CSA SINGAPORE
Cyber Security Agency of Singapore

Building Singapore's **Cybersecurity Workforce** for the Age of AI

ABOUT THE REPORT

Purpose

The "Building Singapore's Cybersecurity Workforce for the Age of AI" publication examines how AI is changing Singapore's cybersecurity workforce and identifies priorities for its continued development. It considers how organisations can benefit from AI while sustaining the technical expertise, professional judgement and talent pathways needed for effective cyber defence.

Intended audience

The report is designed for cybersecurity and HR leaders making decisions about team structures, hiring, training and career progression, alongside policymakers shaping workforce support. It also supports education and training providers, industry partners and professionals in connecting capability requirements with relevant learning, practical experience and career progression.

Editorial Team

Wong Choon Bong
Yeo Boon Hui
Ashley Yap
Kong Tin Jun
Laurentia Ho

Scope

The publication considers the workforce implications of rising AI adoption in cybersecurity work. It examines the evolving nature of cybersecurity work and workforce demand, the capabilities professionals need, and the education, workplace learning and governance priorities that can support their development.

CSA draws on multiple sources to examine key trends and implications for Singapore's cybersecurity workforce. The publication reports on key survey findings, insights from qualitative interviews involving senior cybersecurity professionals across the public and private sectors, as well as relevant international research. The survey was conducted by Blackbox Research between August and September 2026 among 1,000 cybersecurity professionals and HR professionals in Singapore. The Skills Framework for ICT (cybersecurity track) showcased in this publication is intended to provide the starting point for assessing potential changes across cybersecurity roles.

Notes:
CSA does not specifically endorse any third-party claim made in this material or related references, and the opinions expressed by third-parties are theirs alone. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. To the fullest extent permitted by law, CSA does not warrant and hereby disclaims any warranty as to the accuracy, correctness, reliability, timeliness, noninfringement, title, merchantability or fitness for any particular purpose of the contents of this publication. CSA shall also not be liable for any damage or loss of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. CSA also reserves the right to refine its analyses as the threat situation evolves, and/or as further information is made available.

In Collaboration
with Blackbox Research

Contents

Executive Summary 05

AI Is Reshaping the Cybersecurity Landscape 07

AI Is Becoming Part of the Cyber Defence Toolkit 09

How AI is Changing the Roles of Cybersecurity Professionals 11

The Importance of Human Judgement 13

Impact of AI across Cybersecurity Job Roles 15

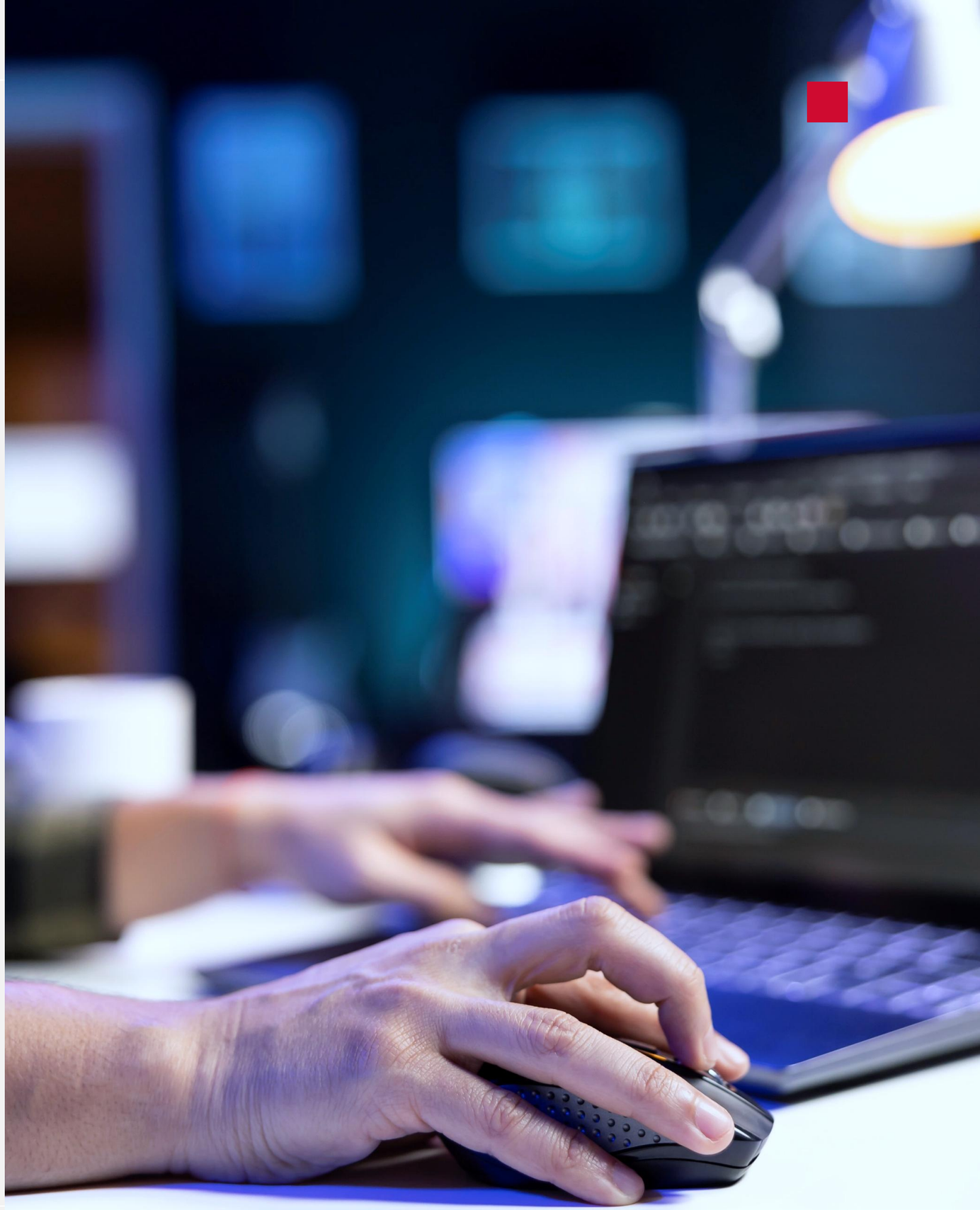
17 Workforce Demand Is Shifting Across Career Levels

19 Strengthening Entry-Level Pathways for an AI-Enabled Cybersecurity Workforce

21 Cybersecurity Foundations Remain Central to AI Readiness for All Levels

23 Growing Imperative for AI Security Governance

25 Conclusions & Way Forward



Executive Summary

AI is changing the demands on Singapore's cybersecurity workforce as it strengthens defensive capabilities and enables faster, more sophisticated attacks. Its adoption is reshaping roles, increasing the value of experienced judgement and changing how expertise develops. Preparing the workforce requires action on job redesign, capability development and governance.

