate security arrangements are in place.

B.2. Cyber Security Technical Standards and IT Risk Management Frameworks for Government

Develop and implement technical controls and policies while adopting industry-accepted IT risk management frameworks and technical maturity standards to safeguard the government's digital infrastructure. These policies, standards and frameworks shall be regularly reviewed and updated to address the ever-evolving cyber threat landscape.

OBJECTIVE C
ALIGN AND ENHANCE REGULATORY FRAMEWORKS

In Sri Lanka's pursuit of a secure and resilient digital landscape, a foremost objective is to enhance the country's regulatory frameworks so that they align with digital goals and allow for emerging technologies. These frameworks serve as the cornerstone of Sri Lanka's cyber security environment, ensuring that Sri Lankan society is well-prepared to navigate the evolving complexities of the digital age.

A series of key initiatives that address gaps or weaknesses in existing legal arrangements in many areas, including Critical National Information Infrastructure Service Providers, complying with international conventions, accrediting cyber security service providers, enhancing supply chain security and safeguarding Personally Identifiable Information (PII). This comprehensive approach aims to create cohesive and robust legal and policy frameworks that safeguards Sri Lanka's digital ecosystem, upholds privacy, and fosters digital trust. The following initiatives collectively aim to harmonize and reinforce our regulatory frameworks, creating a comprehensive cyber security legal framework to protect Sri Lanka's digital landscape.

C.1. Strengthen Legal Provisions to Protect Critical National Information Infrastructure (CNII)

In compliance with the forthcoming Cyber Security Act, establish the parameters used to define and categorize information infrastructure services and sectors crucial for Sri Lanka. Additionally, establish mechanisms for ongoing adherence verification by CNII Providers. This includes implementing a system for CNII providers to regularly submit evidence of compliance with established cyber security policies and standards.

C.2. Strengthen Cyber Crime Legal Frameworks

Conduct a comprehensive analysis of the existing cyber crime legal frameworks to determine any gaps and introduce amendments to the Computer Crimes Act and other relevant legislation to strengthen the legal framework for addressing cyber security related offenses. Furthermore, ensure compliance with the Budapest Convention by assessing the need for adjustments to Sri Lanka's legislative and legal frameworks to bring it into alignment with the Budapest Convention, facilitating international cooperation in combating cyber crime.

C.3. Legal Review and Reform

Establish mechanisms to review and update existing laws to address current and emerging technology trends, ensuring that regulatory frameworks remain relevant and effective.

C.4. Accredit Cyber Security Service Providers

Develop criteria to standardize and accredit cyber security service providers, enhancing the quality and reliability of these services and ensuring that these services meet national needs.

C.5. Enhance Supply Chain Security

Focus Government efforts on strengthening supply chain security to safeguard government institutions and CNII.

C.6. Oversee National Certificate Authority (NCA)

Electronic exchange of information forms the basis of electronic commerce, and the NCA provides a crucial service as part of the e-commerce ecosystem that ensures legally binding data exchange while upholding the confidentiality and integrity of information.

THRUST AREA II - IMPROVE KNOWLEDGE

As Sri Lanka further develops its digital economy, the cyber risks and threats will multiply in line with global trends. Mitigating the risks, addressing threats and responding to incidents requires members of all communities to have the skills and knowledge to navigate the digital realm safely and securely. This begins with an ongoing, comprehensive awareness-raising campaign that reaches a broad range of communities.

In addition, well-trained cyber security professionals form the basis of an ability to monitor and respond to threats and incidents. These professionals emerge from a broad-based approach to skills development, which begins with integrating cyber security concepts into secondary education, followed by accredited and comprehensive university programmes dedicated to cyber security at both the graduate and undergraduate levels. Furthermore, professional cyber security certifications, from specialist service institutions, provide many of the skills that public and private sector institutions need to maintain their cyber security operations.

Strategic Approach

Empower all communities to recognize the risks stemming from the digital realm by enhancing every citizen's capacity to safeguard their identity, privacy, and economic assets in cyber space while deepening Sri Lanka's professional cyber security skills capability through advanced education and professional training opportunities.

