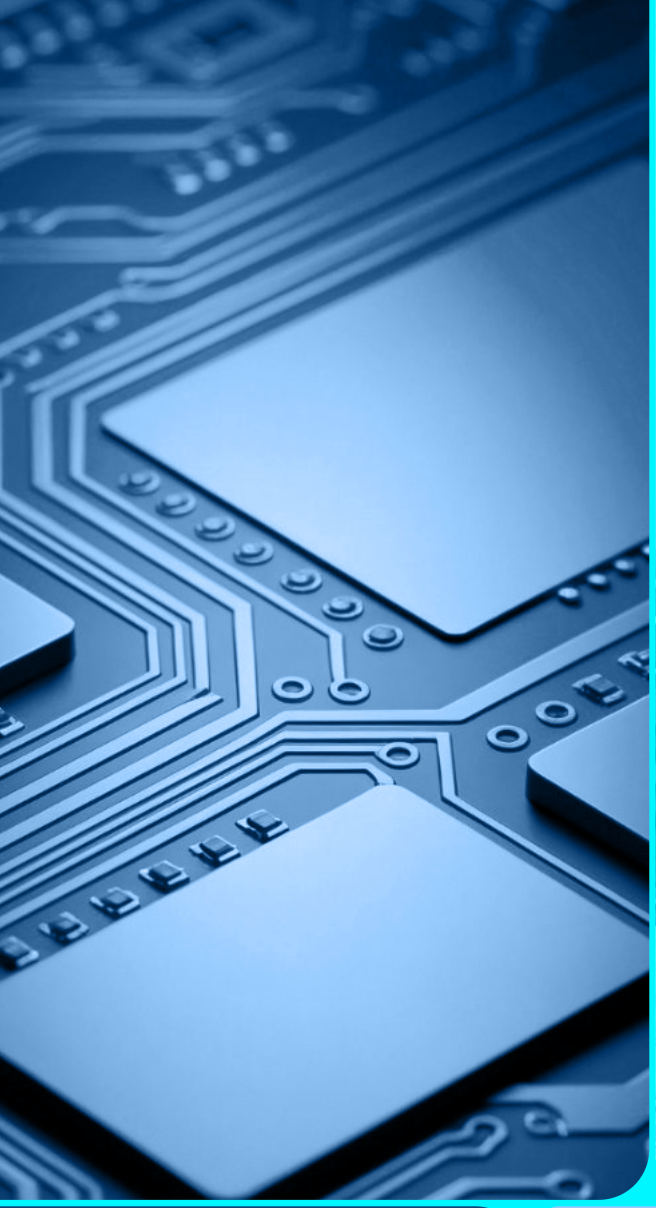






Sarawak Cybersecurity Strategy and Roadmap 2030

A secure and trusted foundation for Sarawak's digital economy

SMA
SARAWAK MULTIMEDIA AUTHORITY

This page is intentionally left blank.


SMA
SARAWAK MULTIMEDIA AUTHORITY

Sarawak Multimedia Authority
Level 5, Bangunan Yayasan Sarawak,
Jalan Masjid, 93000 Kuching,
Sarawak, Malaysia.

W: www.sma.gov.my
T: 082-268012
F: 082-268019

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy or any information storage and retrieval system, without permission in writing from the publisher.



SARAWAK CYBERSECURITY

STRATEGY AND ROADMAP 2030

Foreword by the Premier

The Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) marks an important step in establishing a coordinated approach to cyber security across Sarawak. It is the State's first comprehensive, Whole-of-Sarawak cyber security strategy, bringing together Government agencies, State-owned enterprises, critical infrastructure operators, businesses, academia and the wider community under a common direction.

The Strategy was developed to provide greater clarity on where Sarawak needs to strengthen its cyber security capabilities and how these capabilities can be developed progressively. It brings together priorities that span the protection of strategic information assets, the safety of citizens and businesses, the development of local talent, governance and operational capability, and collaboration with national, regional and international partners.

SCSR 2030 is deliberately designed as a roadmap rather than a collection of standalone projects.

Its initiatives are sequenced over five years so that foundational capabilities can be established first, followed by operationalisation, wider adoption and longer-term institutionalisation. This approach allows Sarawak to build capability progressively while adapting to changes in technology, cyber threats and the needs of the State.

A key principle of the Strategy is that cyber security cannot be managed effectively through fragmented efforts. A Whole-of-Sarawak approach enables common standards, stronger coordination, better sharing of information and more effective use of resources. It also provides a basis for organisations across Sarawak to understand their respective responsibilities and contribute to a stronger overall cyber security posture.



The Sarawak Multimedia Authority will play a central role in providing strategic leadership and coordinating the implementation of the Strategy. This includes working with relevant State agencies and stakeholders to establish the governance, capabilities and partnerships required to deliver the roadmap. The Strategy will also evolve as circumstances change, with progress monitored and priorities reviewed to ensure that it remains relevant and effective.

With SCSR 2030, Sarawak takes an important step towards building a safer and more trusted digital environment; one that protects our people, strengthens our institutions, supports our economy and enables Sarawak to confidently embrace the opportunities of the digital future.

THE RIGHT HONOURABLE DATUK PATINGGI TAN SRI (DR)
ABANG HAJI ABDUL RAHMAN ZOHARI BIN TUN DATUK ABANG HAJI OPENG

PREMIER OF SARAWAK



Preamble by The Honourable Sarawak State Secretary

The digital transformation of Sarawak is no longer a future aspiration. It is an ongoing reality that is reshaping the way Government serves its people. As we accelerate the implementation of the Post COVID-19 Development Strategy (PCDS) 2030, the digitalisation of Government services has become an important enabler in our efforts to build a modern, efficient, responsive and people-centric public service. Increasingly, Government services, operations and decision-making processes are supported by digital platforms, interconnected systems and data.

I wish to express my sincere appreciation to the Right Honourable Premier of Sarawak for his visionary leadership and unwavering commitment in driving Sarawak's digital transformation. His leadership has provided the direction and impetus for Sarawak to embrace technology, innovation and digitalisation as key enablers of the State's continued progress and development.

I would also like to record my appreciation to the Sarawak Multimedia Authority for its dedication and commitment in developing the Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030). This timely and significant initiative provides an important framework to guide our collective efforts in strengthening cyber security as Sarawak advances its digital transformation agenda.

As we expand the delivery of Government services through digital platforms and become increasingly dependent on technology and data, cyber security must become an utmost priority. The same connectivity that enables greater efficiency, accessibility and convenience also exposes our systems and information to increasingly sophisticated and evolving cyber threats.

A disruption or compromise to a digital system can affect not only the organisation concerned, but also the wider Government ecosystem and, ultimately, the people who depend on our services. Protecting our digital infrastructure, systems and data is therefore essential to ensuring the continuity, reliability and integrity of Government services, as well as maintaining public confidence in our digital transformation journey.

It is in this context that the SCSR 2030 assumes particular importance.The Strategy and Roadmap provides a clear and unified direction for Ministries, Departments, State Statutory Bodies, Local Authorities, State Government-Linked Companies and other relevant stakeholders. It will guide our collective efforts to strengthen preparedness, enhance resilience, develop capabilities and respond effectively to an increasingly complex and evolving cyber threat landscape.



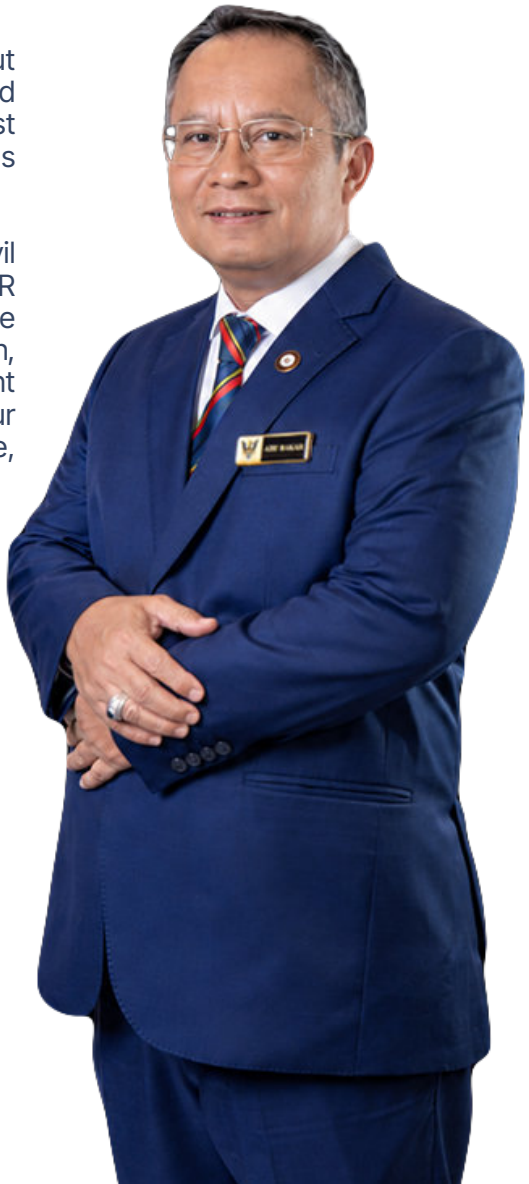
Cyber security cannot be the responsibility of a single organisation or confined solely to ICT and cyber security professionals. Our digital environment is highly interconnected. Just as the various parts of the human body must work together for the whole to function effectively, every organisation and every individual within our digital ecosystem have a role to play in safeguarding it.

Every officer has a responsibility to remain vigilant. How we manage information, protect access, respond to suspicious activities and observe established security practices collectively determine the strength of our cyber defence. Likewise, our vendors, contractors and digital service providers must recognise their responsibilities in protecting the systems and information entrusted to them.

We must therefore move beyond fragmented and siloed approaches and adopt a Whole-of-Sarawak approach to cyber security, founded on stronger collaboration, enhanced capabilities and a shared sense of responsibility. Cyber security must also be embedded from the outset in our planning, system development, technology adoption and procurement processes.

Ultimately, safeguarding our systems and data is about more than security. It is about protecting the continuity and integrity of Government services, sustaining public trust and ensuring that Sarawak's digital transformation remains secure, resilient and sustainable.

I therefore call upon every member of the Sarawak Civil Service and all our strategic partners to embrace the SCSR 2030 and play an active role in its implementation. The Strategy and Roadmap provides us with a common direction, but its success will depend on our collective commitment and the actions we take. Together, let us strengthen our vigilance, deepen our collaboration and build a secure, resilient and trusted digital ecosystem for Sarawak.



The Honourable Datuk Amar Haji Mohamad Abu Bakar Bin Marzuki

State Secretary of Sarawak

Message by the General Manager, Sarawak Multimedia Authority

The Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) marks an important step in establishing a coordinated approach to cyber security across Sarawak. It is the State's first comprehensive, Whole-of-Sarawak cyber security strategy, bringing together Government agencies, State-owned enterprises, critical infrastructure operators, businesses, academia and the wider community under a common direction.

The Strategy was developed to provide greater clarity on where Sarawak needs to strengthen its cyber security capabilities and how these capabilities can be developed progressively.

It brings together priorities that span the protection of strategic information assets, the safety of citizens and businesses, the development of local talent, governance and operational capability, and collaboration with national, regional and international partners.

SCSR 2030 is deliberately designed as a roadmap rather than a collection of standalone projects. Its initiatives are sequenced over five years so that foundational capabilities can be established first, followed by operationalisation, wider adoption and longer-term institutionalisation. This approach allows Sarawak to build capability progressively while adapting to changes in technology, cyber threats and the needs of the State.

A key principle of the Strategy is that cyber security cannot be managed effectively through fragmented efforts. A Whole-of-Sarawak approach enables common standards, stronger coordination, better sharing of information and more effective use of resources. It also provides a basis for organisations across Sarawak to understand their respective responsibilities and contribute to a stronger overall cyber security posture.



The Sarawak Multimedia Authority will play a central role in providing strategic leadership and coordinating the implementation of the Strategy.

This includes working with relevant State agencies and stakeholders to establish the governance, capabilities and partnerships required to deliver the roadmap. The Strategy will also evolve as circumstances change, with progress monitored and priorities reviewed to ensure that it remains relevant and effective.

However, no single organisation can deliver SCSR 2030 alone. Its success will depend on the willingness of government agencies, businesses, critical infrastructure operators, educational institutions, technology partners and communities to participate and take responsibility for the security of the systems, services and information within their respective spheres.

This Public Edition has been prepared to make the Strategy accessible to a wider audience. It provides an overview of the priorities and intended outcomes of SCSR 2030 without the detailed technical and implementation considerations contained in the full strategy. It is intended to help Sarawakians understand the direction we are taking and the role each of us can play.

I encourage all stakeholders to use this Strategy as a common reference point and to work together in turning its priorities into sustained action. Through shared responsibility, continuous improvement and practical collaboration, we can build the capabilities needed to support a secure and resilient digital Sarawak.



YBhg Dato Dr Anderson Tiong Ing Heng

General Manager
Sarawak Multimedia Authority

Table of Contents

Glossary 01

Executive Summary 02

Chapter 1 | Why Cyber Security Matters to Sarawak 06

Chapter 2 | Overview of Sarawak's Cyber Security Strategy & Roadmap 2030 10

Chapter 3 | Pillar 1 — Securing Sarawak's Strategic Information Assets 17

Chapter 4 | Pillar 2 — Protecting People, Businesses and Communities 19

Chapter 5 | Pillar 3 — Talent Development and Capacity Building 21

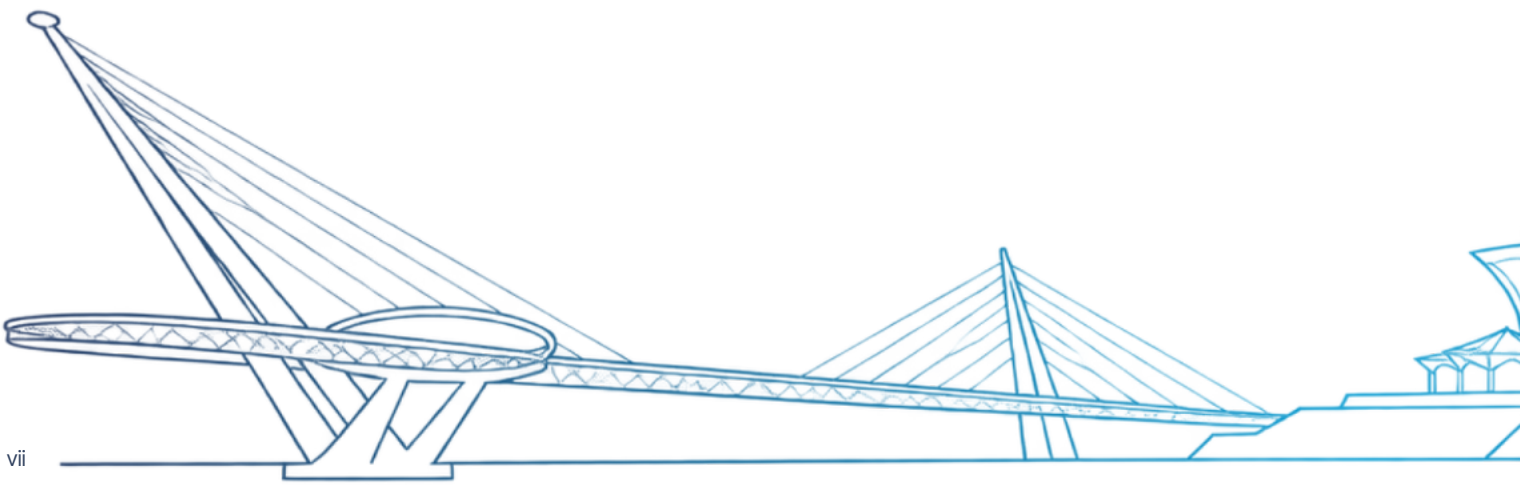
Chapter 6 | Pillar 4 — Strengthening Governance and Operational Framework 23