1

AI is expanding defensive capabilities within a more demanding threat environment

AI is increasing the pace at which both threats and defensive capabilities evolve. With 85% of cybersecurity professionals expecting a meaningful AI-enabled threat within the next 12 months, Singapore's cybersecurity workforce needs to adapt alongside the threat environment.

AI can expand teams' capacity to process information and investigate threats, but sustained readiness requires professionals who can apply these capabilities to changing conditions.

2

Role augmentation and redesign increase the value of professional expertise

AI can extend the reach of cybersecurity expertise, allowing professionals to work across larger volumes of information and more complex workflows. Cybersecurity professionals mainly observe AI augmenting existing jobs and tasks, prompting role redesign as skill requirements change.

As AI handles more analysis and execution, professional contribution increasingly centres on determining whether AI outputs are credible, appropriate, and whether intervention is necessary. Experience and judgement are becoming increasingly valuable in directing this work, and demand for experienced talent is expected to grow, reinforcing the importance of technical depth alongside the ability to work effectively with AI.

3

AI offers career opportunities while increasing the importance of continuous upskilling

Cybersecurity professionals see AI as more of a career opportunity than a threat. Despite concerns about skills relevance, the majority of cybersecurity professionals in Singapore view AI positively for their careers. 77% see AI as more of a career opportunity than a threat, recognising that AI can extend their reach, elevate the value of their expertise, and open pathways to higher-value work.

At the same time, 75% are concerned that some of their current skills may become less relevant as AI becomes more widely adopted, underscoring the need for continuous upskilling rather than one-off training to remain competitive and effective.

4

Workforce development should strengthen foundations and preserve the experiences that build expertise

Workforce development must keep pace with how work is changing. Singapore will need both a steady pipeline of new talent and continued development of its existing cybersecurity workforce.

As AI takes on more routine work, organisations will need to redesign roles so professionals continue to build technical depth, while strengthening capabilities to use AI, secure AI systems and respond to AI-enabled threats. Maintaining critical human competencies will also be important where AI cannot be relied upon.

5

Governance needs to keep pace with AI's growing role in cybersecurity operations

AI governance in cybersecurity operations remains nascent and requires urgent attention. As AI-enabled tools take on a greater role in cybersecurity operations, governance arrangements have not kept pace.

In Singapore, 53% of cybersecurity professionals report that governance for the use of AI in cybersecurity is informal, absent, or incomplete. Globally, only 21% of organisations have a comprehensive AI security and governance framework in place. Organisations will need to establish clear responsibilities, defined escalation thresholds, and sustained human accountability to adopt AI with appropriate safeguards and confidence.

6

Shared responsibility on workforce development, progression and responsible AI use

Building an AI-ready cybersecurity workforce in Singapore calls for continuity between workplace development, job redesign, and career progression. Stronger entry-level pathways, including internships and hands-on training, and closer employer–education collaboration are the leading priorities for strengthening the talent pipeline.

Different parts of the ecosystem have complementary roles. Employers can redesign jobs and provide structured workplace development; education and training providers can keep curricula responsive to changing technologies and workplace needs; professionals must continue to deepen and refresh their capabilities; and Government can support the ecosystem through common competency references, talent development initiatives, partnerships and practical guidance. Sustained coordination across these areas will be important to realise the benefits of AI while building the depth of cybersecurity expertise Singapore will need for the future.

AI Is Reshaping the Cybersecurity Landscape

> AI is such a powerful tool. It can be used just as effectively by bad actors, and it can be used by good actors who are trying to defend the country and companies.

CYBERSECURITY & AI ACADEMIC

Artificial Intelligence (AI) is a double-edged sword in cybersecurity

It represents both a **significant threat** and an **unprecedented opportunity** in the cybersecurity landscape.

As an offensive tool, AI enables adversaries to turbocharge their cyber-attacks, lowering barriers to entry and allowing less-skilled attackers to operate at previously unattainable levels of speed, scale, and sophistication.

CrowdStrike's 2026 Global Threat Report reported that 2025 saw an 89% increase in attacks by "AI-enabled adversaries" compared with the previous year.

In Singapore, 85% of cybersecurity professionals expect their organisation or sector to face a meaningful AI-enabled cyber threat within the next 12 months, with key threats seen in AI-enabled phishing, impersonation, deepfakes or other social engineering, automated reconnaissance, target identification, or vulnerability discovery, and AI-assisted malware development, exploitation or attack evasion.

85%

expect their organisation or sector to face **an impactful AI-enabled cyber threat** within the next 12 months

Top 5 AI-enabled Cyber Threats
Observed in Past 12 months

- **58%** Phishing, impersonation, deepfakes
- **50%** Automated reconnaissance, target identification or vulnerability discovery
- **42%** AI-assisted malware development, exploitation or attack evasion
- **37%** Attacks against AI systems
- **35%** AI-powered ransomware

87%

believe attacker capabilities are **advancing faster** than many organisations in Singapore can **defend** against

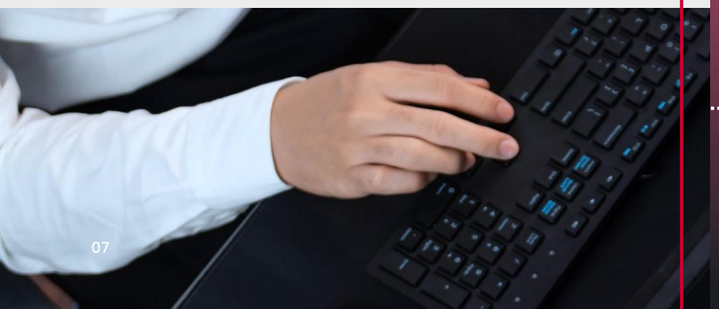
Top 5 Challenges posed by AI-enabled Cyber Attacks

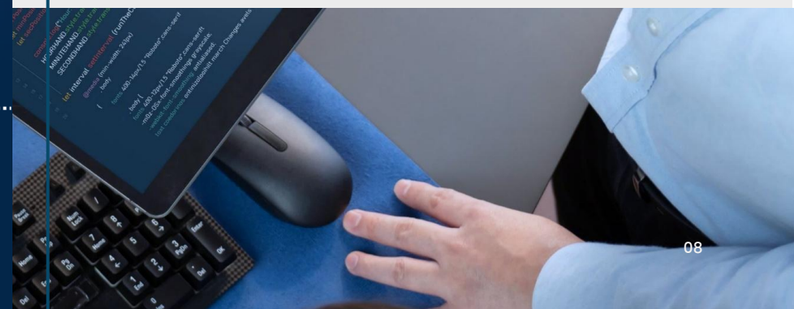
- **73%** Sophistication and adaptability of attacks
- **65%** Speed at which attacks can be prepared or executed
- **51%** Difficulty of detecting or identifying attacks
- **44%** Scale or volume of attacks that can be carried out
- **35%** Degree to which attacks are personalised or precisely targeted

While AI is not necessarily creating entirely new categories of cyber threat, it is amplifying existing threats by making them faster, more scalable and more accessible to a broader range of attackers

Among cybersecurity professionals in Singapore who had observed AI-enabled threats in the past 12 months, 73% identify greater sophistication and adaptability as a key challenge, while 65% point to the increased speed at which attacks can be prepared or executed. A further 51% highlight the difficulty of detecting or identifying AI-enabled malicious activity. 87% believe attacker capabilities are advancing faster than many organisations in Singapore can defend against.