OBJECTIVE D
INCREASE AWARENESS

Enhancing awareness is critical to fostering a secure society. The Sri Lanka CERT has, for many years, organized cyber security awareness training events reaching many thousands of citizens. Nevertheless, these training sessions have not reached all communities. Building on existing initiatives and collaborating with civil society, regional governments and other stakeholders allows for the creation of a comprehensive approach to skills and awareness that meets the needs of a diverse society.

The overarching strategy revolves around empowering all communities to recognize the risks stemming from participation in today's digital society, with the aim to enhance everyone's capacity to safeguard their identity, privacy, and economic assets in cyber space while equipping them to navigate potential pitfalls and to establish cyber security as a life skill.

The following initiatives increase awareness and foster a more cyber-resilient society that can confidently navigate the digital landscape while safeguarding digital identities and assets.

D.1. Assessment of Existing Awareness Capacity
Throughout the strategy period, comprehensive evaluations of the existing awareness landscape allows for adjustment of awareness training programmes and identifies strengths and weaknesses.

D.2. Online Safety and Social Media Security
Partner with civil society to create a cohesive approach to educating individuals on safe practices in the online environment, ensuring security on social media platforms, raise awareness regarding issues such as cyberbullying and create effective response and reporting mechanisms.

D.3. Protect Children in Cyberspace
Develop a national action plan with the support of key stakeholders to protect children from the challenges they face online, including cyber harassment, exposure to inappropriate content, online grooming, etc.

D.4. Centralized Information Hub
Establish a centralized platform to consolidate information related to cyber security awareness raising through printed, electronic and digital media.

D.5. Business Executive Awareness-Raising
Implement awareness-raising initiatives for private sector including Small and Medium Enterprises on Cyber Security.

D.6. Most-vulnerable Community Cyber Security Awareness-Raising
Create inclusive awareness-raising programmes that ensure gender balance and address the needs of unique communities, such as rural, providing them with the knowledge and tools to navigate cyber space securely.

D.7. Educational Curriculum Enhancement
Expedite the development and integration of cyber security topics, including awareness, into primary and secondary education curricula and address the challenges presented by technology unfamiliarity among educators by strengthening training for educators.

OBJECTIVE E
ENHANCE THE EXPERTISE PIPELINE

The ever-evolving landscape of technology and industry demands a continuous and dedicated effort to enhance the country's cyber security expertise pipeline and increase the cyber security workforce. This involves not only addressing immediate needs but also preparing for the future, considering the evolving requirements of both the public and private sectors. The affordability and accessibility of advanced cyber security education are critical elements, as is the need for a workforce that is not only skilled but adaptable.

The strategy envisions a comprehensive approach to create a skilled, adaptable, and motivated workforce that meets the evolving needs of government, academia, and industry. It is a forward-looking approach designed to ensure the country's workforce remains competitive and effective in the digital age.

The following initiatives strive to empower the workforce and create an expertise pipeline that meets the dynamic demands of today and the future.

E.1. Establish a National Cyber Security Skills Framework

Identifying and documenting the skills necessary for each cyber security role clarifies responsibilities and performance metrics, leading to achieving effective staffing goals.

E.2. Government Workforce Competence Enhancements

Enhance the skills and capabilities of government personnel, ensuring they are well-equipped to address the challenges of the digital age. Specific capacity building initiatives for (Chief)/Information Security Officers, Associate Information Security Officers, Officers in Charge of Subject of IT, Internal (Chief) Auditors, and end users. Cyber Security Skills Framework for Government is available on www.cert.gov.lk.

E.3. Affordable Cyber Security Education

Make cyber security education accessible and affordable, enabling individuals to gain the knowledge and skills needed to excel in their roles and contribute effectively to their fields, thus fostering a productive workforce. Integrate new initiatives into existing programmes and align with the National Vocational Qualifications.