Chapter 7 | Pillar 5 — Strategic Collaboration and Cooperation 25

Chapter 8 | Conclusion 27

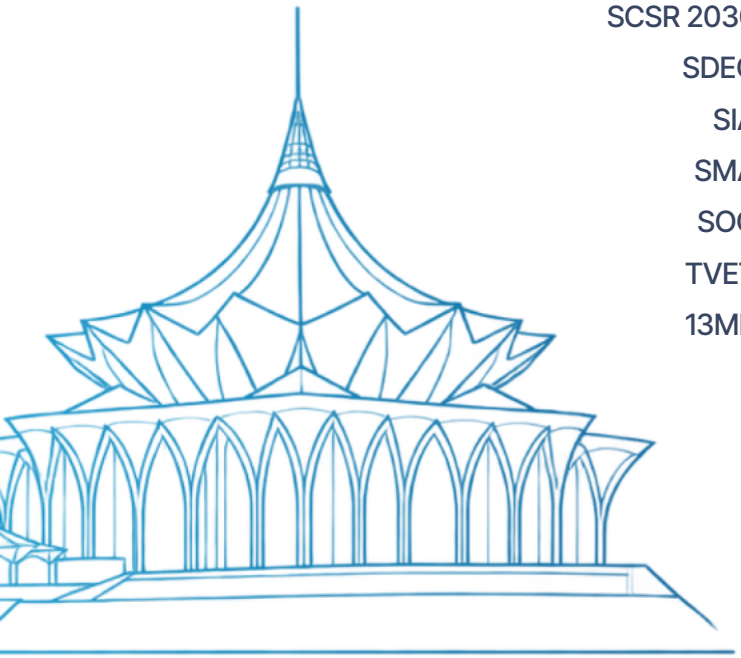
Appendix 1 | Acknowledgement 30

Appendix 2 | The Initiatives 34



Glossary

AI	Artificial Intelligence
CENTEXS	Centre for Technology Excellence Sarawak
CSA 2024	Cyber Security Act 2024 (Malaysia)
CSCDC	Cyber Security Cryptology Development Centre
DGC	Digital Government Committee
GLC	Government-Linked Company
MA63	Malaysia Agreement 1963
MCMC	Malaysian Communications and Multimedia Commision
MSME	Micro, Small and Medium Enterprise
MyCERT	Malaysia Computer Emergency Response Team
NACSA	National Cyber Security Agency
NC4	National Cyber Coordination and Command Centre
NCII	National Critical Information Infrastructure
NSRC	National Scam Response Centre
PCDS 2030	Post COVID-19 Development Strategy 2030
PDRM	Polis Diraja Malaysia (Royal Malaysia Police)
PQC	Post Quantum Cryptography
SAINS	Sarawak Information Systems Sdn Bhd
SCSDU	Sarawak Civil Service Digitalisation Unit
SCSR 2030	Sarawak Cybersecurity Strategy and Roadmap 2030
SDEC	Sarawak Digital Economy Corporation
SIA	Sarawak's Strategic Information Assets
SMA	Sarawak Multimedia Authority
SOC	Security Operations Centre
TVET	Technical and Vocational Education and Training
13MP	Sarawak 13th Malaysia Plan (2026–2030)



Executive Summary

Sarawak is accelerating its transformation into a digital economy where government services, businesses, critical infrastructure and communities increasingly rely on secure and trusted digital technologies. As digital adoption grows, so too does the importance of protecting essential services, sensitive information and public confidence against an evolving cyber threat landscape.

The Sarawak Cybersecurity Strategy and Roadmap (SCSR) 2030 establishes the State's first comprehensive, Whole-of-Sarawak cyber security strategy.

It provides a long-term framework to strengthen cyber resilience across the public sector, industry and society while supporting Sarawak's aspirations under the Post COVID-19 Development Strategy (PCDS) 2030 and the Sarawak Digital Economy Blueprint 2030. The strategy is aligned with Malaysia's national cyber security direction while addressing Sarawak's unique governance, economic priorities and digital ecosystem.

The Strategy recognises that cyber security is no longer solely a technical issue. It is a strategic enabler of economic growth, digital innovation, investor confidence, public trust and the continuity of essential services. Achieving a secure digital future requires collaboration among government agencies, critical infrastructure operators, businesses, academia, industry partners and the wider community.

The Strategy is guided by a clear vision:

"A secure and trusted foundation for Sarawak's digital economy"

To realise this vision, the Strategy seeks to achieve six long-term outcomes:

- Secure and resilient critical digital infrastructure supporting essential services.
- Better protection for citizens, businesses and communities against cyber threats.
- A skilled and sustainable cyber security workforce.
- Mature governance and coordinated cyber security management across the State.
- Stronger national and international cyber security partnerships.
- Greater confidence in Sarawak as a trusted digital economy and investment destination.

Vision of the Sarawak Cybersecurity Strategy and Roadmap 2030 are delivered through five strategies pillars:



Pillars and its respective outcomes

Pillar 1

Securing Sarawak's Strategic Information Assets

Protects the digital assets Sarawak depends on most — from government platforms to the networks behind power, water and other essential services.

Expected Outcome:

Critical information infrastructure across Sarawak operates with a mature, risk-based cyber security posture that safeguards essential services and public trust.

Pillar 2

Protecting People, Businesses and Communities

Equips Sarawakian citizens, MSMEs and communities with the awareness, tools and support to stay safe online and avoid scams.

Expected Outcome:

A safer and more trusted digital environment enables confident participation in Sarawak's digital economy by citizens and businesses.

Pillar 3

Talent Development and Capacity Building

Builds a homegrown pipeline of cyber security professionals, from school-age exposure through to certified experts and a growing local industry.

Expected Outcome:

Sarawak has a self-sustaining cyber security ecosystem supported by a skilled local workforce, thriving industry and continuous innovation.

Pillar 4

Strengthening Governance and Operational Frameworks

Gives Sarawak clear cyber security leadership and a centralised operational centre to coordinate protection and incident response statewide.

Expected Outcome:

Cyber security becomes an integrated and trusted enabler of Sarawak's digital government and digital economy.

Pillar 5

Strategic Collaboration and Cooperation

Connects Sarawak into national, regional and international cyber security networks for shared intelligence and coordinated response.

Expected Outcome:

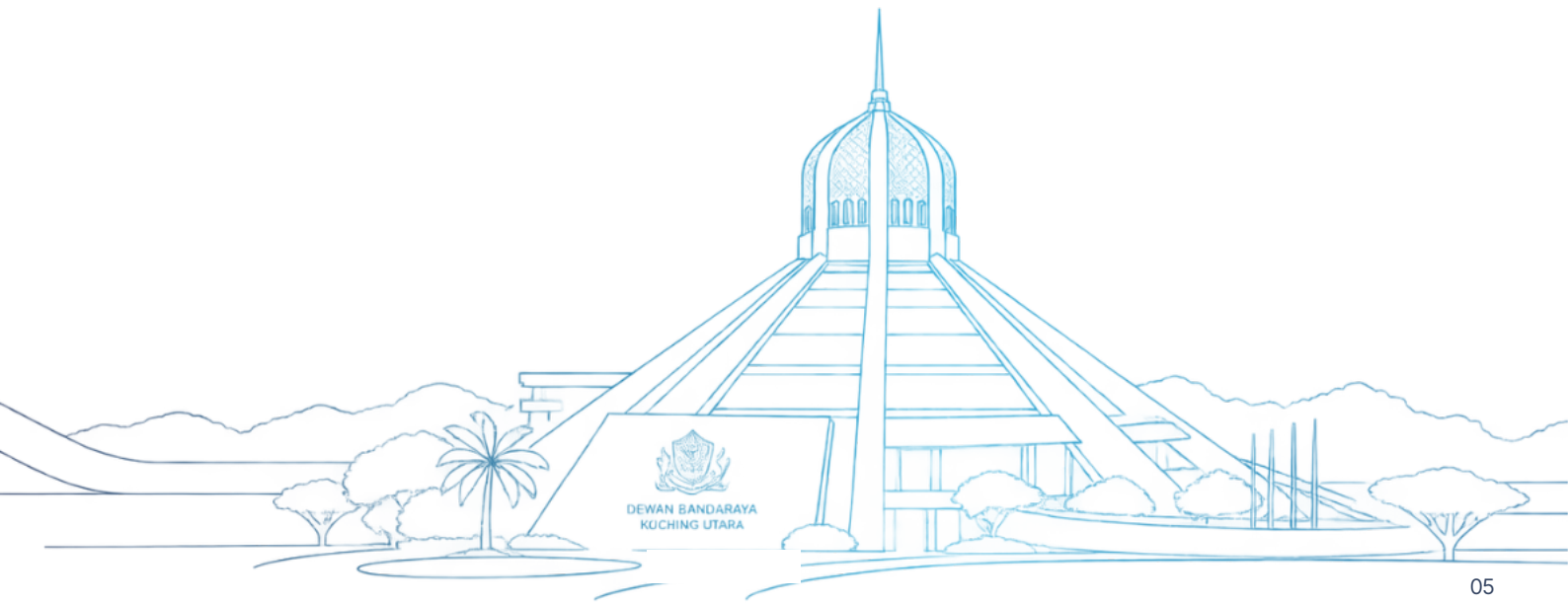
Strong national and international partnerships enhance collective cyber resilience while increasing investor confidence in Sarawak's secure digital economy.

Progressive phases to ensure readiness and sustainable long-term capability

Implementation of the Strategy will be phased over 5 years, allowing foundational capabilities to be established before progressively expanding cyber security programmes across the State. The roadmap sequences initiatives according to strategic priorities, organisational readiness and interdependencies, ensuring that investments build upon one another to create sustainable long-term capability.

The Strategy adopts a practical and collaborative implementation model. Success depends on sustained leadership, effective governance, strong partnerships and continuous improvement as technology, threats and business needs evolve. Progress will be monitored through measurable outcomes and regular reviews to ensure that the Strategy remains relevant and responsive throughout its implementation period.

Success will be reflected in a Sarawak where critical services are protected, businesses and MSMEs have access to practical cyber security support, Sarawakians can recognise and avoid online scams, a homegrown cyber security workforce and industry is taking root, and the State works hand-in-hand with Federal agencies and international partners to keep Sarawak's digital economy safe. Through this Strategy, cyber security will become a foundational capability that safeguards the State's digital future while supporting innovation, economic growth and the wellbeing of all Sarawakians.



Chapter 1

Why Cyber Security Matters for Sarawak

Connecting the foundation for Sarawak's digital economy

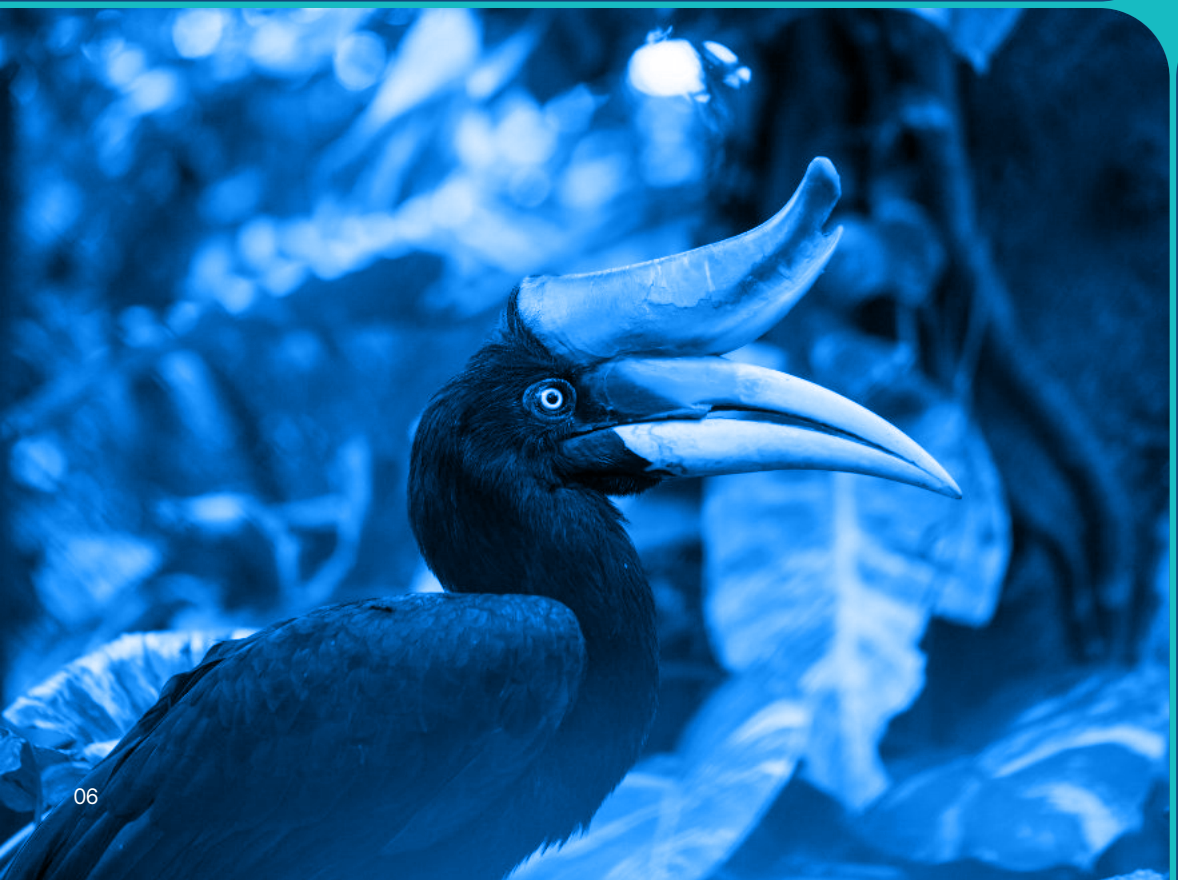
1.1 Cyber Security is the Foundation of Sarawak's Digital Future

1.2 Digital Transformation Creates New Opportunities and New Risks

1.3 Cyber Security is a Shared Responsibility

1.4 Building Trust in the Digital Economy

1.5 A Secure Future for Sarawak



Building trust and sharing resposibility in the era of digital transformation.

1.1 Cyber Security is the Foundation of Sarawak's Digital Future

Sarawak is rapidly becoming a more digitally connected economy. Government services, businesses and communities increasingly rely on digital technologies, while emerging technologies such as cloud computing, artificial intelligence and smart infrastructure with embeded Internet of Things (IoT) create new opportunities for growth and improved public services.

As digital dependence grows, cyber security becomes an essential foundation for protecting essential services, information, businesses and communities, while maintaining confidence in Sarawak's digital future.

Cyber security is therefore not simply an information technology concern. It is a strategic enabler of secure digital transformation, resilient public services, economic growth and public trust.