Together, these shifts are creating a faster-moving and more demanding operating environment for the cybersecurity workforce. AI therefore needs to be understood in three ways: as a threat, as a target and as a tool. Professionals will need to defend against adversaries using AI to increase the speed and sophistication of attacks; secure AI systems, models and data as they introduce new attack surfaces; and use AI-enabled capabilities to strengthen cyber defence. These three dimensions will shape how cybersecurity roles, skills and workforce requirements evolve.





AI Is Becoming Part of the Cyber Defence Toolkit

AI presents tremendous defensive opportunities

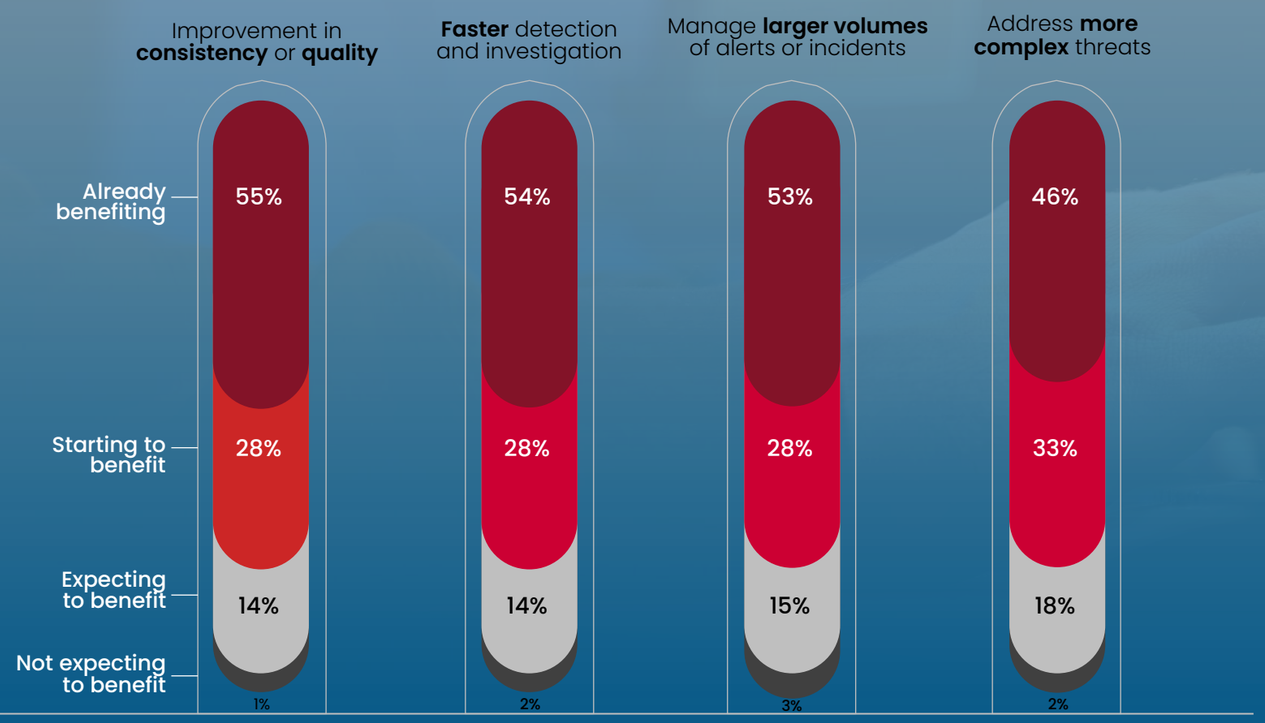
AI-enabled capabilities are increasingly being applied across areas ranging from threat detection and investigation to penetration testing and security operations.

According to Fortinet's 2025 Cybersecurity Skills Gap Report, 97% of organisations were already using or planning to implement AI-enabled cybersecurity solutions.

The benefits of AI in cybersecurity are clear: faster response times, fewer false positives, and defences that scale as attacks grow more complex.

> "In the past, an incident or event could take days or hours to resolve, now it takes seconds. So this type of productivity has actually improved tremendously.
>
> CHIEF TECHNOLOGICAL OFFICER, GOVERNMENT-LINKED ENTERPRISE, SINGAPORE

Key Operational Benefits of AI Observed by Singapore Cybersecurity Professionals



Excludes those who indicated "Not Applicable"

In Singapore, AI is already being integrated into a wide range of cybersecurity activities

Its most common use today is in monitoring, detection and alert prioritisation, where AI can help security teams process large volumes of logs and alerts, identify suspicious activity and surface higher-priority cases for investigation. It is also being used for security reporting, documentation and workflow support, helping professionals consolidate information, draft reports and streamline repetitive administrative tasks.

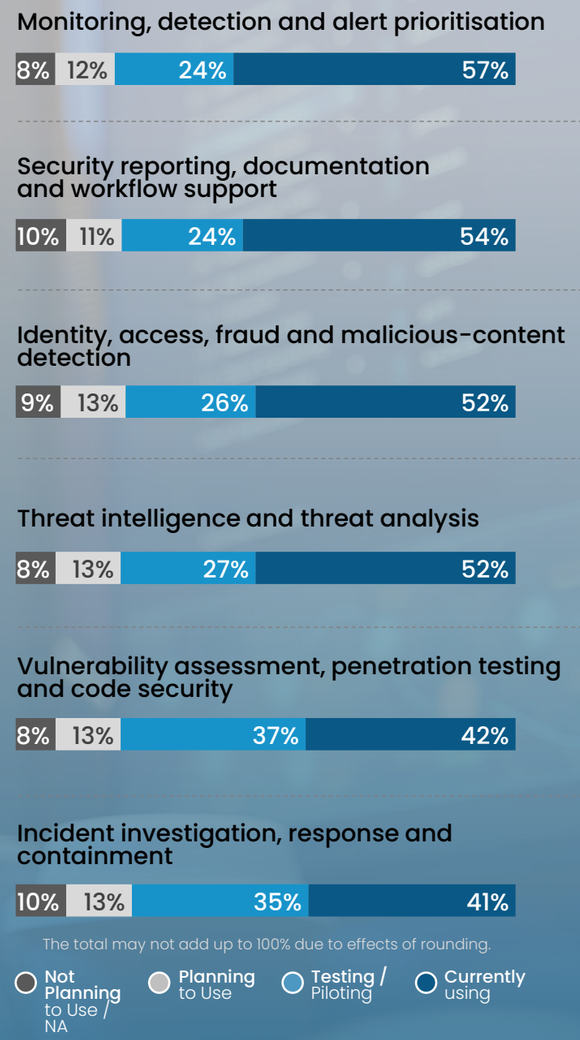
Organisations are also moving beyond these established use cases into more complex areas. In vulnerability assessment and penetration testing, AI can support activities such as scanning, code review and the generation of test cases, while cybersecurity professionals remain responsible for validating whether findings are genuinely exploitable. In incident investigation and response, AI can help correlate threat information, analyse incidents and generate response recommendations, but human judgement remains critical in deciding how to contain and recover from an incident.