E.4. Improve or Maintain Talent Pool

Investigate strategies that enhance the government cyber security workforce, such as a mechanism to incentivize cyber security professionals to join the public sector (particularly for CNIIs) and to retain a skilled workforce in government, ensuring that these valuable individuals remain committed, motivated, and engaged in their roles. Further, women are globally underrepresented in the cyber security profession. Therefore, special attention will be given to creating an interest in cyber security among female school students.

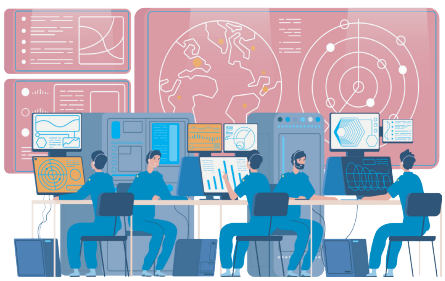
THRUST AREA III - STRENGTHEN PREPAREDNESS AND RESPONSE CAPACITY

Along with growing and maintaining the cyber security talent pool, the country will also strengthen its monitoring and response capabilities and enhance institutional technical capabilities to ensure the cyber security of critical national information infrastructure and other digital assets.

The Sri Lanka CERT, working together with other public and private sector monitoring functions, will continue to coordinate cyber security activities across the country as a joint effort to provide a secure cyber environment. At the same time, the CSA will include a focus on strengthening CNII operators and other government institutions.

Strategic Approach

Enhance the country's ability to monitor, prevent and respond to cyber incidents as well as strengthen recovery abilities.



OBJECTIVE F
STRENGTHEN INCIDENT RESPONSE AND RECOVERY CAPABILITIES

Effective cyber attack response and recovery capabilities depend on a range of skills, but planning and practice are fundamental actions that can make the difference between long down times and quickly resuming operations. The following initiatives are designed to sharpen the country's ability to respond effectively and efficiently to cyber incidents.

F.1. Crisis Management Plan for Cyber Incidents

Create a crisis management plan tailored to address cyber incidents that have the potential to disrupt critical infrastructure or national security. This plan should outline the procedures for incident response, coordination among relevant stakeholders, communication strategies, and recovery efforts to minimize the impact of such incidents.

F.2. Implement the National Cyber Security Operations Centre

Finalize the deployment of a National Cyber Security Operations Centre (NCSOC) to manage and initially oversee government systems. A further phase increases the NCSOC capacity to include CNII operators and other institutions to participate.

F.3. Incident Reporting and Response Improvement

Establish mechanisms to support the reporting of cyber security incidents, with a specific emphasis on engagement with public and private sector institutions, including civil society, and strengthen the ability of institutions to effectively identify, classify and respond to cyber incidents.

F.4. Promote Cyber Insurance

Advocate for the adoption of cyber insurance among organizations to enhance their protection against cyber incidents. Provide education on available coverage options, and foster partnerships between organizations and insurance providers to ensure that policies are tailored to align with national cyber security standards and strategic objectives.

OBJECTIVE G
INCREASE THE TECHNICAL CAPABILITIES OF NATIONAL CYBER SECURITY OPERATIONS

The proposed Cyber Security Authority (CSA) consolidates pivotal functions required for cyber security incident management and the oversight of the country's cyber security landscape. Key components, such as the CERT, and newer elements, such as the NCSOC, play vital coordination, response and support roles. These strategic activities are essential components of the country's national strategy, designed to fortify technical cyber security capabilities and ensure the nation is well-prepared to address cyber security challenges. The following initiatives enhance the technical cyber security capabilities of these functions.

G.1. Elevating Technical Proficiency of the Government's Central Cyber Security Authority
Establish mechanisms to ensure that specialists within the central cyber security authority have the necessary skills and procedures to effectively monitor and respond to cyber incidents and the competence to support national institutions. This can include implementing internationally recognized cyber security standards such as those from ISO.

G.2. Enhancing National CERT Competence
Increase the operational maturity of the national CERT functions, including through pursuing SIM3 certification and establishing staff training programmes.