1.2 Digital Transformation Creates New Opportunities and New Risks

Greater digital connectivity also brings greater exposure to cyber threats. Cyber incidents can disrupt services, compromise information, affect businesses and undermine confidence in digital platforms.

As systems become increasingly interconnected, the impact of a cyber incident can extend beyond an individual organisation to government services, businesses, supply chains and communities.

Sarawak's cyber security capabilities must therefore evolve alongside its digital transformation, ensuring that digital progress is secure, resilient and sustainable.

1.3 Cyber Security is a Shared Responsibility

Cyber security cannot be achieved by government alone. Government agencies, critical infrastructure operators, businesses, educational institutions, technology providers and citizens all have a role in maintaining a secure digital environment.

The Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) adopts a Whole-of-Sarawak approach, bringing stakeholders together to strengthen cyber security awareness, capability and resilience across the State, supported by collaboration with Federal, regional and international partners.

Developing local skills and organisational capability is an important part of this effort, strengthening Sarawak's ability to manage cyber risks and support continued digital growth.

People first, Working together, For the future.

1.4 Building Trust in the Digital Economy

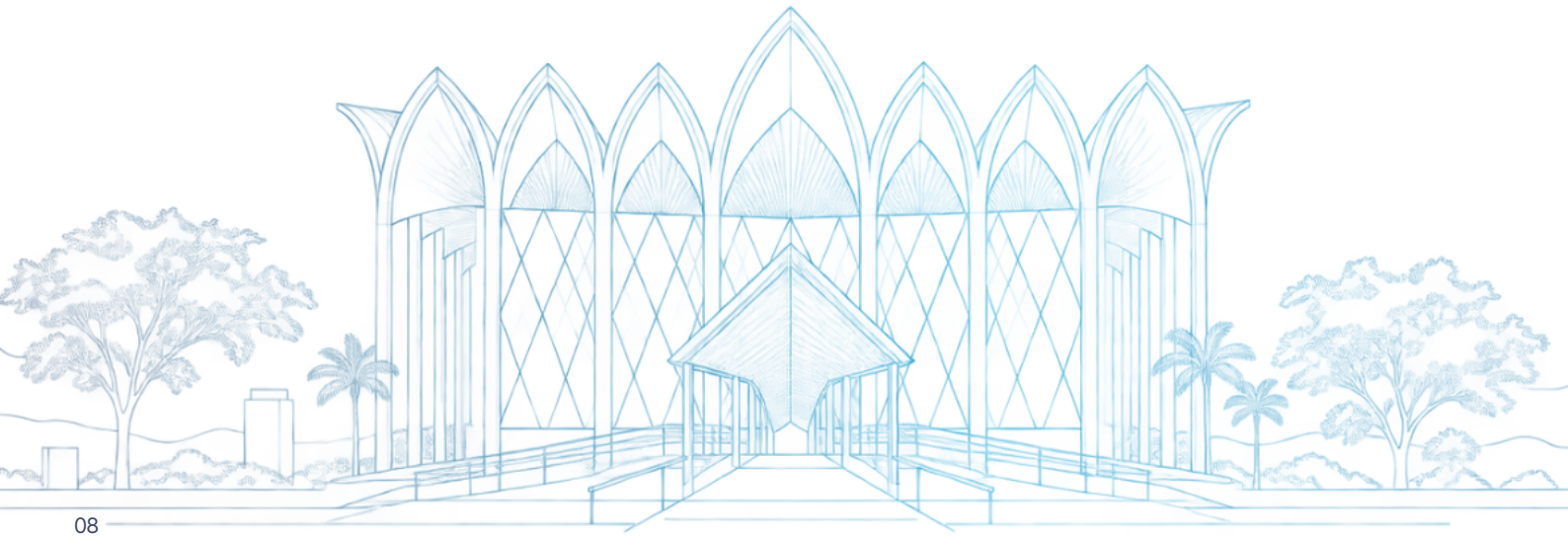
Trust is one of the most valuable assets in a digital economy. Citizens are more willing to use digital services when they are confident that their information is protected. Businesses invest more readily when digital infrastructure is reliable and secure. Investors seek jurisdictions that demonstrate strong governance, resilience and responsible management of cyber risks.

By strengthening cyber security, Sarawak strengthens the confidence that underpins digital government, digital commerce, innovation and investment. A trusted digital environment enables organisations to innovate, collaborate and grow with greater confidence.

1.5 A Secure Future for Sarawak

Cyber security is fundamental to achieving Sarawak's aspirations as a leading digital economy. Protecting critical services, supporting businesses, developing local talent and strengthening collaboration will help create a secure and trusted digital environment where innovation can flourish and communities can confidently embrace digital technologies.

The Sarawak Cybersecurity Strategy and Roadmap 2030 provides the strategic direction to achieve this vision. Through coordinated implementation across government, industry and society, cyber security will become an enduring foundation for sustainable economic growth, resilient public services and a safer digital future for all Sarawakians.



SCSR 2030

Supporting Sarawak's digital transformation, driven by SDE 2030 and PCDS 2030.

SECURE RESILIENT TRUSTED

Trusted Digital Government

- Reliable online government services
- Protected public data
- Public confidence
- Digital service continuity

Resilient Infrastructure

- Essential services remain available
- Critical systems protected
- Business continuity

Safe Citizens & Businesses

- Cyber awareness and resilience
- Strong cyber hygiene
- Digital trust for all

Skilled Cyber Workforce

- Education and professional development
- Local talent
- Future-ready workforce

Competitive & Innovative Digital Economy

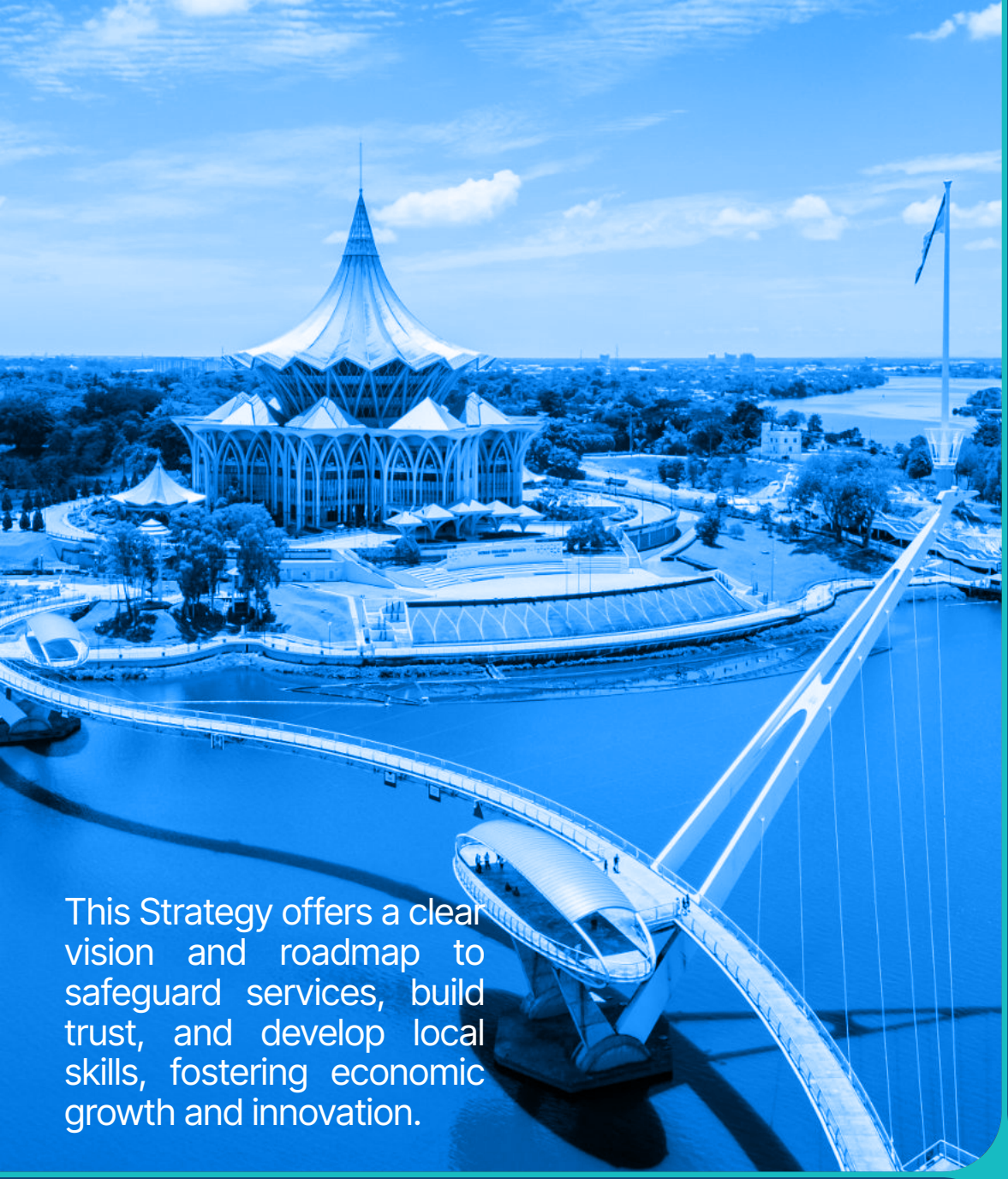
- Investor confidence
- Trusted digital ecosystem
- Innovation and economic growth

WORKING TOGETHER TO BUILD A SECURE DIGITAL FUTURE

Government | Industry | Critical Infrastructure | Academia | Communities | Citizen

VISION 2030

A Secure and Trusted Foundation For Sarawak's Digital Economy



This Strategy offers a clear vision and roadmap to safeguard services, build trust, and develop local skills, fostering economic growth and innovation.

Chapter 2

Overview of the Sarawak Cybersecurity Strategy and Roadmap 2030

2.1 A Strategic Roadmap for a Secure Digital Future
2.2 Purpose of the Strategy
2.3 Strategy Framework
2.4 A Whole-of-Sarawak Approach
2.5 A Phased Roadmap over Five Years

Building trust and sharing resposibility in the era of digital transformation.

2.1 A Strategic Roadmap for a Secure Digital Future

The Sarawak Cybersecurity Strategy and Roadmap (SCSR) 2030 is the State's long-term strategic framework for strengthening cyber security and building a secure, resilient and trusted digital ecosystem.

The Strategy provides a coordinated direction for government, industry, academia and the wider community to work together in addressing cyber security challenges while enabling Sarawak's digital transformation and economic growth. It recognises that cyber security is no longer solely a technical issue, but a strategic enabler that underpins public trust, protects essential services and supports innovation, investment and sustainable development.

Designed as a Whole-of-Sarawak strategy, the SCSR 2030 establishes a common vision, shared priorities and a structured implementation roadmap to guide cyber security development across Sarawak through to 2030.

2.2 Purpose of the Strategy

The Strategy provides a common direction for strengthening cyber security across the State by:

- Establishing a long-term vision for cyber security in Sarawak;
- Providing a coordinated framework for government, industry and other stakeholders;
- Strengthening cyber resilience across critical sectors;
- Promoting a secure and trusted digital environment for citizens and businesses;
- Developing sustainable cyber security capabilities and talent; and
- Supporting Sarawak's aspirations as a leading digital economy.

Rather than creating standalone cyber security programmes, the Strategy integrates cyber security into Sarawak's broader digital transformation journey, ensuring that security and resilience become integral components of future development.

The roadmap and strategic framework for long-term and continuous improvement

2.3 Strategy Framework

The Sarawak Cybersecurity Strategy and Roadmap (SCSR) 2030 is the State's long-term strategic framework for strengthening cyber security and building a secure, resilient and trusted digital ecosystem.

The framework comprises of three key components:

Vision
A clear long-term aspiration that defines the future state Sarawak seeks to achieve.

Strategic Initiatives
A coordinated portfolio of strategic initiatives that progressively deliver the outcomes through a phased implementation roadmap.

Strategic Pillars
Five strategic pillars that organise the Strategy into priority areas for action and collectively strengthen every dimension of Sarawak's cyber security ecosystem.

Together, these components ensure that every initiative contributes towards a common vision while providing a structured pathway for implementation and continuous improvement.

2.4 A Whole-of-Sarawak Approach

No single organisation can secure the State's digital ecosystem alone. The Strategy therefore adopts a Whole-of-Sarawak governance and delivery model that brings together policy leadership, programme coordination and operational implementation to achieve a common vision.

By fostering partnership, information sharing and coordinated action, the Strategy promotes a shared responsibility for protecting Sarawak's digital future.

The Strategy therefore adopts a phased implementation approach that progressively builds cyber security capability while ensuring that each stage establishes the foundation for the next.

This structured approach enables Sarawak to strengthen governance and institutional capabilities first, before expanding cyber security programmes, developing advanced capabilities and embedding cyber security as a long-term enabler of the State's digital economy.

2.5 A Phased Roadmap over Five Years

Recognising that cyber security capability develops progressively over time, the Strategy adopts a phased implementation approach over a period of five years. This allows foundational capabilities to be established before progressively expanding cyber security programmes across the State. The roadmap sequences initiatives according to strategic priorities, organisational readiness and interdependencies, ensuring that investments build upon one another to create sustainable long-term capability.

Building sustainable cyber security capability

Phase 1

Build - Year 1

The first phase establishes the foundations necessary for successful implementation. It focuses on building the tools and knowledge Sarawak will rely on for years to come. This includes creating common cyber security frameworks — essentially, shared rules and standards that everyone can follow — alongside the first awareness programmes to help government agencies, businesses and the public understand cyber risks. Sarawak also begins developing its first real cyber defence capability, meaning it starts to actively monitor for and respond to threats rather than simply reacting after something goes wrong. By the end of this year, priority government agencies will already be under active protection, and Sarawak will have a shared understanding of what good cyber security looks like across the State.

Phase 2

Operationalise - Year 2

This is the year the groundwork laid previously starts running in full swing. Cyber security services become fully operational across the State Government, supported by common protection standards and access to timely threat intelligence — meaning up-to-date information about the latest scams and cyberattacks. Rather than being tested in small pilot projects, government digital services and critical infrastructure move to being consistently protected and monitored, day in and day out. At the same time, businesses, citizens and agencies begin to benefit directly, gaining access to practical tools and early warnings that help them avoid falling victim to cyber threats. This marks the point where Sarawak's cyber security efforts move from planning to genuine, everyday protection.

Phase 3

Scale - Year 3

Having proven that its cyber security approach works, Sarawak now expands it further — reaching more critical sectors, more businesses and more communities across the State. This is the year Sarawak's cyber resilience is truly put to the test at a state-wide scale for the first time, demonstrating that the systems and protections put in place can hold up under real pressure. As this expansion takes hold, confidence grows among both the public and the business community, who begin to see and feel the benefits of a safer digital environment. Sarawak's growing credibility in this space also starts to be recognised beyond its own borders, laying the groundwork for stronger regional standing in the years ahead.

Building sustainable cyber security capability

Phase 4 **Institutionalise - Year 4**

By this stage, cyber security is no longer treated as a special project or a one-off initiative — it becomes a normal, ongoing part of how Sarawak's government and workforce operate. This year focuses on weaving cyber security into everyday government operations, continuing to grow local talent through workforce development, and strengthening ties with international partners. The result is equitable protection for all Sarawakians, regardless of where they live or which agency serves them, along with a strengthening pipeline of future cyber security professionals coming up through Sarawak's own education and training systems. This year also marks Sarawak's first formal international collaboration credential — a milestone that signals the State's cyber security efforts are being recognised on the global stage.