These gains also have implications for how cybersecurity teams are structured. AI can act as a force multiplier by allowing existing teams to process larger volumes of information, automate repeatable activities and extend their coverage. This does not necessarily mean fewer cybersecurity professionals will be required; rather, the mix of work may change as less time is spent on routine execution and greater attention is directed towards complex investigations, exceptions and higher-risk decisions.

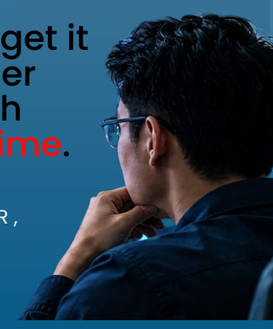
Yet adoption does not automatically translate into readiness. Just over half (53%) of cybersecurity professionals rate their organisations as very or fully prepared to manage AI-enabled threats.

The critical question has shifted from "when" to "how", specifically, how organisations can implement AI solutions efficiently, effectively, and securely while maintaining robust cybersecurity standards, and how the cybersecurity workforce must adapt to stay relevant.

AI Use across Cybersecurity Work Areas



> "Attacker needs to get it right once. Defender has to keep up with defending, every time.
>
> SENIOR DIRECTOR, TELECOMMUNICATIONS SECTOR , SINGAPORE



How AI is Changing the Roles of Cybersecurity Professionals

Traditionally, cybersecurity work has involved significant manual effort, with professionals monitoring systems, analysing alerts, testing defences, investigating incidents and responding to threats as they emerge.

Today, AI is changing how this work is performed. Among cybersecurity professionals in Singapore, 53% report using generative AI tools and 33% agentic capabilities, extending AI's role from assisting individual tasks to supporting broader workflows.

Agentic AI could deepen this shift. Unlike Generative AI tools that primarily generate analysis or recommendations, agentic systems can be configured to carry out sequences of actions across cybersecurity workflows with varying degrees of autonomy. As adoption grows, cybersecurity professionals may increasingly need to define what actions AI systems are permitted to take, establish thresholds for human escalation, monitor their behaviour and intervene when outcomes fall outside intended boundaries.

53% of Singapore cybersecurity professionals are using **generative AI tools**

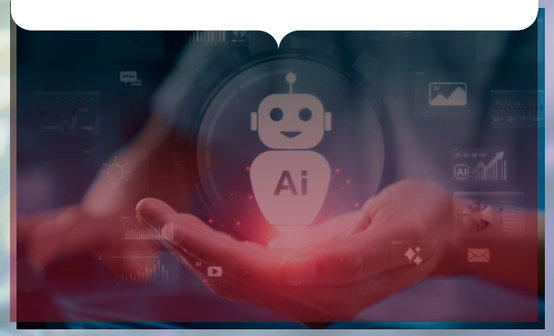
Generative AI can support*

- Risk assessments and attack simulations
- Classify sensitive information
- Recommend and test security measures
- Analyse user behaviour and detect anomalies
- Create simulated phishing attacks

33% of Singapore cybersecurity professionals are using **agentic AI capabilities**

Agentic AI can support*

- Real-time network monitoring
- Autonomous intrusion detection and response
- Vulnerability scanning and patching
- Predictive threat intelligence
- Offensive testing and attack simulation
- Case management and next-step recommendations



*This list is illustrative and not exhaustive.

AI is also changing where cybersecurity professionals contribute most

As tools assume more routine analysis and execution, professionals have greater scope to investigate complex problems, anticipate threats and evaluate recommendations. Cybersecurity professionals in Singapore identify routine task automation as a significant change, alongside greater focus on higher-value work, and a more proactive approach.

Key Changes in Cybersecurity Work with AI Adoption

96% of cybersecurity professionals have observed AI transforming **cybersecurity work**

- **54%** **Automating** routine or repetitive tasks
- **42%** Enabling professionals to focus on more **complex** or higher-value work
- **39%** Enabling cybersecurity work to become more **proactive**
- **35%** Shifting professionals towards **AI oversight**, validation and judgement
- **30%** Creating **new work** related to securing or governing AI systems
- **30%** Enabling the existing cybersecurity workforce to manage **more work or tasks**

These shifts extend beyond individual tasks to how cybersecurity roles are organised

53% of respondents observed AI augmenting existing roles, while an equal proportion reported role redesign as skill requirements change. The workforce impact is therefore not simply about automation; it is also about how responsibilities are redistributed and where professionals contribute most.

Key Changes in Cybersecurity Job Roles with AI Adoption

96% of cybersecurity professionals have observed AI transforming **cybersecurity job roles**

- **53%** Roles are being **augmented**
- **53%** Roles are being **redesigned**
- **39%** New roles are being **created**
- **35%** Roles are being **combined**
- **23%** The number of positions is being **reduced**

The Importance of Human Judgement

AI is reducing the operational burden of cybersecurity work by augmenting and accelerating tasks, and by translating human intent into queries, analysis and technical actions. Simpler workflows, however, do not make the underlying security decisions simpler.

Professionals must still determine whether alerts and indicators are credible, distinguish false positives from genuine threats, assess impact in context, and decide what action or escalation is appropriate.

Reflecting this shift, nearly half of cybersecurity professionals (47%) identified human review, validation, and judgement as the most important measure governing the use of AI.

As AI takes on more execution, the value of human expertise increasingly lies in deciding when automated conclusions can be relied upon, when they should be challenged, and who remains accountable for the resulting action.

47%

of cybersecurity professionals identified **human review of AI-generated findings** or recommendations as the **most important** governance measure to adopt amid rising AI adoption

Where human judgement remains critical

Assessing credibility
Determining whether alerts and indicators are genuine or false positives.

Evaluating impact
Applying experience and context to separate benign activity from real risks.

Deciding on action
Determining the appropriate response or escalation.

Taking accountability
Ensuring decisions are well-justified and accountable.

AI analysis
Detects and analyses potential threats at scale

Human judgement
Reviews, validates and applies context

Action
Responds or escalates based on assessed risk

> "Human judgement remains important even as AI capabilities improve, particularly for higher-risk decisions and complex investigations.
>
> CHIEF TECHNOLOGICAL OFFICER, GOVERNMENT-LINKED ENTERPRISE, SINGAPORE

Impact of AI across Cybersecurity Job Roles

AI is changing how cybersecurity work gets done, augmenting people across the end-to-end lifecycle. The following table illustrates how AI can augment work across cybersecurity role families, from risk analysts to the CISO. It outlines the activities AI can support, where human judgement and oversight remain essential, and the additional competencies required.