G.3. Malware Analysis and Threat Hunting Lab
Create a centralized threat-hunting platform designed to continuously monitor, analyze, and adapt to the rapidly changing cyber threat landscape. This repository will serve as a comprehensive resource for collecting, correlating, and assessing threat intelligence, enabling proactive identification and mitigation of emerging threats.

OBJECTIVE H
SECURE CRITICAL INFORMATION INFRASTRUCTURE

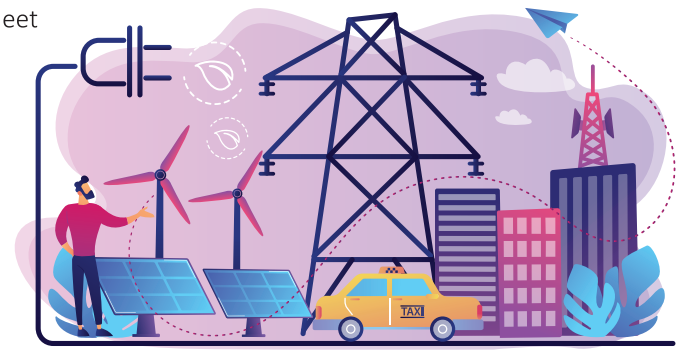
Like all countries, everyday life in Sri Lanka depends on access to a broad range of services, such as communication, finance, water, electricity, transportation, etc. These services increasingly depend on modern information technology, which may be vulnerable to malicious disruption. Therefore, securing these services becomes of paramount importance and can encompass a focus on access controls, surveillance systems, encryption protocols, and developing redundant infrastructure as needed. These can apply to systems operating within operators that are deemed essential, such as cable landing stations for telecommunications operators and medical information systems for health providers.

The measures outlined below are designed to enhance the security and resilience of critical infrastructure, safeguarding these essential systems against potential threats and vulnerabilities.

H.1. Enhancing CNII Protection
Utilize risk assessments to clearly identify vital systems, particularly those within government entities, and develop plans for strengthening the protection of critical systems.

H.2. Minimum Cyber Security Requirements
Implement already-established minimum cyber security requirements for CNII and create mechanisms to ensure that essential systems meet security standards.

H.3. Crisis Preparedness for Critical Infrastructure Providers
Conduct crisis exercises (including incident simulations, table top exercises and cyber drills) for critical infrastructure service providers to ensure readiness in the face of potential cyber security incidents.



OBJECTIVE I
SUPPORT THE BROADER STAKEHOLDER COMMUNITY

Even though a substantial attention is focused on securing critical information infrastructure, many other components of Sri Lankan society remain at risk. Therefore, the strategy will also strive to enhance the cyber security abilities of a broad range of institutions. The following initiatives will seek to support institutions throughout the country:

I.1. Enhance Core Cyber Security Services
Sri Lanka CERT continues to enhance core cyber security functions, such as pentesting, risk and vulnerability assessments, etc.

I.2. Enhance Threat and Risk Assessment Capabilities
The central cyber security authority, working with partners, will strengthen its ability to identify and evaluate the evolving cyber threat environment and establish a risk management approach to assess the potential impact and consequences of cyber incidents on critical infrastructures and essential services.

I.3. Enhance Digital Forensics Capabilities
Make strategic investments instate-of-the-art forensic equipment,advanced training for forensic experts and the adoption of updated tools and methodologies for digital evidence analysis to support the central cyber security authority's function as a panel member for investigating financial and other cyber crimes, under the authority of the Payment Device Fraud Act.

THRUST AREA IV - INCREASE COOPERATION

In a global economic environment, countries depend on many relationships that extend beyond their borders. These international dependencies become multiplied for island nations like Sri Lanka, which maintains trading relationships for a wide array of good and services and for a broad range of industries. And while digitization of economies brings substantial productivity gains, it also compounds the risks. Consequently, since cyber threats for all nations extend beyond national borders, no country can adequately address the inherent cyber risks on its own. International mechanisms exist that allow for cross-border collaboration to mitigate cyber risks and respond to cyber threats, and in its strategy, Sri Lanka will leverage regional and global cyber resources not only to respond to challenges but also to contribute to international forums that address issues of cyber crime and cyber security.