Phase 5 **Sustain - Year 5**

In the final phase of this roadmap, Sarawak reaches a place where its cyber security ecosystem can largely sustain itself. Nearly all of the State's critical infrastructure — the systems and services Sarawakians depend on every day — will be under mature protection. This is made possible not just by government effort alone, but by a thriving local cyber security industry that has grown alongside the Strategy, creating jobs and expertise within Sarawak itself. Reaching this point of maturity earns the trust of both the public and investors, giving them confidence that Sarawak's digital economy is being safeguarded for the long term, well beyond the life of this Strategy.

By providing a clear vision, coordinated priorities and a practical roadmap for implementation, the Strategy will help safeguard essential services, build public confidence, develop local capabilities and create a secure environment in which innovation and economic growth can flourish.

Given that the Strategy spans a five-year period, its action plans and initiatives may be refined and updated to keep pace with technological advancements, emerging cyber threats and changing needs. Such changes will be guided by regular reviews throughout the implementation period, ensuring that the SCSR 2030 remains relevant, responsive and effective while maintaining its overall strategic direction and intended outcomes.

The following chapters describe the Strategy in greater detail, beginning with the five strategic pillars, their objectives, intended outcomes, and in Appendix 2, the subsequent individual initiatives under each pillars.

Building a secure, resilient and trusted digital future

	Results	Value
Year 1 Build	Common cyber security frameworks, awareness programmes and the State initial cyber defence capability are established.	Sarawak gains a shared baseline and common understanding to guide future programmes, plus its first tangible Whole-of-Sarawak cyber defence capability, already protecting priority services from Year-1.
Year 2 Operationalize	Statewide cyber security services become fully operational across government, supported by common protection standards and threat intelligence.	Government digital services and critical infrastructure move from pilot to consistently protected and monitored statewide, while businesses, citizen and agencies gain practical tools and early threat intelligence to reduce cyber risk.
Year 3 Scale	Cyber security capabilities expand across critical sectors, businesses, and communities, strenthening statewide resilience.	Sarawak's cyber resilience is tested and proven at state scale for the first time. Public and businesses confidence grows through wider protection and support, and Sarawak's cyber security credibility begins to extend regionally.
Year 4 Institutionalize	Cyber security becomes embedded in government operations, workforce development and international collaboration.	Cyber security becomes embedded as a standard, ongoing practice rather than a project – delivering equitable protection for all Sarawakians, a strengthening future worksforce pipeline, and Sarawak's first international collaboration embedded.
Year 5 Sustain	A mature, agile cyber security ecosystem supports secure digital government, industry and economic growth.	Sarawak achieves a mature, continously adapting cyber security ecosystem – protecting nearly all critical infrastructure, anchored by a thriving local industry, an emerging high-skilled and innovative talent seeded to sustain long-term digital economic growth.

Five Strategic Pillars of Sarawak's Cyber Security Strategy

	Description
Pillar 1	Sarawak's Strategic Information Assets (SIA) operates with a mature, risk-based cyber security posture that safeguards essential services and public trust.
Pillar 2	Protects Sarawak's people and businesses from growing cyber and scam risks, reducing financial and social harm while building confidence in the State's digital economy.
Pillar 3	Build a sustainable local cyber security capability, reducing Sarawak's dependence on scarce external expertise while strengthening its ability to protect its digital economy and respond to emerging cyber threats.
Pillar 4	Strengthens Whole-of-Sarawak coordination and accountability, enabling faster and more effective management of cyber risks and reducing disruption to essential digital services.
Pillar 5	Connects Sarawak to national and regional cyber defence networks, enabling earlier access to intelligence, expertise and collective action against threats that cross organisational and geographical boundaries.



Source: Sarawak Metro. *Autonomous Rapid Transit (ART)*. 2023. Sarawak Metro. https://www.mysarawakmetro.com/what-we-do/kuching-urban-transportation-system

Chapter 3

Pillar 1 — Securing Sarawak's Strategic Information Assets

Why this pillar matters

Essential services — from digital government platforms to power, water and transport systems — depend on computer systems that, if disrupted, could affect the safety, economy and daily lives of Sarawakians. This pillar identifies, classifies and protects those systems, complementing Malaysia's National Critical Information Infrastructure (NCII) framework with a State-level layer of protection.

Expected Outcome

Sarawak's Strategic Information Assets (SIA) operate with a mature, risk-based cyber security posture that safeguards essential services and public trust.

Initiative 1

Identification and Prioritisation of Sarawak's Strategic Information Assets (SIA)

Summary:

Sarawak depends on many digital systems, from government platforms to power, water and transport networks and as digitalisation continues to expand, there is a need to further strengthen the State's understanding of which systems are most critical to Sarawak's essential services and strategic interests. This initiative creates that picture: a clear, up-to-date map of Sarawak's most important digital assets, so government can focus protection and resources on the systems that matter most, working alongside Malaysia's national framework for critical infrastructure rather than duplicating it.

Initiative 2

Sarawak's SIA Cyber Security Baseline and Maturity Assessment

Summary:

Not every organisation managing an critical digital system in Sarawak currently follows the same cyber security standards. This initiative sets a common, practical benchmark for what "good" cyber security looks like, and helps each organisation understand where it stands today and what it needs to improve so that protection becomes more consistent across the State rather than depending on which agency or company happens to be involved.

Initiative 3

SIA Cyber Security Implementation Guidance and Best Practices

Summary:

Knowing the standard to meet is only half the battle, organisations also need practical help getting there. This initiative provides straightforward guidance, checklists and sector-specific advice so that those responsible for Sarawak's critical systems know exactly what steps to take, without needing to be cyber security experts themselves.

Initiative 4

State Cyber Resilience Exercises and Preparedness

Summary:

Plans and defences are only as good as they prove to be when tested. This initiative introduces regular cyber-attack simulations and emergency exercises, from tabletop discussions to full-scale drills so that government agencies and critical service providers can find and fix weaknesses before a real incident happens, and respond faster and more effectively if one ever does.

Chapter 4

Pillar 2 — Protecting People, Businesses, and Communities

Why this pillar matters

Over 90% of Sarawakian households are online, while MSMEs make up more than 90% of the State's business sector. As online crime losses nearly doubled between 2021 and 2023, most businesses still lack baseline cyber security protection. This pillar equips citizens and businesses, particularly MSMEs and vulnerable communities, with the awareness, tools and support to stay safe online.

Expected Outcome

People, businesses and communities across Sarawak are better able to recognise, prevent and respond to cyber threats, resulting in safer digital behaviour, fewer avoidable cyber incidents and greater confidence in participating in the digital economy.



Initiative 5

Cyber Hygiene Adoption for Sarawak Businesses

Summary:

Sarawak businesses, particularly micro, small and medium enterprises (MSMEs), can benefit from practical and accessible support to strengthen their cyber security practices. This initiative brings simple, practical cyber security habits — like using strong passwords, keeping software updated and backing up important data — directly into the business support programmes many Sarawak MSMEs already use, with trained local business champions and district-level support helping them along the way.

Initiative 6

Tailored Cyber Security Awareness and Digital Resilience for Sarawak Communities

Summary:

A single awareness campaign cannot reach everyone in Sarawak the same way — rural communities, indigenous groups, senior citizens and young people all have different needs and different ways of accessing information. This initiative delivers cyber security awareness that is tailored to each community, in local languages and through trusted local messengers, so that safe online habits reach every corner of the State.

Initiative 7

Sarawak Scam Prevention and Victim Support

Summary:

When someone in Sarawak falls victim to an online scam, getting quick, clear local advice matters. This initiative sets up local scam prevention and support services that work alongside national bodies such as the National Scam Response Centre and the police — helping people report scams easily, get timely guidance, and access the right support to recover, while also using scam trends to warn others before they become victims too.

Initiative 8

Sarawak Cyber Security Readiness and Recognition Programme

Summary:

Sarawak businesses can benefit from a practical and accessible way to assess and progressively strengthen their cyber security readiness. This initiative gives Sarawak businesses a simple way to check their own readiness, improve step by step, and earn recognition for doing so — creating a practical stepping stone towards stronger protection and, for those who need it, a pathway to nationally or internationally recognised certification.

Chapter 5

Pillar 3 — Talent Development and Capacity Building

Why this pillar matters

Cyber security is only as strong as the people and capabilities available to sustain it. This pillar ensures Sarawak has the people, skills, and local expertise needed for its digital ambitions. By developing a stronger local talent pipeline and institutional capability, Sarawak can reduce dependence on external expertise, create high-value opportunities and remain prepared for increasingly sophisticated cyber threats.

Expected Outcome

Sarawak has a self-sustaining cyber security ecosystem supported by a skilled local workforce, thriving industry and continuous innovation.



Initiative 9

Cyber Security Career Pathway and Youth Talent Development

Summary:

Sarawak has a growing pool of young people with the potential to pursue careers in cyber security, and increasing their exposure to this dynamic and rapidly evolving field from an early stage can help encourage greater interest and participation. This initiative introduces students to cyber security through school workshops, hands-on activities and youth competitions, helping to inspire interest, develop practical skills and strengthen the pipeline of local cyber security talent that Sarawak will need in the years ahead.

Initiative 10

Sarawak Cyber Security Workforce Demand and Skills Alignment

Summary:

As the cyber security landscape continues to evolve, there is an opportunity to further strengthen the alignment between cyber security education and the skills sought by employers. This initiative brings government, industry and universities together to enhance training and course offerings in line with emerging industry needs and employment opportunities in Sarawak, helping graduates build relevant skills for the workforce while supporting local employers in developing and accessing the talent they need closer to home.

Initiative 11

Cyber Security Leadership and Governance Capability

Summary:

Cyber security isn't just a job for IT departments — it's a responsibility that belongs in the boardroom too. This initiative helps business leaders and senior managers understand cyber risk well enough to make good decisions about it, so that protecting the organisation becomes a shared priority at every level, not just something left to technical staff.

Initiative 12

Cyber Security Professional Development and Certification

Summary:

Building a strong pool of recognised cyber security professionals requires accessible pathways for Sarawakians to develop and validate their skills against recognised industry standards. This initiative expands access to globally recognised cyber security certifications through targeted sponsorship and support, while establishing a registry of certified local professionals to help Sarawak develop, recognise and showcase its growing cyber security talent.

Initiative 13

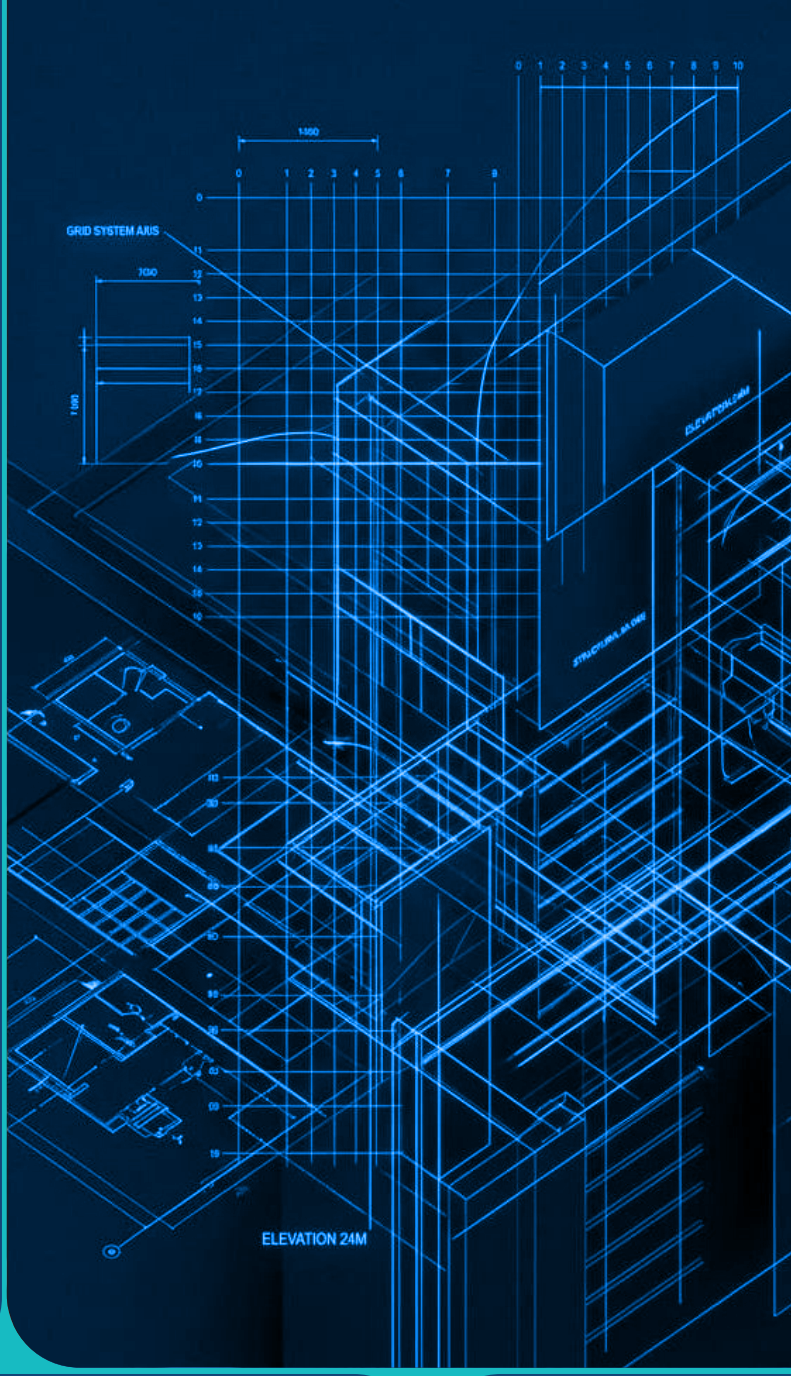
Emerging Technologies Adoption for Advanced Cyber Threats Protection

Summary:

New technologies like artificial intelligence bring real benefits, but they also open the door to new kinds of cyber threats — and one day, powerful "quantum" computers will even challenge the encryption we rely on today to keep information safe. This initiative helps Sarawak stay ahead of these changes, building the skills and readiness needed to adopt new technologies safely and prepare early for the security challenges of tomorrow.

Chapter 6

Pillar 4 — Strengthening Governance and Operational Framework



Why this pillar matters

Cyber security responsibilities today are spread across multiple State entities without a single coordinating operational function, and 86% of surveyed organisations say they need technical advisory support during a cyber incident. This pillar gives Sarawak clear cyber security leadership and a single operational centre capable of coordinating protection, incident response and advisory services across the whole State.

Expected Outcome

Cyber security becomes an integrated and trusted enabler of Sarawak's digital government and digital economy.