Cyber Risk

AI can support **risk assessment, research, monitoring and the preparation of risk and governance materials**, enabling cyber risk professionals to analyse information more efficiently.

Domain expertise and judgement remain central to assessing risks in context, determining their business and regulatory implications, and recommending appropriate risk treatment and controls.

Security Operations

AI can augment **monitoring, alert categorisation, large-scale log analysis, correlation, detection and reporting**, helping security operations teams process and analyse information more efficiently and at greater scale.

Security operations professionals remain central to detecting and investigating threats, responding to incidents and maintaining effective security operations, applying their expertise and judgement to interpret findings, handle complex cases and escalations, and refine detection approaches.

Vulnerability Assessment & Penetration Testing

AI can augment aspects of **testing, analysis and reporting**, enabling VAPT professionals to assess systems more efficiently and explore potential attack paths at greater scale.

Technical expertise and judgement remain central to determining whether vulnerabilities are genuinely exploitable, designing and conducting effective tests, and investigating complex attack paths. Professionals also provide oversight, establish and enforce appropriate boundaries and guardrails for AI-enabled testing, and ensure that testing is conducted safely without causing unintended harm to the systems or environments being tested.

Forensics

AI can augment the **processing, correlation and analysis of large volumes of digital evidence**, enabling forensic investigators to work more efficiently and at greater scale.

Forensic expertise and judgement remain central to examining and interpreting evidence, establishing root cause, maintaining evidential integrity and ensuring that investigative findings and conclusions are robust and defensible.

Incident Response

AI can support **threat-information analysis, incident analysis and response planning, help incident-response professionals process information and assess incidents more efficiently**.

Human judgement remains central to understanding the context and impact of an incident, determining appropriate containment and recovery actions, and adapting the response as circumstances evolve. At senior levels, command decisions and accountability remain particularly important, especially where incidents have significant operational or organisational consequences.

Threat Analysis

AI can expand the scale at which teams **monitor external threats, connect information and assess potential attack activity**.

AI-generated intelligence can support threat-analysis professionals in their work, but human validation, contextualisation and analysis remain important, particularly where work requires judgement around attribution, severity, hostile intent and novel threats. Attribution may also require geopolitical context and understanding of adversary tradecraft that AI may not consistently capture.

Security Engineering & Architecture

AI can support **security analysis, configuration review, research, design development and documentation**, enabling engineers and architects to work more efficiently and at greater scale.

Their technical expertise and judgement remain central to developing secure designs, making architecture and technology decisions, addressing complex requirements and resolving implementation issues in real-world environments. As AI adoption grows, engineers and architects will also need to consider security risks associated with AI systems, models, deployment infrastructure and supply chains.

Cybersecurity Leadership

At the leadership level, AI can help synthesise information, identify patterns, develop scenarios and support decision-making at greater scale.

However, the CISO retains **intellectual ownership and accountability for cybersecurity analysis and decisions**, including determining material risks, setting priorities and deciding where action and resources are required. The role also expands to overseeing the cybersecurity implications of AI adoption and the responsible use of AI within the cyber function.

Workforce Demand Is Shifting Across Career Levels

As AI takes on a larger share of cybersecurity execution, the value of professional judgement increases

Cybersecurity professionals must be able to recognise gaps in AI-generated analysis, interpret findings in context and decide when further investigation or intervention is needed.

This places greater emphasis on professionals who have the technical depth and operational experience to assess whether AI recommendations are not just technically valid but also appropriate for the circumstances.

Demand is expected to strengthen at the mid and senior levels

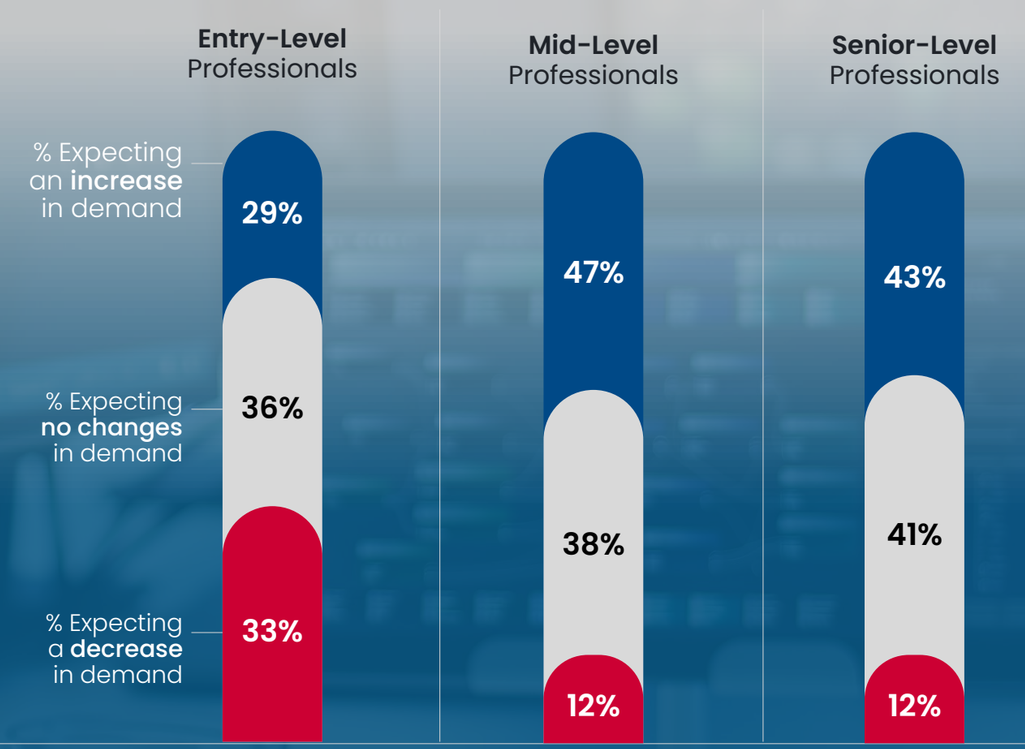
Over the next three years, 47% of respondents expect mid-level demand to increase and 43% expect growth at the senior level, compared with 29% for entry-level roles. Among those expecting greater mid-level demand, the most common reasons were the need for professionals who can interpret and challenge AI-generated outputs, and who can oversee the use of AI in cybersecurity work.

The entry-level outlook is more mixed

Most respondents expect junior roles to be redesigned rather than eliminated, suggesting that the main change will be in the nature of the work and the capabilities expected at the start of a cybersecurity career.

The workforce challenge extends beyond immediate hiring. If demand increasingly concentrates at the experienced end of the market, organisations will also need to sustain the pipeline through which today's less-experienced professionals develop into tomorrow's mid-level specialists and senior practitioners.