Furthermore, the cyber security strategy acknowledges the importance and value of local cyber expertise. Through partnerships with private sector institutions, the strategy will seek to establish coordinating structures and information-sharing processes and protocols along with best practices for improving security.

Strategic Approach

Foster increased cooperation on a global scale and leverage local partnerships to build a robust cyber security ecosystem, including public private partnerships for coordination and building trust.

OBJECTIVE J
ENHANCE INTERNATIONAL INTERACTION AND FULFILL INTERNATIONAL OBLIGATIONS

Enhancing international interaction and fulfilling obligations to the international community requires a strategic approach that encompasses various aspects of diplomacy, cooperation, and engagement. Here are some key activities to achieve this goal:

J.1. Participation in Regional and Global Forums

Actively engage in regional (such as APCERT) and global (such as FIRST) cyber security forums, conferences, and organizations to share knowledge, insights, and best practices while fostering international cooperation. Host international cyber security events, conferences, and workshops to bring together experts and stakeholders from around the world, fostering a platform for knowledge exchange and collaboration on cyber security challenges.

J.2. Cooperation Agreements with Regional CERTS

Establish and strengthen formal cooperation agreements with regional Computer Emergency Response Teams (CERTs) to facilitate information sharing, collaboration during major cyber incidents, and the exchange of cyber security experts and resources to bolster regional cyber resilience. Provide technical assistance and support to other nations in their cyber security endeavors, including capacity building programs, training initiatives, and information sharing, thereby contributing to international cyber security capacity and collaboration.

J.3. Sharing Threat Intelligence

Promote the sharing of threat intelligence with international partners, aiding in the early detection and mitigation of cyber threats on a global scale, while fostering a network of trust and cooperation.

J.4. Mutual Legal Assistance Agreements

Negotiate and implement mutual legal assistance agreements with foreign nations to enhance cooperation in investigating and prosecuting cyber crimes, ensuring a seamless exchange of information and legal support. This includes further integration and adoption of the Budapest Convention principles and exploring the value of other emerging international and governmental treaties.

J.5. Contribute to and Implement Internationally Accepted Cyber Security Practices

Develop an action plan with initiatives that ensure Sri Lanka conforms to The UN norms of responsible state behaviour in cyber space as called for by multilateral bodies. Through the implementation of the action plan, Sri Lanka aims to promote stability, security, and cooperation in cyber space while mitigating the risks of cyber conflict and ensuring the protection of individuals' rights and freedoms online.

J.6. Collaboration with the Foreign Ministry

Work closely with the Foreign Ministry in policy formulation, involving key stakeholders in decision making to ensure that national cyber security policies are strategically aligned with broader foreign policy objectives.

OBJECTIVE K
LEVERAGE LOCAL PARTNERSHIPS

Recognizing the significance of collaborative efforts in bolstering the country's cyber defenses, this objective emphasizes engagement across various sectors. By harnessing the collective strengths of academia, local industries, government organizations, service providers, and other authorities, the strategy aims to cultivate a thriving cyber security ecosystem.

K.1. Collaborative Research and Development

Create policies that encourage partnerships with industry, academia, and research institutions to drive innovation and research in cyber security technologies, aligning with current and future tech trends.

K.2. Develop Local Industry Partnerships

Facilitate collaborations with local industries as well as cyber security and technology professional associations to increase awareness across sectors, develop and implement best practices, share threat intelligence, and identify system vulnerabilities through programs such as bug bounty initiatives. These partnerships also aim to build trust and support a resilient cyber security ecosystem, while strengthening the private sector's role in national cyber security.

K.3. Enhance Nationwide Threat Intelligence Sharing

Facilitate the sharing of threat intelligence between government organizations and private sector entities to enhance collective cyber security awareness, preparedness, and response capabilities.