Initiative 14

Institutionalising Whole-of-Sarawak Cyber Security Governance

Summary:

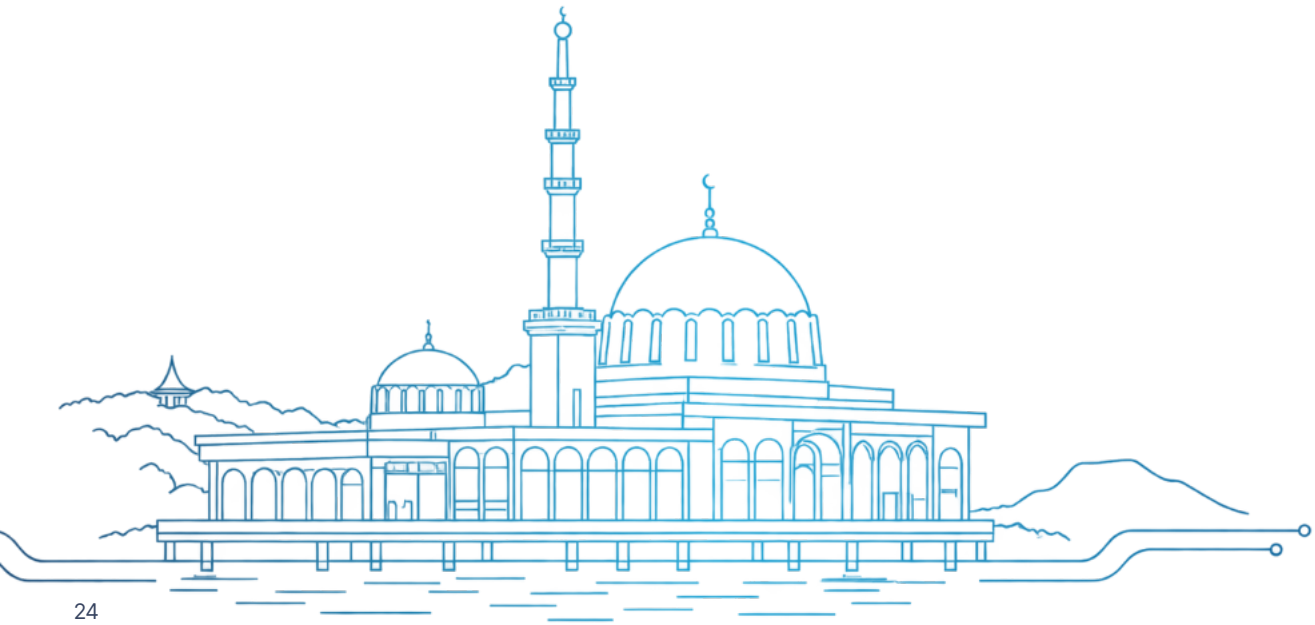
As cyber security responsibilities span different State agencies and stakeholders, strong coordination and clarity of roles are essential to ensuring consistent and effective action across the State. This initiative establishes a clear governance framework that defines responsibilities and accountabilities, enabling Sarawak's cyber security efforts to operate in a more coordinated and cohesive manner, with agencies and stakeholders better positioned to respond collectively to emerging cyber threats.

Initiative 15

Establishing a Centralised State Cyber Security Operations and Coordination Capability

Summary:

When a cyber incident happens, every minute counts. As Sarawak's digital ecosystem continues to grow, stronger coordination and shared situational awareness are increasingly important for detecting, assessing and responding to cyber threats across the State. This initiative establishes a central capability to provide round-the-clock monitoring, support faster and more coordinated incident response, and serve as a trusted point of contact for government agencies, critical information assets operators and businesses when cyber incidents occur.





Chapter 7

Pillar 5 — Strategic Collaboration and Cooperation

Why this pillar matters

No state can secure its digital ecosystem alone. As cyber threats increasingly transcend organisational and national boundaries, Sarawak must work closely with Federal agencies, industry and trusted international partners to strengthen collective resilience. This pillar positions Sarawak as an active contributor to national, regional and international cyber security networks, enabling the State to leverage partnerships, shared expertise and coordinated action to better protect its digital economy and critical services.

Expected Outcome

Sarawak strengthens its cyber resilience through trusted partnerships, coordinated information sharing and collaborative action with Federal agencies, industry and international partners, enabling a more secure and resilient digital ecosystem.

Initiative 16

Strategic Cyber Security Partnerships and Collaboration

Summary:

No state can fight cyber threats alone, and building Sarawak's reputation as a trusted digital economy means being an active, visible partner on the regional and global stage. This initiative builds Sarawak's relationships with national, regional and international cyber security organisations, turning these connections into practical support — from shared learning to joint programmes — that directly benefit Sarawak.

Initiative 17

State Cyber Threat Intelligence Coordination and Operationalisation

Summary:

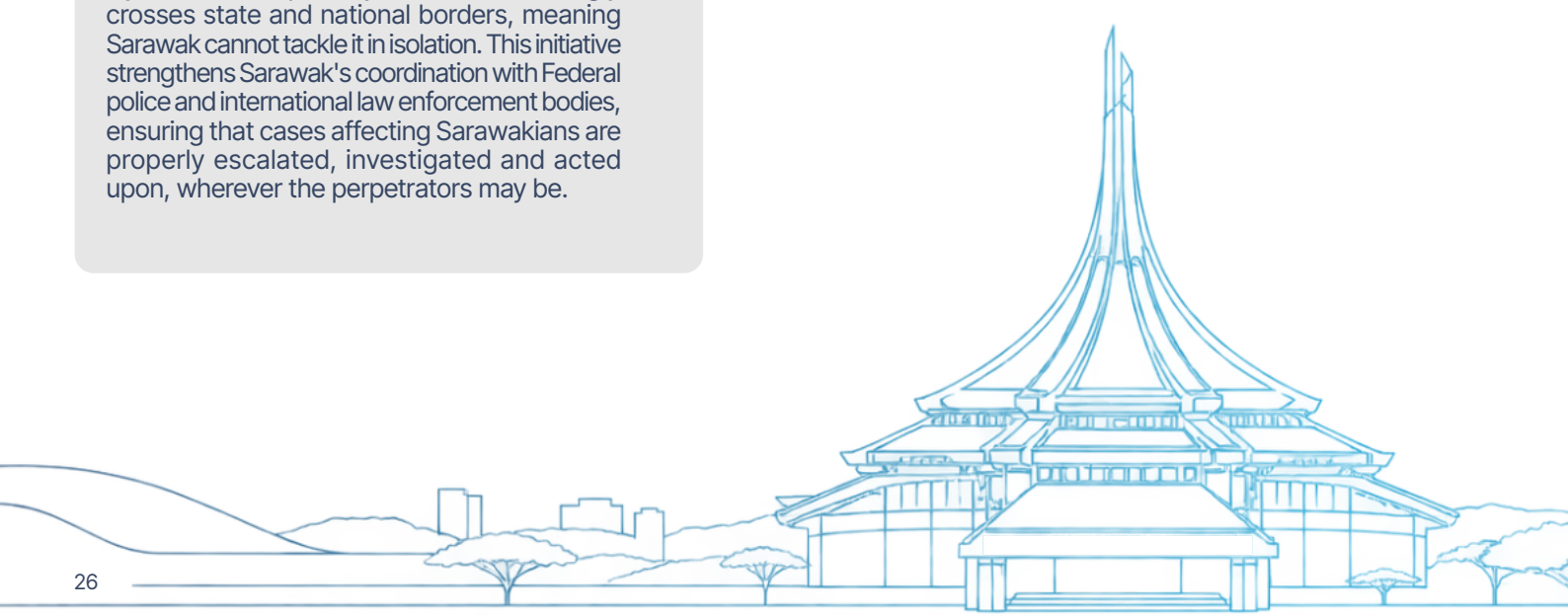
Knowing about a cyber threat early can make all the difference between preventing an incident and cleaning up after one. This initiative sets up formal channels for Sarawak to receive timely, relevant threat information from Federal agencies and trusted partners, and to turn that information into clear warnings and guidance that Sarawak's own agencies and businesses can act on quickly.

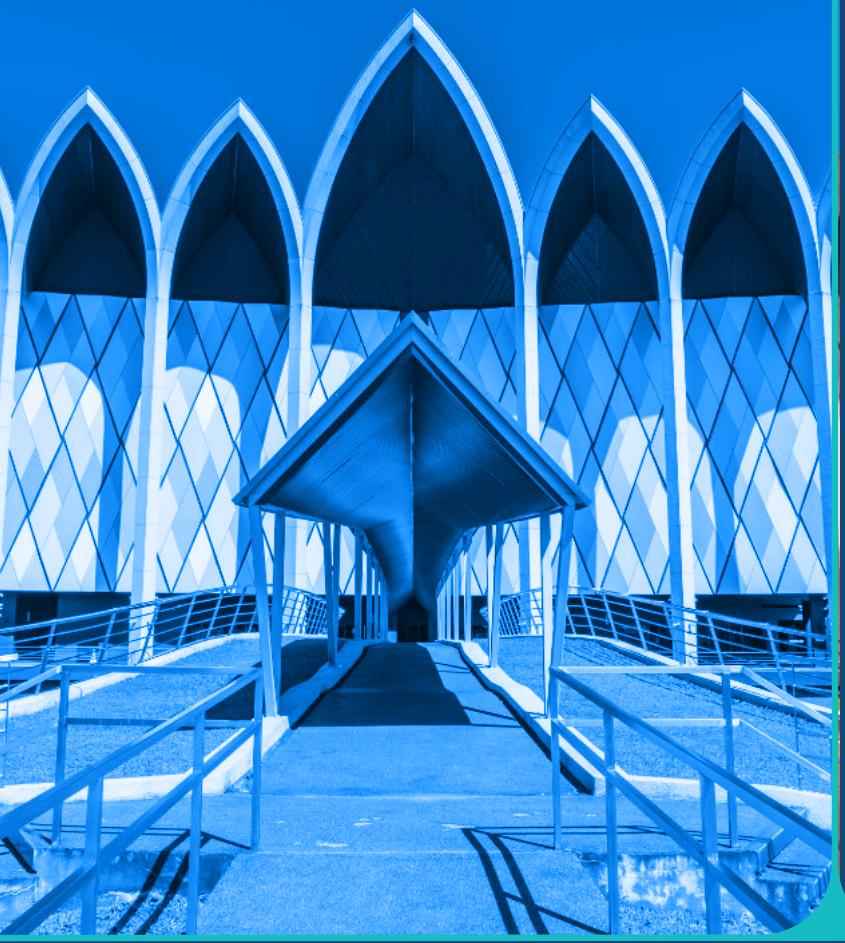
Initiative 18

Collaborative Cybercrime Prevention and Response

Summary:

Cybercrime, especially scams, increasingly crosses state and national borders, meaning Sarawak cannot tackle it in isolation. This initiative strengthens Sarawak's coordination with Federal police and international law enforcement bodies, ensuring that cases affecting Sarawakians are properly escalated, investigated and acted upon, wherever the perpetrators may be.





Chapter 8

Conclusion

Sarawak's digital future depends on technology being adopted securely, responsibly and with confidence. As Government, businesses, critical services and communities become increasingly connected, cyber security must remain a shared and ongoing responsibility.

A secure digital Sarawak is a continuous commitment to resilience, trust and readiness for the future.

Conclusion

Sarawak's digital future will depend not only on how effectively we adopt technology, but also on how confidently we can trust and rely on it. As more government services, businesses, essential services and communities become digitally connected, cyber security must become an integral part of how Sarawak plans, develops and operates its digital ecosystem.

The Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) establishes the State's first comprehensive, Whole-of-Sarawak direction for achieving this. Its vision is clear that is to be A Secure and Trusted Foundation for Sarawak's Digital Economy.

SCSR 2030 provides a common direction for Government, businesses, critical infrastructure operators, academia and communities.

Its five strategic pillars bring together the key areas that must be strengthened: protecting strategic information assets; protecting people, businesses and communities; developing local talent and capabilities; strengthening governance and operational coordination; and building strategic partnerships.

The Strategy is designed to be implemented progressively. Foundational capabilities will be established first, followed by the expansion of protection, services and capabilities across the wider State. This phased approach allows Sarawak to build on what has been achieved, learn from implementation and direct resources towards areas of greatest need.

The Strategy is also deliberately designed to evolve. Cyber threats will continue to change, technologies will advance and Sarawak's digital ecosystem will expand. The initiatives and action plans under SCSR 2030 may therefore be refined over time to remain relevant to emerging risks, technologies and State priorities, while its long-term vision and strategic direction remain constant.

Cyber security cannot be achieved by Government alone. Every organisation and individual connected to Sarawak's digital ecosystem has a role to play.



Government agencies must strengthen the security and resilience of the services they provide. Businesses must protect their systems, information and customers. Educational institutions and industry must help develop the skills Sarawak needs. Communities and individuals must remain informed and adopt safer digital practices. Federal, regional and international partnerships will also remain important because cyber threats do not stop at organisational or geographical boundaries.

A Whole-of-Sarawak approach brings these efforts together so that progress in one part of the ecosystem strengthens resilience across the State.

The success of SCSR 2030 will not ultimately be measured by the number of initiatives completed or technologies deployed. It will be reflected in the outcomes experienced by Sarawakians.

It will mean that essential digital services are more resilient and better protected. Citizens and businesses are better equipped to recognise and avoid cyber threats. Organisations have access to the skills and support they need. Sarawak develops a stronger pool of local cyber security talent and expertise.

Government and industry work together with greater coordination and confidence. And Sarawak's growing digital economy operates within an environment that people and investors can trust.

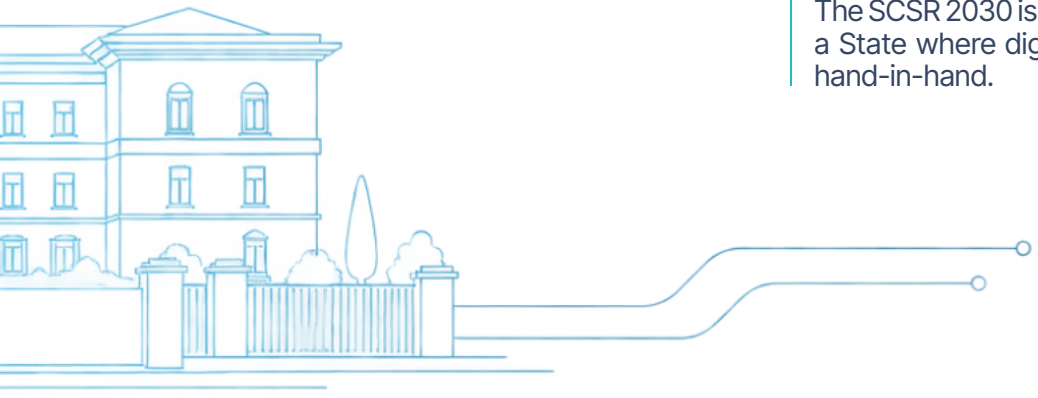
These outcomes will strengthen not only Sarawak's cyber security posture, but also its capacity to pursue digital innovation, economic development and better public services with greater confidence.

SCSR 2030 is therefore not an endpoint. It is the foundation for a continuing journey of strengthening resilience, building capability and maintaining trust as Sarawak's digital economy evolves.

The commitment is straightforward: Sarawak must be able to embrace the opportunities of digitalisation without compromising the security, trust and resilience on which those opportunities depend.

By working together, strengthening our own capabilities and continuously improving our approach, Sarawak can build a digital environment in which people can participate with confidence, businesses can grow securely, essential services can remain resilient, and innovation can flourish.

The SCSR 2030 is Sarawak's commitment to that Future: a State where digital growth and digital trust advance hand-in-hand.