Expected Demand for Singapore's Cybersecurity Workforce by Seniority over the Next 3 Years



Excludes those who indicated "Not sure" or "Not Applicable"

Strengthening Entry-Level Pathways for an AI-Enabled Cybersecurity Workforce

Meeting future demand for experienced cybersecurity talent depends on how entry-level professionals are developed today

As AI changes the work assigned to junior professionals, organisations will need to consider not only their immediate contribution, but also whether entry-level roles continue to provide the experiences needed for progression.

The survey indicates that these roles are more likely to be redesigned than eliminated. Most respondents expect entry-level professionals to take on more complex work with the support of AI and to increasingly supervise or direct AI-enabled systems. This means junior professionals will be expected to contribute differently, with less emphasis on routine execution and greater emphasis on understanding, interpreting and managing AI-supported work.

Greater automation may reduce some of the conventional opportunities through which junior professionals build practical experience

Investigation, testing hypotheses, examining evidence and making decisions have historically helped practitioners develop the technical instincts required for more advanced roles.

Reflecting this concern, 86% of respondents agreed that greater reliance on AI could weaken entry-level professionals' ability to investigate problems or make decisions independently, while 83% were concerned that fewer opportunities for foundational learning could make progression into more senior roles harder.

Outlook on Entry-level Jobs among Singapore Cybersecurity Professionals

87%
Entry-level jobs are more likely to be redesigned rather than eliminated

87%
Entry-level professionals will be expected to perform more complex work

86%
Greater reliance on AI may weaken entry-level professionals' ability to investigate problems or make decisions independently

84%
Entry-level professionals will increasingly shift from performing routine tasks to supervising and directing AI-enabled systems

83%
Entry-level professionals may find it harder to progress into senior positions as AI reduces opportunities for foundational learning

This makes the quality of entry-level development increasingly important

The survey shows that respondents place the greatest emphasis on strong core cybersecurity fundamentals (65%), followed by the ability to validate and challenge AI-generated outputs (57%) and hands-on technical experience (51%). These priorities suggest that effective use of AI depends on understanding the cybersecurity work behind it. Junior professionals need sufficient technical depth to recognise missing evidence, question assumptions and determine whether an AI-generated recommendation is credible and appropriate.

The challenge, therefore, is not simply to preserve entry-level jobs, but to **preserve the developmental value** of those roles. As AI takes on more routine execution, employers may need to create learning opportunities more deliberately rather than assume they will arise naturally through day-to-day work. This could include supervised casework, manual validation of AI-generated findings, structured rotations, realistic exercises, progressively greater responsibility, participation in external cybersecurity competitions or hackathons, and hands-on practice through cyber ranges.

This focus on technical depth is also consistent with wider workforce needs. The SANS-GIAC 2026 study found that 60% of organisations identified a lack of the right skills as a greater staffing challenge than insufficient staffing. The implication is that sustaining Singapore's cybersecurity workforce will require not only a steady supply of new entrants, but also deliberate development pathways that enable them to progress into more complex roles over time.

Well-designed entry-level roles can therefore serve two purposes at once: enabling junior professionals to contribute effectively in an AI-enabled environment today, while building the technical depth and judgement needed to become the mid-level specialists and future senior practitioners the industry will need tomorrow.

Priority Skills for Entry-Level Professionals

65% Strong core cybersecurity fundamentals

57% Ability to validate and challenge AI-generated outputs

51% Hands-on technical experience

40% Evidence-based judgement and reasoning

36% Understanding how AI systems can fail or be manipulated

29% Applying AI governance, privacy, accountability and responsible-use principles

22% Prompting or instructing AI tools effectively

Cybersecurity Foundations Remain Central to AI Readiness for All Levels

AI is expanding the capabilities cybersecurity professionals need to strengthen defence and secure AI systems, but it is not replacing the foundations of cybersecurity practice

This reflects the three dimensions of AI in cybersecurity: professionals need to respond to AI-enabled threats, secure AI systems as an expanding attack surface, and use AI effectively as part of cyber defence.

The survey on cybersecurity workforce in Singapore reinforces this broader capability stack. Judgement and problem-solving, cybersecurity domain knowledge and the ability to detect and respond to AI-enabled threats remain among the most important capabilities for the coming years, alongside understanding AI limitations and securing AI applications, models, data and infrastructure. AI proficiency should therefore be developed on top of, rather than at the expense of, core cybersecurity expertise.

The findings suggest that readiness for an AI-enabled environment requires professionals to build AI capabilities on top of strong cybersecurity knowledge and professional judgement. Respondents placed judgement and problem-solving, cybersecurity domain knowledge and the ability to detect and respond to AI-enabled threats among the most important capabilities for the coming years. Rather than treating AI proficiency as a standalone skill, professionals will increasingly need to understand where AI can support their work, where its outputs may be unreliable, and when human intervention is required.

Key Capabilities for Cybersecurity Professionals over the Next 3 Years

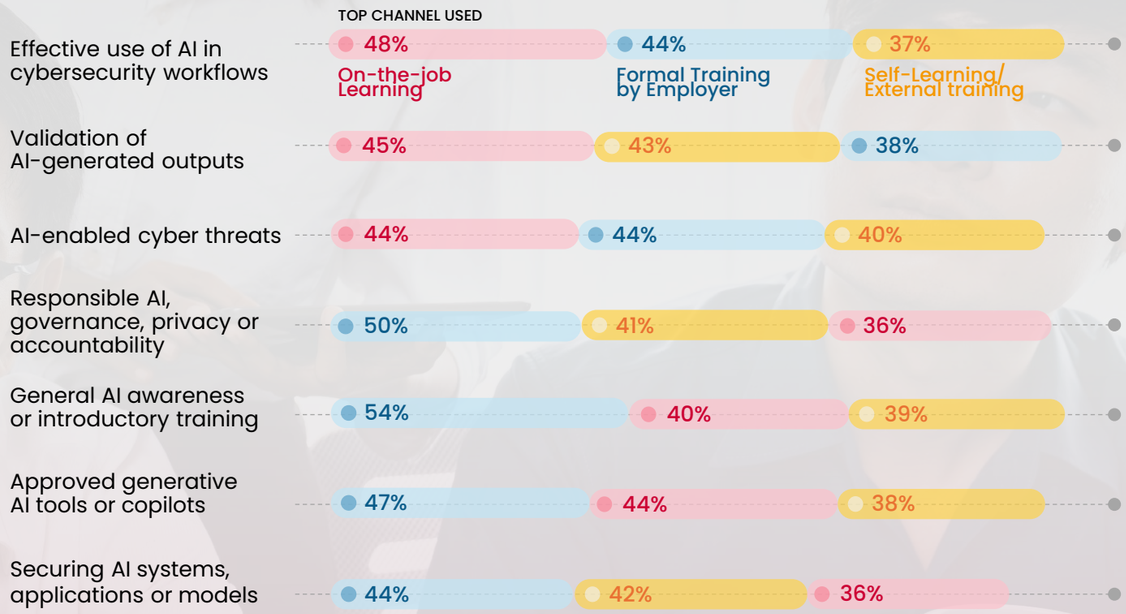
- **69%** Applying judgement and problem-solving in business and operational contexts
- **66%** Cybersecurity domain knowledge and technical fundamentals
- **65%** Detecting and responding to AI-enabled cyber threats
- **61%** Understanding AI systems, including their limitations and potential failure modes
- **61%** Securing AI applications, models, data and infrastructure
- **57%** Applying AI governance, privacy, accountability and responsible-use principles
- **56%** Using, configuring and supervising AI-enabled cybersecurity tools and agents

Deepening AI Capabilities Through Training and Workplace Learning

Developing AI-related cybersecurity capabilities requires both structured training and opportunities to apply that learning in the workplace. The survey reflects these complementary pathways: 54% of respondents developed general AI awareness through formal employer-provided training, while 48% built practical capability in applying AI to cybersecurity workflows through on-the-job learning.