K.4. Support Sectoral Cyber Security Response Capabilities

The ability of key business sectors to monitor and respond to incidents within their sectors forms an additional measure of national protection. Using existing sectoral CSIRTs (such as the financial industry's FinCSIRT) as a template, and in partnership with the relevant institutions within each sector, support the development of additional CSIRTs. Examples include an Educational Computer Security Incident Response Team (EduCSIRT), developed in collaboration between the national cyber security authority and academia, and, in partnership with Internet Service Providers (ISPs) an ISP Computer Security Incident Response Team (ISP CSIRT).

K.5. Initiate a Partnership with Data Protection Authority

Provide technical support and guidance to the Data Protection Authority to ensure compliance with data protection regulations and collaborate to establish a cohesive regulatory framework that strengthens data security and cyber security measures.

SUMMARY

The Cyber Security Strategy for Sri Lanka is a comprehensive plan designed to establish and maintain a secure, trusted, and inclusive digital ecosystem within the country. This strategy is guided by fundamental core values such as privacy, prioritization, adherence to international standards, future-oriented capacity development, and alignment across sectors. Central to this strategy, there are four key thrust areas designed to address specific challenges and priorities in the realm of cyber security. They are, enhance regulatory frameworks, improve knowledge, strengthen preparedness and response capacity and increase cooperation. Implementing these thrust areas safeguards the country's vital infrastructure, ensuring its continuous operation and resilience against cyber threats.

Further, it promotes economic stability by creating a secure and trusted environment for businesses and citizens and encouraging innovations. By building cyber resilience, enhancing incident response capabilities, and promoting collaboration among stakeholders, the national cyber security strategy aims to create a secure and trusted digital ecosystem which is helpful to economic prosperity and the nation's security. This strategy will be implemented from 2025 to 2029 with the involvement of key stakeholders, including citizens, the government, industry, and international counterparts. Through implementing this strategy it is expected to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digital technology and facilitate growth, prosperity, and a better future for all.

Reference

[1] *Gmcdouga (2023) Check point research reports a 38% increase in 2022 global cyberattacks, Check Point Blog. Available at: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (Accessed: 22 April 2024).*

[2] *International Telecommunication Union (2024) Global cybersecurity index 2024. Available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (Accessed: 10 September 2024).*

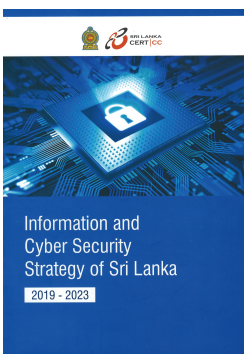
[3] *World Economic Forum, "Digital Trust Framework." [Online]. Available: https://initiatives.weforum.org/digital-trust/framework. [Accessed: 31January 2025].*

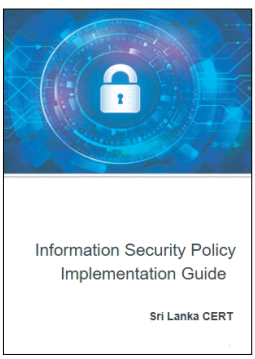
[4] *National People's Power, "Digital Policy for Sri Lanka," Aug. 2024. [Online]. Available: https://www.npp.lk/up/policies/en/digitalpolicy.pdf. [Accessed: 02 February 2025].*

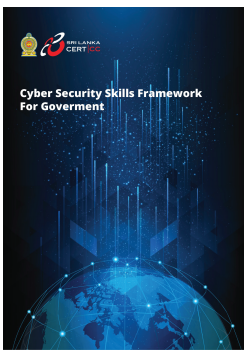
[5] *Ministry of Technology, Sri Lanka, "National Digital Economy Strategy 2030 - Sri Lanka". [Online]. Available: https://mot.gov.lk/assets/files/National%20Digital%20Economy%20Strategy%202030%20Sri%20Lanka-bc77184e0b6035d235cd0bb1ebf75707.pdf. [Accessed: 31 August 2024].*

Notes

Our Publications







Ministry of Digital Economy

SRI LANKA CERT | CC

Sri Lanka Computer Emergency Readiness Team
(Sri Lanka CERT)

ISBN 978-624-6352-01-1