Appendix 1 | Acknowledgement

Acknowledgement and Gratitude to Sarawak Cybersecurity Strategy and Roadmap 2030 Team

SMA wishes to record its highest appreciation to The Right Honourable Premier of Sarawak, Datuk Patinggi Tan Sri (Dr) Abang Haji Abdul Rahman Zohari bin Tun Datuk Abang Haji Openg, as Chairman of the Authority, and to the Members of the Authority, for their leadership, guidance, support, and institutional oversight in relation to the development and adoption of the SCSR 2030.

Sarawak Multimedia Authority Member of Authority

- YAB Datuk Patinggi Tan Sri (Dr) Abang Haji Abdul Rahman Zohari Bin Tun Datuk Abang Haji Openg
  2017 – Present
- YB Datuk Amar Douglas Uggah Anak Embas
  2018 – Present
- YBhg Datuk Patinggi Tan Sri Datuk Amar Dr George Chan Hong Nam
  2018 – Present
- YB Datuk Haji Julaihi Bin Haji Narawi
  2022 – Present
- YB Datuk Amar Haji Mohamad Abu Bakar bin Marzuki
  2022 – Present
- YBhg Dato Sri Dr Wan Lizozman bin Wan Omar
  2021 – Present
- Yang Arif Dato Sri Saferi Bin Ali
  2023 – Present
- YBhg Dato Sri Dr Muhammad Abdullah Bin Haji Zaidel
  2023 – Present
- YBhg Tan Sri Datuk Amar Haji Mohamad Morshidi bin Abdul Ghani
  2017 – Present
- YBrs Professor Jugdutt Singh
  2018 – Present

Digital Government Committee

- YB Datuk Amar Haji Mohamad Abu Bakar bin Marzuki
  2021 – Present
- YBhg Dato Sri Dr Wan Lizozman bin Wan Omar
  2021 – Present
- Yang Arif Dato Sri Saferi Bin Ali
  2023 – Present
- YBhg Dato Sri Dr. Muhammad Abdullah Bin Haji Zaidel
  2023 – Present
- YBhg Datu Hii Chang Kee
  2023 – Present
- YBhg Datu Felicia Tan Ya Hua
  2026 – Present
- YBhg Datu Haji Abdullah Bin Julaihi
  2023 – Present
- YBhg Datu Chiew Chee Yau
  2025 – Present
- YBhg Datu Haji Adana Bin Haji Jed
  2025 – Present
- YBhg Datu Jafri bin Lias
  2023 – Present
- YBhg Datu Elizabeth Loh
  2023 – Present
- YBhg Datu Sharifah Rohana Binti Wan Alwi
  2025 – Present
- YBhg Datu Grace Huong Siew Hung
  2023 – Present
- YBhg Datu Ir Ts Awg. Mohammad Fadillah bin Awg. Redzuan
  2026 – Present
- YBhg Dato Dr Anderson Tiong
  2023 – Present
- YBrs Madam Nur Alina Abdullah @ Colliner Gohe
  2026 – Present

SMA also wishes to record its sincere appreciation to YB Datuk Amar Haji Mohamad Abu Bakar bin Marzuki, Sarawak State Secretary, as Chair of the Digital Government Committee, and to the Members of the Digital Government Committee, for their leadership, guidance, consideration, and support in the approval and adoption of the Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) as a strategic framework to advance cyber security governance and strengthen the cyber resilience of the Sarawak Government.

Consultant

SMA wishes to express its sincere appreciation to PricewaterhouseCoopers Risk Services Sdn. Bhd. (PwC) for its professional expertise, strategic guidance and technical support as the consultant engaged to assist in the development of SCSR 2030. Through its assessments, stakeholder engagements, research, analysis and recommendations, PwC has made a significant contribution towards the formulation of a comprehensive and future-ready cyber security strategy to strengthen cyber security governance and resilience across Sarawak.

Stakeholders and Contributors

SMA further wishes to record its sincere appreciation to all participating agencies, stakeholders and contributors who have provided their time, commitment, institutional knowledge, technical expertise, valuable insights and support towards the development of the Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030). The participation and contributions received throughout the consultation process have been instrumental in shaping a comprehensive and forward-looking cyber security strategy for Sarawak.

The development of SCSR 2030 was informed through a series of stakeholder engagements, workshops, consultations, discussions, feedback sessions, review exercises and validation activities involving representatives from government agencies, statutory bodies, government-linked companies, academia, industry associations and private sector organisations. The contributions received throughout this process have been invaluable in ensuring that SCSR 2030 reflects Sarawak's cyber security priorities, operational realities, emerging cyber threats, digital transformation objectives and long-term cyber resilience aspirations.

SMA extends its appreciation to the following participating agencies for their valuable input, cooperation and constructive feedback:

Premier's Departments of Sarawak

Sarawak Civil Service Digitalisation Unit (SCSDU)

Sarawak Security and Enforcement Unit (UKPS)

Office of the Chief Government Security Officer (CGSO) Sarawak

Ministries

Ministry of Utility and Telecommunication Sarawak

Ministry of Public Health, Housing and Local Government Sarawak

Ministry of Infrastructure and Port Development Sarawak

Ministry of Youth, Sports and Entrepreneur Development Sarawak

Ministry of Natural Resources and Urban Development Sarawak

Ministry of Food Industry, Commodity and Regional Development Sarawak

Ministry of Education, Innovation and Talent Development Sarawak

Ministry of Transport Sarawak

Ministry of Energy and Environmental Sustainability Sarawak

State Departments

State Financial Secretary's Office

Department of Agriculture Sarawak

Department of Rural Water Supply Sarawak

Statutory Bodies

Sarawak Biodiversity Centre

Kuching Port Authority

Rajang Port Authority

Samalaju Port Authority

Government Link Companies and State-Owned Enterprises

Sarawak Forestry Corporation

Sarawak Economic Development Corporation (SEDC)

Bintulu Port Holdings Berhad

Petroleum Sarawak Berhad (PETROS)

Sarawak Energy Berhad

Sarawak Water Sdn. Bhd.

Sarawak Information Systems Sdn. Bhd. (SAINS)

Sarawak Digital Economy Corporation Berhad (SDEC)

Sarawak Metro Sdn. Bhd.

Sarawak Artificial Intelligence Centre Sdn. Bhd. (SAIC)

Development Bank of Sarawak Berhad (DBOS)

SACOFA Sdn. Bhd.

Academic Institutions

Swinburne University of Technology Sarawak

i-CATS University College

Curtin University Malaysia

Industry Associations and Private Sector Organisations

SiliconNet Technologies Sdn. Bhd.

IRIX Sdn. Bhd.

Kuching Blockchain Technology Association (KBTA)

Associated Chinese Chambers of Commerce and Industry of Sarawak (ACCCIS)

Sarawak ICT Association (SICTA)

SME Association of Sarawak

Appendix 2 | The Initiatives

Initiative 1

Identification and Prioritisation of Sarawak's Strategic Information Assets (SIA)

Summary:

Initiative 1 establishes a State-level SIA identification framework by Year 1 and a consolidated inventory by Year 2, enabling Sarawak to prioritise protection of its most critical digital assets.

Objective:

Prioritise strategic digital assets

To establish a consistent State-level process to identify, assess and prioritise digital infrastructure that is critical to Sarawak's Government, essential services and economy.

Description:

Prioritise Strategic Information Assets

Sarawak relies on digital systems across Government, energy, utilities, transport, healthcare, communications and other essential services. While the Federal Cyber Security Act 2024 provides the national framework for identifying and designating National Critical Information Infrastructure (NCII), Sarawak requires a systematic State-level view of the digital assets and dependencies that are critical to its own operations and service delivery.

This initiative establishes a State-level identification and prioritisation process aligned with the Federal NCII framework without creating regulatory duplication. It will identify systems that may not meet Federal NCII thresholds, while maintaining a broader State inventory of digital assets that are critical to Sarawak's operations and essential services.

The resulting inventory will provide a common evidence base for prioritising cyber security investment, applying appropriate protection measures and coordinating resilience activities under subsequent SCSR initiatives. The process will be periodically reviewed as services, technologies, dependencies and threats evolve. A State-level framework to identify and classify critical information infrastructure in Sarawak, complementing Federal NCII requirements while addressing systems critical to State operations and service delivery.

Output:

Establish SIA Inventory

- State SIA identification and prioritisation methodology established by Year 1.
- Consolidated inventory of Sarawak's Strategic Information Asset established by Year 2.
- Critical dependencies and service impacts documented for priority State's SIA
- Annual SIA inventory and criticality review established from Year 3 onwards.

Outcome:

Strategic Assets Protected

Sarawak has a clear, current view of the digital infrastructure most critical to its essential services and economy, enabling the State and asset owners to prioritise cyber security investment and protection where disruption would have the greatest impact.

Value:

Prioritised Cyber Security Investment

State resources can be focused on protecting the systems that matter most, reducing the risk that a cyber incident disrupts essential services, Government operations or economic activity.

Initiative 2

Sarawak SIA Cyber Security Baseline and Maturity Assessment

Summary:

Initiative 2 establishes a common SIA cyber security baseline and maturity assessment by Year 1, enabling priority entities to identify gaps and strengthen cyber security readiness from Year 2 onwards.

Objective:

Standardised Cyber Security Baseline

To establish a consistent, risk-based baseline and maturity assessment approach that enables Sarawak's strategic information asset owners to understand their cyber security readiness, identify gaps and progressively strengthen protection in line with applicable Federal requirements and State priorities.

Description:

SIA Cyber Security Maturity Framework

Sarawak's SIA operators currently have varying levels of cyber security capability and maturity. While designated NCII entities are subject to Federal cyber security requirements, other systems critical to Sarawak's services and economy may not have a common reference point for assessing their cyber security readiness.

This initiative establishes a State SIA cyber security baseline and maturity assessment approach aligned with NACSA's Cyber Security Act 2024 Code of Practice and other applicable national standards. It provides a common reference point for assessing cyber security readiness, identifying gaps and developing prioritised improvement plans.

The framework will be applied proportionately according to the criticality, risk and regulatory status of each entity. For entities already subject to Federal requirements, the State framework will complement rather than duplicate statutory obligations. For other State-critical entities, it will provide a practical pathway to progressively improve cyber security readiness.

Output:

Deploy Assessment Framework

- Sarawak SIA Cyber Security Baseline established by Year 1.
- SIA maturity assessment toolkit developed and deployed by Year 1.
- Priority SIA entities assessed against the baseline by Year 2.
- Entity-level improvement plans established for identified material gaps by Year 2.
- Periodic State-level SIA cyber security readiness report established by Year 3.

Outcome:

SIA Security Readiness Strengthened

Sarawak SIA owners have a consistent understanding of their cyber security readiness and progressively address priority gaps, resulting in stronger and more consistent protection of services that are essential to Sarawak.

Value:

More Consistent Service Protection

The State can identify and reduce common cyber security weaknesses before they cause disruption, improving the reliability of essential services and reducing the potential economic and social impact of cyber incidents.

Initiative 3

SIA Cyber Security Implementation Guidance and Best Practices

Summary:

Initiative 3 provides practical implementation guidance from Year 1, with sector-specific playbooks from Year 2 to help SIA owners strengthen protection and address cyber security gaps.

Objective:

Practical Cyber Security Guidance

To provide practical, sector-relevant cyber security guidance that enables SIA owners to implement the State baseline, address identified weaknesses and embed security into the design and operation of critical digital systems.

Output:

Develop Sector Guidance

- State SIA cyber security implementation guidance established and aligned with applicable Federal requirements from Year 1 onwards.
- Priority sector-specific cyber security playbooks developed from Year 2 onwards.
- Security-by-design reference architectures and implementation guidance established from Year 3 onwards.
- Guidance piloted with priority SIA entities and refined based on operational feedback.
- Technical advisory and implementation support mechanism established.
- Guidance reviewed and updated periodically to reflect changing technologies and threats.

Description:

Translate Baseline into Practice

The State cyber security baseline provides a common reference point for SIA cyber security readiness, but SIA owners may require practical guidance on how to apply those expectations within their specific operational and technical environments.

This initiative translates the baseline into practical, risk-based implementation guidance, reference architectures and sector-specific playbooks covering priority areas such as identity and access management, data protection, network and application security, monitoring, incident response and recovery. Guidance will also address security-by-design for new digital systems and emerging technologies such as AI and Post-Quantum Cryptography (PQC) where relevant.

The guidance will complement, rather than replace, Federal cyber security requirements and recognised national and international standards. It will focus on the practical needs of Sarawak's SIA ecosystem, particularly State-critical entities that are not subject to detailed Federal technical requirements.

Outcome:

SIA Cyber Protection Strengthened

Sarawak SIA owners are better able to implement effective cyber security measures and address priority weaknesses, resulting in more consistent protection of the digital systems that support Sarawak's essential services.

Value:

Essential Services Better Protected

SIA organisations have clearer and more practical ways to strengthen their systems, reducing avoidable weaknesses and the risk of disruption to essential services.

Initiative 4

State Cyber Resilience Exercises and Preparedness

Summary:

Initiative 4 establishes a State cyber resilience exercise framework by Year 2, with regular sector and State-wide exercises from Year 3 to strengthen incident preparedness, response and recovery.

Objective:

Cyber Resilience Testing

To regularly test and strengthen the ability of Sarawak's Government and strategic information asset operators to withstand, respond to and recover from significant cyber incidents.

Description:

Cyber Resilience Preparedness

Cyber security controls and incident response plans cannot be assumed to work effectively without being tested. This initiative establishes a structured, recurring programme of cyber exercises and resilience testing for Sarawak's Government and SIA ecosystem.

The programme will progressively test leadership decision-making, incident response, technical recovery, cross-agency coordination, communications, third-party dependencies and continuity of essential services. Exercises will range from tabletop simulations to sector-specific technical stress tests and State-wide cyber crisis exercises.

Each exercise will produce an after-action review identifying weaknesses, assigning remediation actions and tracking improvements through subsequent exercises and maturity assessments. The programme will therefore create a continuous cycle of test → learn → improve → retest.

Output:

Establish Exercise Programme

- State Cyber Resilience Exercise Framework established by Year 2.
- CyberSarawak's Stay Ready programme piloted with priority SIA sectors by Year 3.
- Annual State-wide cyber crisis exercise institutionalised by Year 3.
- Sector-specific cyber stress-testing programme established.
- After-action review and remediation tracking mechanism established.
- Priority SIA entities progressively participate in resilience exercises on a defined cycle.

Outcome:

Cyber Resilience Strenghthen

Sarawak's Government and critical infrastructure operators are better prepared to withstand and recover from major cyber incidents, with tested response arrangements, clearer cross-sector coordination and critical weaknesses identified and addressed before they cause real-world disruption.

Value:

Reduce Service Disruption

Regular testing reduces the risk of prolonged disruption when a major cyber incident occurs, helping keep essential services operating and enabling faster recovery when disruption cannot be avoided.

Initiative 5

Cyber Hygiene Adoption for Sarawak Businesses

Summary:

Initiative 5 establishes a business cyber hygiene baseline by Year 2 and expands guidance and support from Year 3 onwards, helping Sarawak businesses, especially MSMEs, adopt safer digital practices and reduce cyber risks.

Objective:

Business Cyber Hygiene Adoption

To accelerate the adoption of essential cyber security practices among Sarawak businesses, particularly MSMEs, by embedding practical cyber hygiene into existing business digitalisation and support programmes.