These approaches are complementary. Structured training can establish common concepts, technical foundations and expectations for responsible use, while workplace learning enables professionals to apply them to real operational settings, learn from exceptions and receive feedback. Together, they help translate knowledge into demonstrable capability.

Key Channels of AI-related Cybersecurity Training in Past 12 Months



Capability development must also keep pace with changing technologies, threats and job requirements. While 77% of cybersecurity professionals see AI as more of a career opportunity than a threat, 75% are concerned that some of their current skills may become less relevant as AI becomes more widely used. This reinforces the need for continuous upskilling, rather than one-off training. Employers can support this through a combination of formal courses, workplace learning and practical assessment to help professionals deepen their capabilities and keep their skills current.

Capability development should also guard against over-reliance on AI. As more activities become AI-assisted, organisations should consider which human competencies must remain independently executable, particularly for critical or high-risk functions. Periodic exercises, manual practice and contingency procedures can help ensure that professionals retain the ability to operate when AI systems are unavailable, produce unreliable results or cannot appropriately address an unfamiliar situation.

Growing Imperative for AI Security Governance

As AI-enabled tools take on a greater role in cybersecurity operations, organisations will need robust governance that keeps pace with advancements in AI. This means establishing clear responsibilities for how AI is used, what decisions it may support or execute, and when human review or escalation is required.

Governance maturity remains uneven

In Singapore, 53% of cybersecurity professionals reported that governance for the use of AI in cybersecurity was informal, absent or incomplete.

The SANS-GIAC 2026 Cybersecurity Workforce Research Report found that only 21% of organisations had a comprehensive AI security and governance framework, while a further 33% had a basic policy. The findings point to a common challenge: adoption is progressing while governance arrangements are still maturing.

53%

of cybersecurity professionals reported that their organisation's governance for the use of AI in cybersecurity was absent, informal, or incomplete

21%

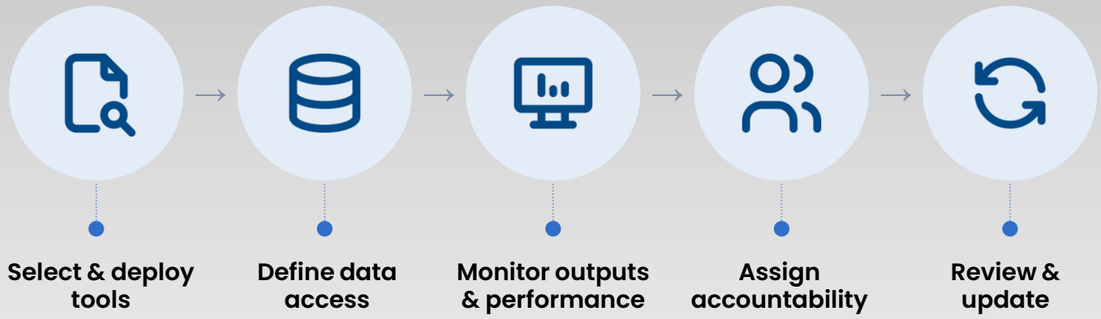
of organisations had a comprehensive AI security & governance framework

33%

of organisations had a basic policy

Effective governance needs to extend across the AI lifecycle

Organisations should consider how AI-enabled cybersecurity tools are selected and deployed, what data they can access, how their performance and outputs are monitored, and where accountability rests when AI contributes to operational decisions. As AI capabilities evolve, these arrangements will also need to be reviewed and updated.



Effective AI governance and secure deployment are inherently cross-functional

Cybersecurity professionals will increasingly need to work alongside AI/ML engineers, data scientists, technology teams, risk, legal, compliance and business functions throughout the development and deployment of AI systems.

AI practitioners bring knowledge of models, data and system behaviour, while cybersecurity professionals contribute threat modelling, security assurance, risk assessment and incident-response expertise. Bringing these perspectives together early can help identify security risks before systems are deployed and establish appropriate controls, monitoring and escalation arrangements.

The objective is not to constrain the use of AI, but to enable organisations to adopt it with appropriate safeguards and confidence

Clear governance, defined escalation points and continued human accountability can help organisations realise the benefits of AI while managing the new risks introduced by its use.

CONCLUSION

Building an AI-Ready Cybersecurity Workforce Is a Shared Responsibility

AI is increasing the speed and scale of cybersecurity operations while expanding the capabilities available to attackers. An AI-ready cybersecurity workforce will therefore need to respond to AI as a threat, secure AI systems as a target, and harness AI as a tool for cyber defence.

The workforce impact centres on augmentation and role redesign, with routine execution increasingly supported by AI and professional expertise applied to more complex analysis, decisions and oversight.

As AI changes how work is performed, the opportunities through which professionals acquire experience will also need to evolve. Building an AI-ready cybersecurity workforce is therefore a shared responsibility, connecting job redesign, education, workplace development and career progression. Stronger entry-level pathways and hands-on training (46%), closer employer–education collaboration (45%), and updated competency frameworks with clearer career pathways (40%) are the leading priorities for workforce support. Coordinating these efforts can help translate changing role requirements into relevant learning and practical development opportunities.

Top 5 Support Priorities for Strengthening Singapore's Cybersecurity Workforce and Talent Pipeline

46%	45%	40%	39%	38%
Stronger entry-level pathways, internships, and hands-on training	Stronger collaboration between employers and educational institutions to align training opportunities	Updated cybersecurity skills and competency frameworks for clearer career-progression pathways	Subsidised training and professional development programmes	Leadership, mentoring and specialist-development programmes to help professionals progress

1

Employers can treat AI adoption and job redesign as opportunities to develop workforce capability. Supervised investigations, rotations and mentoring can preserve opportunities to build technical depth, while practical assessment can inform progression into more complex responsibilities. Clear boundaries for AI use, human review and escalation can also keep accountability aligned with changing workflows.