Output:

Expand Business Support

- Sarawak Business Cyber Hygiene Baseline established by Year 2.
- Cyber hygiene resources integrated into relevant digitalisation programmes by Year 3.
- StaySmart Business Champion network established and progressively expanded by Year 3.
- District-level business cyber hygiene support available across Sarawak by Year 4.
- Business self-assessment and adoption tracking mechanism operational.
- Progressive increase in adoption of essential cyber hygiene practices among participating businesses.

Description:

Embed Essential Cyber Practices

As more Sarawak businesses adopt digital platforms, online transactions and cloud-based services, basic cyber security practices become essential to protecting business operations, customer information and digital transactions. However, many MSMEs have limited cyber security expertise, resources and time to implement security measures independently.

This initiative will embed practical cyber security hygiene into existing Sarawak business digitalisation and support programmes rather than creating a separate delivery channel. Businesses will be provided with simple, actionable guidance covering areas such as account protection, multi-factor authentication, software updates, device protection, data backup, phishing awareness and incident reporting.

The programme will leverage existing business digitalisation initiatives, community technical outreach programme, industry associations and local business networks to reach businesses across Sarawak, including those outside the major urban centres. Appointed “StaySmart Business Champions” will provide peer-level support and encourage sustained adoption.

The initiative complements Federal cyber security programmes by focusing on localised delivery, adoption and follow-through, particularly among Sarawak MSMEs that may otherwise have limited access to cyber security support.

Outcome:

Safer Digital Businesses

Sarawak businesses, particularly MSMEs, adopt safer digital practices as a normal part of their digital operations, reducing avoidable cyber risks and strengthening confidence in the State’s digital economy.

Value:

Stronger Digital Economy Confidence

Businesses become better able to protect their operations, customer information and digital transactions without requiring every MSME to build its own cyber security capability, supporting safer and more inclusive digitalisation across Sarawak.

Initiative 6

Tailored Cyber Security Awareness and Digital Resilience for Sarawak Communities

Summary:

Initiative 6 launches a statewide cyber security awareness and digital resilience programme from Year 1, with tailored community initiatives expanding from Year 2 onwards to promote safer digital behaviours and strengthen resilience across Sarawak.

Objective:

Strengthen Digital Resilience

To strengthen safe digital behaviour across Sarawak by delivering locally relevant, culturally appropriate and accessible cyber security awareness and digital resilience programmes for communities with different needs, vulnerabilities and levels of digital literacy.

Output:

Expand Community Programmes

- Sarawak Community Cyber security Awareness Framework established by Year 1.
- Tailored modules developed for priority community segments from Year 2 onwards.
- StaySmart Ambassador Network expanded across all Sarawak divisions.
- Localised and accessible cyber security materials made available from Year 2 onwards.
- Community cyber security programmes delivered across Sarawak from Year 3.
- Community cyber volunteer/ champion network established from Year 3.
- Annual awareness and behavioural assessment conducted from Year 3.

Description:

Community Cyber Resilience

Sarawak's communities have diverse levels of digital access, literacy, language, age, location and exposure to cyber risks. National cyber security awareness programmes provide an important foundation, but a one-size-fits-all approach may not effectively reach rural communities, indigenous populations, elderly citizens, youth and other groups with different digital behaviours and vulnerabilities.

This initiative establishes a statewide, community-led cyber security awareness and digital resilience programme that localises and extends national cyber security guidance for Sarawak's communities. Content will be adapted to local circumstances, languages and community needs and delivered through trusted local institutions and networks.

The programme will build on the existing CyberSarawak "StaySmart" initiative and expand its network of trained ambassadors across Sarawak's divisions. Delivery will leverage existing channels including Digital Community Centres, Digital Villages, schools, district offices, community organisations and other trusted local channels. Community ambassadors will act as first-line sources of practical cyber security guidance and direct individuals to appropriate support or Federal channels when specialised assistance is required.

The programme will focus on practical behaviours such as protecting accounts, recognising scams and phishing, safeguarding personal information, using devices safely, managing online risks and knowing where to seek help. It will complement national awareness programmes by providing the local reach and community-level engagement needed to turn cyber security awareness into safer everyday digital behaviour.

Outcome:

Improve Safe Digital Behaviour

People across Sarawak, particularly vulnerable and underserved communities, demonstrate safer digital behaviours and are better able to recognise, avoid and respond to common cyber risks, enabling more confident participation in the digital economy.

Value:

Reduce Digital Harm

A more cyber-aware population reduces avoidable digital harm, strengthens public confidence in online services and enables more Sarawakians—including those in rural and underserved communities—to participate safely in the digital economy.

Initiative 7

Sarawak Scam Prevention and Victim Support

Summary:

Initiative 7 establishes a Sarawak scam prevention and victim-support framework by Year 2, providing localised advisories, reporting and referral pathways to help citizens and businesses recognise scams earlier, reduce losses and access timely support.

Objective:

Scam Risk Reduction

To reduce the impact of scams on Sarawak's citizens and businesses through localised prevention, early advisory support, accessible reporting and referral pathways, and coordinated victim support that complements Federal scam-response mechanisms.

Output:

Establish Support Network

- Sarawak scam prevention and victim-support framework established by Year 2.
- Statewide scam reporting and referral pathway operational by Year 2.
- Local scam advisory support available across all Sarawak divisions by Year 2.
- StaySmart/community network enabled to provide first-line scam guidance.
- Targeted scam prevention advisories and campaigns delivered based on relevant Federal and State intelligence from Year 2.
- Structured post-incident support available to victims requiring follow-up assistance from Year 3.
- Annual Sarawak Scam Impact and Trend Assessment established from Year 3.

Description:

Strengthen Scam Support

Scams increasingly affect Sarawak's citizens and businesses, causing financial loss, emotional distress and reduced confidence in digital transactions. While national scam intelligence, investigation, enforcement and disruption are led through Federal mechanisms such as the National Scam Response Centre (NSRC) and PDRM, victims often require immediate local advice and assistance to understand what to do, where to report and how to reduce further harm.

This initiative establishes a Sarawak-level scam prevention and victim-support network that complements Federal mechanisms by bringing timely, locally relevant advice and assistance closer to communities. It will use intelligence and scam trends made available through Federal channels to inform targeted prevention campaigns and local advisories, without creating a parallel intelligence or investigation function.

Accessible support will be delivered through existing State and community networks, including StaySmart ambassadors, divisional and district channels, SDEC digitalisation networks and other trusted community organisations. The programme will provide early guidance, referral to the appropriate Federal authorities and financial institutions, and structured post-incident support for victims.

The programme will also identify scam patterns and community vulnerabilities affecting Sarawak and use these insights to continuously improve local prevention and awareness activities.

Outcome:

Improve Scam Response

Citizens and businesses in Sarawak are better able to recognise, avoid and respond to scams, with victims receiving timely local guidance and effective referral to the appropriate Federal and industry support mechanisms.

Value:

Reduce Losses and Harm

Earlier local advice and easier access to the right support reduce avoidable losses and harm from scams, strengthen public confidence in digital transactions, and ensure Sarawak communities benefit fully from national scam-response capabilities.

Initiative 8

Sarawak Cyber Security Readiness and Recognition Programme

Summary:

Initiative 8 develops a cyber security readiness and recognition pathway by Year 2, enabling Sarawak businesses to assess, improve and demonstrate their cyber security readiness against recognised standards.

Objective:

Cyber-Ready Businesses

To provide Sarawak businesses with a practical pathway to assess, improve and demonstrate their cyber security readiness, while complementing Federal and internationally recognised cyber security standards and certification schemes.

Output:

Establish Recognition Programme

- Sarawak Business Cyber security Readiness Baseline established by Year 2.
- Online business cyber readiness self-assessment tool operational by Year 2.
- Tiered readiness and recognition programme launched by Year 3.
- Independent assessment pathway established for higher-risk businesses.
- State recognition mechanism and business incentives established by Year 4.
- Progressive adoption across MSMEs, State-linked companies and relevant supply-chain businesses.

Description:

Build Readiness Pathway

Many businesses, particularly MSMEs, lack the resources or expertise to determine whether their cyber security practices are adequate. At the same time, formal international certifications may be disproportionate to the needs and resources of smaller businesses.

This initiative establishes a progressive Sarawak Cyber Security Readiness and Recognition Pathway that enables businesses to start with a simple self-assessment and progressively strengthen their cyber security posture. The programme will provide a practical baseline aligned with relevant Federal requirements and recognised standards, while allowing businesses to progress towards independently assessed national or international certifications where appropriate.

The programme will be integrated into Sarawak's business digitalisation ecosystem so that cyber security readiness becomes part of the process of becoming digitally enabled. Incentives such as recognition, access to selected State programmes and, where appropriate, procurement preferences may be considered to encourage adoption.

The programme will complement rather than replace Federal certification and regulatory schemes. Where an existing national or internationally recognised certification adequately meets a business's needs, the Sarawak programme should recognise or provide a pathway towards that certification rather than creating another competing certification requirement.

Outcome:

Strengthen Business Cyber Resilience

Sarawak businesses have a clear and credible pathway to improve and demonstrate cyber security readiness, resulting in stronger protection of digital operations and greater trust in Sarawak's digital business environment.

Value:

Enable Progressive Cyber Improvement

Businesses can progressively strengthen cyber security according to their size and risk without facing the cost or complexity of full certification at the outset, while Sarawak gains a more trusted and resilient digital business ecosystem.

Initiative 9

Cyber Security Career Pathway and Youth Talent Development

Summary:

Initiative 9 develops a structured cyber security career pathway for Sarawak youths, connecting education, industry experience and employment opportunities to build a sustainable local talent pipeline.

Objective:

Build Youth Talent Pipeline

To build Sarawak's future cyber security talent pipeline by increasing youth interest in cyber security careers and providing structured pathways from school exposure to cyber security education, industry experience and employment.

Output:

- Sarawak Cyber Security Youth Talent Working Group established in Year 2.
- Baseline assessment of cyber security education, enrolment and graduate pathways completed by Year 2.
- Sarawak Cyber Security Career Pathway developed and maintained.
- Cyber security career exposure programme delivered through schools and TVET institutions by Year 3.
- Annual Sarawak Cyber Youth Challenge established by Year 3.
- Industry mentorship and internship network established by Year 4.
- Participating universities/ TVET institutions and industry partners connected through structured pathways.
- Youth talent tracking mechanism established to monitor progression into cyber security education, internships and employment.

Description:

Create Cyber Career Pathways

Sarawak's growing digital economy will require a sustainable pipeline of cyber security professionals across Government, critical infrastructure, businesses and the emerging local cyber security industry. Limited early exposure to cyber security has been identified during the development of this Strategy as one factor contributing to low enrolment in cyber security-related programmes and the subsequent loss of graduates to opportunities outside Sarawak.

This initiative establishes a structured youth cyber security career pathway that connects school-level exposure, TVET and higher education, industry engagement and employment opportunities. It will build on the community and school outreach mechanisms developed under Pillar 2, while focusing specifically on converting interest into sustained education and career choices.

Existing established platforms will be used as key delivery channels, while MEITD, schools, universities, TVET institutions, and industry partners provide education, mentoring, internships, competitions and employment pathways. The programme will also leverage cyber security professionals and industry practitioners as role models and mentors.

The initiative will complement national cyber security awareness and youth programmes by focusing on the State-specific talent pipeline, including the skills and employment opportunities required by Sarawak's Government, SIA sectors, GLCs and growing digital economy.

Outcome:

Grow Local Cyber Talent

More Sarawak youths choose and successfully progress through cyber security education and industry pathways, resulting in a stronger pipeline of locally trained cyber security talent available to support Sarawak's digital economy.

Value:

Reduce External Talent Dependence

A stronger local cyber security talent pipeline reduces long-term dependence on external expertise, creates higher-value career opportunities for Sarawak youths and provides the skilled workforce needed to sustain the State's digital economy.

Initiative 10

Sarawak Cyber Security Workforce Demand and Skills Alignment

Summary:

Initiative 10 aligns cyber security education and training with Sarawak's workforce needs through Government, industry and academia collaboration.

Objective:

Align Workforce Skills

To align cyber security education, training and workforce development with the current and future cyber security skills required by Sarawak's Government, critical sectors and digital economy.

Output:

Establish Workforce Alignment

- Sarawak Cyber Security Workforce Advisory Panel established Year 1.
- Sarawak Cyber Security workforce demand baseline established.
- Priority sector cyber security roles and skills identified.
- Education and training gap assessment completed.
- Annual Sarawak Cyber Security Workforce Demand and Capability Outlook published by Year 2.
- Industry-linked internship and placement pathways established.

Description:

Match Skills to Demand

Sarawak's cyber security workforce must grow in step with the State's digital transformation and the changing needs of Government, critical infrastructure operators and businesses. While national cyber security competency and training programmes provide an important foundation, education and training providers require visibility of the specific roles, skills and emerging capabilities demanded by Sarawak's employers.

This initiative establishes a structured Government-Industry-Academia mechanism to identify Sarawak's cyber security workforce needs and translate those needs into practical education, training and employment pathways. It will map priority cyber security roles, identify current and emerging skills gaps, provide demand signals to universities and TVET institutions, and facilitate industry placements aligned with actual workforce requirements.

The initiative will complement national competency and training programmes rather than create a separate national framework. Where suitable national competency frameworks or certifications exist, Sarawak will adopt and localise them to reflect State-specific sector requirements.

Outcome:

Improve Talent Readiness

Cyber security education and training in Sarawak increasingly matches the skills demanded by employers, resulting in a stronger flow of suitably skilled talent into cyber security roles within the State.

Value:

Reduce Skills Gaps

Sarawak invests in cyber security skills that its economy actually needs, reducing skills shortages, improving employment opportunities for local graduates and reducing dependence on external cyber security expertise.

Initiative 11

Cyber Security Leadership and Governance Capability

Summary:

Initiative 11 strengthens cyber security leadership and governance by equipping boards and senior leaders to better manage cyber risk, investment and accountability.

Objective:

Strengthen Cyber Leadership

To strengthen the ability of boards, senior executives and business leaders in Sarawak to understand, govern and make informed decisions about cyber security risk as a strategic business and organisational responsibility.

Output:

Establish Leadership Programmes

- Board and Executive Cyber Security Governance Guide established by Year 3.
- Executive cyber security module integrated into relevant leadership programmes by Year 3.
- Board and senior-management cyber governance sessions delivered annually starting from Year 4.
- Sarawak Cyber Leadership Forum established by Year 4.
- Participating organisations develop or strengthen board-level cyber risk oversight arrangements.

Description:

Build Governance Capability

Cyber security is increasingly a business and organisational risk rather than solely a technical issue. Boards and senior management influence investment decisions, risk appetite, business continuity and organisational accountability, yet cyber security responsibilities are often delegated primarily to technical teams.

This initiative develops cyber security leadership capability among boards, senior executives and management of State-linked companies, SIA entities and other priority businesses. It will focus on practical decision-making rather than technical training, covering cyber risk oversight, investment prioritisation, incident accountability, regulatory responsibilities, business continuity and emerging cyber risks.

Delivery will be integrated into existing leadership and business-development platforms rather than creating a separate executive training institution.

Outcome:

Stronger Cyber Security Governance

Boards and senior leaders increasingly treat cyber security as a strategic business risk, resulting in stronger oversight, better-informed investment decisions and clearer accountability for cyber resilience.

Value:

Strengthen Organisational Resilience

Stronger leadership decisions reduce the likelihood that cyber security risks are underfunded or overlooked, improving organisational resilience and protecting the continuity and reputation of Sarawak's businesses and critical services..

Initiative 12

Cyber Security Professional Development and Certification

Summary:

Initiative 12 strengthens Sarawak's cyber security workforce by improving access to recognised professional training, certification and career development opportunities.

Objective:

Develop Certified Professionals

To increase the number and quality of cyber security professionals in Sarawak by improving access to recognised certifications, targeted professional development and career progression opportunities.

Output:

Expand Certification Pathways

- Priority cyber security certification pathways identified by Year 2.
- Certification sponsorship and incentive programme established by Year 3.
- Partnerships with recognised training and certification providers established.
- Professional certification programmes delivered through accredited providers.
- Industry co-funding mechanism progressively established.
- Sarawak Cyber Security Professional Directory established, where appropriate by Year 2.

Description:

Strengthen Professional Development

Sarawak's cyber security workforce requires a sustained pathway for professionals to develop and maintain recognised skills as cyber threats and technologies evolve. The cost and accessibility of professional training and certification can be a barrier, particularly for individuals and smaller organisations.

This initiative establishes a structured professional development programme that improves access to recognised cyber security training and certifications through sponsorship, incentives and partnerships with accredited training providers. Priority certifications will be selected based on the cyber security roles and skills identified through Initiative 10.

The programme will use existing accredited providers as delivery platforms and encourage industry co-investment over time. Rather than creating a separate State certification regime, Sarawak will recognise and support appropriate national and internationally recognised qualifications.

A professional directory may be established to improve visibility of qualified cyber security practitioners and service providers operating in Sarawak, subject to alignment with Federal licensing and professional requirements.

Outcome:

Grow Skilled Cyber Workforce

More cyber security professionals in Sarawak possess recognised and relevant skills, strengthening the availability and quality of local cyber security expertise to support Government, critical sectors and businesses.

Value:

Reduce External Dependence

A larger pool of recognised cyber security professionals reduces reliance on external expertise, improves access to skilled local services and creates higher-value career opportunities within Sarawak.

Initiative 13

Emerging Technologies Adoption for Advanced Cyber Threats Protection

Summary:

Initiative 13 strengthens Sarawak's cyber resilience by accelerating the secure adoption of AI and emerging technologies through local talent, innovation and practical cyber security solutions.

Objective:

Enable Secure Technology Adoption

Develop a future-ready cyber ecosystem by building local talent, strengthening home-grown capabilities, and accelerating the secure adoption of artificial intelligence and other emerging technologies to enhance Sarawak's cyber resilience

Output:

Establish Innovation Lab

- Sarawak Cyber Security Innovation and Emerging Technology Lab established and operational by Year 3.
- State AI and Emerging Technology Cyber security Roadmap developed by Year 2.
- Practical guidance, reference architectures and best practice frameworks published for emerging technology adoption including AI and PQC.

Description:

Build Future-Ready Cyber Capabilities

The rapid advancement of artificial intelligence (AI) and other emerging technologies is transforming both the opportunities and risks within Sarawak's digital ecosystem. As AI becomes increasingly embedded across Government, critical infrastructure and industry, cyber threats are expected to become more sophisticated, automated and difficult to detect. At the same time, evolving technologies, cloud-native platforms, quantum-resistant cryptography and autonomous systems require new cyber security capabilities that are not yet widely available within the State.

This initiative aims to develop a future-ready cyber security ecosystem by strengthening local expertise, accelerating innovation and enabling the secure adoption of AI and other emerging technologies. Through collaboration among Government, industry, academia and technology partners, Sarawak will establish an environment that supports research, skills development, solution testing and the responsible adoption of emerging cyber security technologies.

The initiative will establish a Cyber security Innovation and Emerging Technology Lab as a shared platform to evaluate, prototype and validate cyber security solutions before deployment. Priority areas include AI-enabled cyber defence, secure AI governance, post-quantum cryptography, cloud-native security and other emerging technologies relevant to Sarawak's digital transformation. Successful innovations will be translated into practical guidance, operational capabilities and scalable solutions that strengthen the cyber security resilience of Government, critical infrastructure and businesses.

Outcome:

Strengthen Emerging Technology Readiness

Sarawak develops the capability to securely adopt artificial intelligence and other emerging technologies through a skilled local workforce, stronger home-grown innovation and trusted cyber security practices, enabling a more resilient, competitive and future-ready digital economy.

Value:

Accelerate Secure Innovation

Sarawak can adopt AI and other emerging technologies with greater confidence, build local high-value capability and avoid falling behind as the technology landscape changes.

Initiative 14

Institutionalising Whole-of-Sarawak Cyber Security Governance

Summary:

Initiative 14 establishes a Whole-of-Sarawak cyber security governance framework by Year 1, enabling clearer accountability, coordinated decision-making and more consistent cyber security implementation across Government.

Objective:

Unified Cyber Governance

To establish a Whole-of-Sarawak Cyber Security governance framework that enables coordinated decision-making, clear accountability, and consistent implementation across Government and strategic stakeholders.

Output:

Establish Governance Framework

- Whole-of-Sarawak Cyber Security Governance Framework formally adopted by Year 1.
- Sarawak Cyber Security Operating Model implemented across participating agencies by Year 2.
- Government Orders, procurement requirements and supporting policy instruments operational by Year 3.
- Annual Whole-of-Sarawak cyber security governance review institutionalised from Year 4 onwards.
- All core cyber security functions assigned with clear agency ownership and accountability.

Description:

Institutionalise Statewide Governance

Effective cyber security requires more than technical controls—it requires clear leadership, defined responsibilities and coordinated decision-making across Government. As Sarawak's digital ecosystem continues to expand, cyber security responsibilities are shared across multiple agencies and organisations. Without a common governance framework, efforts may become fragmented, inconsistent and difficult to sustain.

This initiative establishes a Whole-of-Sarawak cyber security governance framework that defines roles, responsibilities, decision-making processes and accountability across Government agencies and key stakeholders. It institutionalises cyber security requirements through Government Orders, procurement policies and other administrative instruments.

The initiative also establishes regular performance reviews, cross-agency coordination mechanisms and continuous governance improvement to ensure cyber security remains aligned with Sarawak's digital transformation priorities and evolving cyber risk landscape.

Outcome:

Improve Coordinated Implementation

Government agencies work together under a coordinated governance framework with clear accountability, resulting in more consistent cyber security implementation, better resource utilisation and stronger protection of Sarawak's digital services.

Value:

Enhance Accountability and Efficiency

A coordinated Whole-of-Sarawak governance model enables faster decision-making, reduces duplication of effort, improves accountability and ensures public investments in cyber security deliver greater value and impact for Sarawak.

Initiative 15

Establishing a Centralised State Cyber Security Operations and Coordination Capability

Summary:

Initiative 15 establishes a centralised State cyber security operations and coordination capability by Year 1, enabling faster threat detection, incident coordination and response across Government and participating critical sectors.

Objective:

Integrated Cyber Defence

To establish and operationalise a dedicated central operational cyber security centre for monitoring, incident coordination, threat-informed defence and cyber security advisory services, providing coordinated support to State Government and participating critical sectors while complementing Federal cyber security capabilities.

Output:

Establish Cyber Security Centre

- A centralised Cyber Security Centre is established by Year 1.
- Core cyber security services operational and serving State government entities by Year 2.
- Core cyber security services extended to serve Sarawak entities beyond State Government, including SIA operators and businesses by Year 3.

Description:

Coordinate Cyber Security Services

A dedicated cyber security centre that serve as Sarawak's central operational cyber security capability, providing coordinated monitoring, threat detection, incident coordination, cyber security advisory and situational awareness services for State Government and participating critical sectors. It will consolidate operational capabilities that are currently fragmented across different organisations and establish a common point of coordination for significant cyber incidents affecting the State.

The centre will operate as a trusted, non-punitive cyber security service and coordination capability, separate from regulatory and law-enforcement functions. It will work closely with NACSA, NC4, MyCERT, PDRM and other Federal agencies where national coordination, regulatory action or law enforcement is required.

The centre will progressively extend its services from State Government to participating SIA entities and other priority organisations, based on risk, readiness and available capacity. This approach enables Sarawak to build a practical State-level operational capability while leveraging national cyber security mechanisms and avoiding duplication of Federal functions.

Outcome:

Improve Incident Response

Government and participating critical sectors are able to detect, coordinate and respond to cyber threats more quickly and consistently, reducing disruption to essential digital services and strengthening Sarawak's overall cyber resilience.

Value:

Strengthen State Cyber Resilience

Sarawak acquires a centralised operational capability that reduces fragmented cyber security response, limits the impact and duration of cyber incidents, and helps keep essential Government and critical services available to the people and economy of Sarawak.

Initiative 16

Strategic Cyber Security Partnerships and Collaboration

Summary:

Initiative 16 strengthens Sarawak's cyber security ecosystem through strategic partnerships with Federal agencies, industry, academia and international organisations.

Objective:

Build Strategic Partnerships

To establish strategic partnerships that strengthen Sarawak's cyber security ecosystem maturity through collaboration, knowledge exchange, innovation and shared expertise while complementing national and international cyber security initiatives.

Output:

Establish Partnership Framework

- State Cyber Security Partnership Framework established by Year 2.
- Strategic partnership agreements established with priority Federal, industry, academic and international organisations by Year 2.
- Joint research, innovation or policy projects established by Year 4.
- Sarawak represented in selected regional cyber security collaborations by Year 3.

Description:

Strengthen Collaborative Ecosystem

Cyber security is a shared responsibility that extends beyond organisational and geographical boundaries. As cyber threats continue to evolve, Sarawak must remain connected to national, regional and international cyber security ecosystems to access emerging knowledge, best practices, innovation and strategic partnerships.

This initiative establishes a structured partnership framework that enables Sarawak to collaborate effectively with Federal agencies, industry, academia and selected international organisations. Rather than duplicating national initiatives, Sarawak will leverage existing national and international programmes wherever they provide sufficient value, while establishing complementary State partnerships where local priorities require faster implementation or greater operational focus.

The initiative also promotes collaboration in cyber security research, innovation, policy development, technology evaluation and professional exchanges that directly support Sarawak's digital transformation priorities. Through these partnerships, Sarawak contributes practical experience and innovation back to the wider cyber security community while strengthening its own resilience and credibility as a trusted digital economy.

Outcome:

Expand Trusted Collaboration

Sarawak becomes a trusted and well-connected cyber security partner, enabling faster access to expertise, innovation and collaborative opportunities that strengthen the State's cyber resilience and digital economy.

Value:

Accelerate Cyber Maturity

Strategic partnerships enable Sarawak to leverage external expertise, innovation and resources, reducing duplication of effort while accelerating cyber security maturity and strengthening investor confidence in Sarawak's digital ecosystem.

Initiative 17

State Cyber Threat Intelligence Coordination and Operationalisation

Summary:

Initiative 17 establishes a State-level cyber threat intelligence capability to coordinate, contextualise and share actionable threat intelligence across Sarawak.

Objective:

Coordinate Threat Intelligence

To establish a trusted State-level cyber threat intelligence coordination capability that enables Sarawak to receive, contextualise, share and act upon relevant cyber threat intelligence in collaboration with Federal agencies and trusted partners.

Output:

Establish Intelligence Mechanisms

- Formal Intelligence-sharing arrangements established by Year 2.
- Secure Intelligence-sharing platform operational by Year 2.
- Periodic cyber threat advisories issued by Year 3.
- Participating Government agencies and priority SIA operators receive actionable threat intelligence by Year 3.
- Annual Sarawak Cyber Threat Landscape Report published by Year 3.

Description:

Operationalise Threat Intelligence

Effective cyber defence depends on timely access to relevant and actionable threat intelligence. While Federal agencies such as NACSA, NC4 and MyCERT maintain national cyber threat intelligence capabilities, Sarawak requires a State-level coordination mechanism to ensure that intelligence is contextualised and translated into practical guidance for Government agencies, critical information infrastructure operators and other stakeholders.

This initiative employs a dedicated centralised operation centre as the State's trusted cyber threat intelligence coordination hub. Working closely with Federal agencies and trusted regional partners, the centre will receive relevant threat intelligence, enrich it with State-level operational context, disseminate timely advisories and indicators of compromise, and coordinate protective actions across the Sarawak cyber security ecosystem.

The initiative also establishes governance arrangements, secure information-sharing mechanisms and standard operating procedures that enable trusted collaboration while respecting national ownership of intelligence and existing Federal responsibilities.

Outcome:

Improve Threat Preparedness

Government agencies and critical infrastructure operators are able to anticipate, prepare for and respond more effectively to cyber threats through timely access to trusted and actionable cyber threat intelligence.

Value:

Enable Early Preventive Action

Earlier awareness of emerging cyber threats enables Government and critical sectors to take timely preventive action, reducing disruptions to essential services while strengthening public confidence in Sarawak's digital ecosystem.

Initiative 18

Collaborative Cybercrime Prevention and Response

Summary:

Initiative 18 strengthens Sarawak's cybercrime resilience through coordinated prevention, reporting, victim support and collaboration with Federal law enforcement agencies.

Objective:

Strengthen Cybercrime Resilience

To strengthen Sarawak's resilience against cybercrime through coordinated prevention, timely information sharing, victim support and collaboration with Federal law enforcement agencies and strategic partners.

Output:

Establish Response Mechanisms

- Sarawak Cybercrime Coordination Framework defining roles between State Agencies, Federal law enforcement and other key stakeholders established by Year 1.
- Formal coordination arrangements established with Federal law enforcement agencies established by Year 2.
- State cybercrime reporting and referral mechanism operational by Year 3.
- Annual Sarawak Cybercrime Situation Report published by Year 4.
- Regular joint cybercrime prevention exercises conducted.
- Statewide cybercrime awareness campaigns delivered annually.

Description:

Coordinate Cybercrime Response

Cybercrime continues to affect individuals, businesses and Government agencies throughout Sarawak, resulting in financial losses, service disruptions and declining public confidence in digital services. While investigation, prosecution and international law enforcement cooperation remain Federal responsibilities, Sarawak has an important role in preventing cybercrime, improving reporting pathways and coordinating local responses.

This initiative establishes a Whole-of-Sarawak cybercrime coordination framework that strengthens collaboration between Government agencies, law enforcement, financial institutions, telecommunications providers and other key stakeholders. It focuses on improving public awareness, facilitating timely reporting, supporting victims, sharing operational information and coordinating preventive actions to reduce the impact of cybercrime on Sarawak.

Outcome:

Improve Cybercrime Response

Government agencies, businesses and citizens respond more effectively to cybercrime through coordinated prevention, reporting and collaboration with Federal law enforcement agencies.

Value:

Reduce Cybercrime Impact

A coordinated Whole-of-Sarawak approach reduces the impact of cybercrime on citizens, businesses and Government by improving prevention, reporting and collaboration while leveraging Federal enforcement capabilities.

This page is intentionally left blank.

This page is intentionally left blank.

Sarawak Cybersecurity Strategy and Roadmap 2030

Sarawak Multimedia Authority
Level 5, Bangunan Yayasan Sarawak,
Jalan Masjid, 93000 Kuching,
Sarawak, Malaysia.

W: www.sma.gov.my
T: 082-268012
F: 082-268019

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy or any information storage and retrieval system, without permission in writing from the publisher.