2

Professionals remain responsible for deepening and refreshing their expertise. Keeping pace with cybersecurity and AI developments and seeking out role-relevant learning can strengthen their ability to think critically and exercise informed judgement as technologies evolve.

3

Education and training providers can ensure cybersecurity training keeps pace with emerging AI requirements. Collaboration with employers can inform curricula, realistic exercises and assessments that test how professionals investigate problems and justify decisions. Connecting classroom learning with workplace application can help turn knowledge into operational capability.

4

Government can provide a common direction for this transition. Working with industry and education partners to review role-specific competencies and career pathways can clarify expectations at different levels of practice. Talent development initiatives, partnerships and practical guidance can support organisations and professionals in responding to these requirements.

Together, these contributions can help Singapore use AI to strengthen cybersecurity capacity — building a workforce equipped to use it effectively, secure it responsibly, and develop the specialists and leaders needed to safeguard our digital way of life.

APPENDIX

The following table illustrates how AI can augment work across cybersecurity role families, from risk analysts to the CISO. It outlines the activities AI can support, where human judgement and oversight remain essential, and the additional competencies required.

The assessment uses the cybersecurity track of the Skills Framework for ICT (Navigate SFw for ICT) as its starting point, drawing on each role's work functions, key tasks and competencies to assess potential changes in how work is performed. The examples are illustrative and non-exhaustive, providing a basis for role redesign and professional development.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate?*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Cyber Risk Analyst *Governance, Risk & Control*	• Performing risk assessments against established plans • Assessing third-party controls and internal systems • Researching emerging risk trends, issues and alerts • Monitoring risks and incidents against policy • Drafting risk-assessment and threat-awareness reports	• Defining the scope of risk analysis for new systems and technologies • Exercising judgement to determine the cause and impact of security violations • Recommending appropriate corrective actions and risk controls • Assessing remediation progress and whether identified risks have been adequately addressed	• Using AI tools to support cybersecurity risk assessment and analysis • Assessing the reliability and limitations of AI-generated risk analysis • Validating AI-generated risk findings and recommendations using professional judgement • Understanding the risks and limitations of using AI in cybersecurity risk assessments	AI can support risk assessment, research, monitoring and reporting, enabling cyber risk analysts to process and analyse information more efficiently. The analyst continues to require cyber risk expertise and judgement to assess risks in context, determine their potential impact, recommend appropriate controls and assess whether identified risks have been adequately addressed.
Cyber Risk Manager *Governance, Risk & Control*	• Drafting risk frameworks, methodologies and requirements • Running and coordinating ongoing cyber risk assessments at scale • Synthesising emerging threat and risk trends into the assessment framework • Drafting governance procedures, policies and compliance-audit frameworks • Generating cyber risk and threat-awareness report drafts	• Recommending strategies to address key cyber risk areas • Anticipating regulatory and business challenges and their implications for cybersecurity risk • Setting and overseeing the organisation's Cyber Risk Maturity model • Leading responses to regulatory inquiries, inspections and audits • Providing expert judgement in breach investigations and remediation	• Understanding how AI can support cyber risk management and decision-making • Evaluating and challenging AI-generated risk analysis and recommendations • Understanding the risks and limitations of using AI in cyber risk management • Understanding the cybersecurity implications of enterprise AI adoption	AI can support risk analysis and the preparation of risk assessments and governance materials, enabling cyber risk managers to process and synthesise information more efficiently. The manager continues to require cyber risk expertise and judgement to assess risks in context, set risk direction, determine appropriate responses and address regulatory, business and breach-related matters.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Associate Security Analyst *Entry, Security Operations*	• Monitoring IT systems and applications for security events • Categorising incidents and tracking alerts • Compiling security-operations performance reports • Enriching and triaging routine security queries	• Escalating and validating incidents for remediation • Assisting hands-on in threat investigations • Educating users on security policies and practices • Monitoring third-party and user adherence to policies • Piloting and recommending new tools and improvements	• Recognising AI-orchestrated threat activities • Engineering prompts to achieve desired AI outcomes • Supporting configuration of AI guardrails and security controls • Validating and escalating AI-generated alerts or actions • Recognising limitations, hallucinations and false positives/negatives in AI outputs	AI can augment routine monitoring, alert categorisation, triage and reporting, enabling associate security analysts to process security information more efficiently and at greater scale. The associate continues to build and apply foundational security operations skills through monitoring, investigation and escalation of security events. As AI adoption grows, this also includes using AI-enabled security tools effectively, assessing AI-assisted findings and recognising their limitations.
Security Operations Analyst *Security Operations*	• Real-time analysis and trending of security log data • Analysing event data to flag suspicious activity • Drafting incident status updates and final reports • Maintaining data sources feeding the monitoring system • Drafting detection and alert rules and monitoring plans	• Exercising judgement to determine incident type and severity • Validating and escalating incidents that require further investigation • Refining monitoring rules and alerts based on emerging threats and operational experience • Determining appropriate response actions for detected incidents • Adapting response procedures to novel or complex incidents	• Recognising AI-orchestrated threat activities • Engineering prompts to achieve desired AI outcomes • Continuously optimising AI workflows based on operational feedback and performance • Configuring AI security controls and guardrails • Assessing AI-generated detections and recommendations for reliability	AI can augment large-scale log analysis, correlation, detection and reporting, enabling security operations analysts to process and analyse security information more efficiently and at greater scale. The analyst continues to require security operations expertise and judgement to interpret and investigate detections, determine incident type and severity, handle escalations and refine detection approaches. As AI adoption grows, this also includes assessing AI-assisted detections and recognising AI-enabled attack techniques.
Security Operations Manager *Security Operations*	• Measuring and reporting SecOps metrics and service levels • Consolidating incident and breach reports for review • Prioritising alerts and resources for incident response • Drafting periodic status reports for management	• Setting SecOps strategy and aligning it with business priorities • Determining operational coverage and escalation requirements • Advising senior leaders on critical security issues and response decisions • Reviewing and approving incident findings before escalation • Driving continuous improvement of security operations	• Understanding the capabilities and limitations of AI-enabled security monitoring and incident response • Evaluating the reliability and effectiveness of AI-enabled detection and response tools • Interpreting AI-generated security analysis and recommendations to support operational decisions • Applying appropriate human-oversight principles when using AI in security operations • Understanding the security and responsible-use considerations of AI in security operations	AI can augment the development of detection rules, analysis of operational metrics, preparation of incident summaries and prioritisation of alerts, enabling security operations to be managed more efficiently and at greater scale. The manager continues to require security operations expertise and judgement to set operational priorities, assess the effectiveness of detection and response capabilities, oversee escalations and drive continuous improvement. As AI adoption grows, this also includes overseeing the appropriate use and performance of AI-enabled security capabilities.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
VAPT Analyst *Vulnerability Assessment and Penetration Testing*	• Scoping which components require testing • Translating requirements into test plans and scripts • Running scans, black-box tests and code reviews • Drafting reports on VAPT results • Preparing and maintaining certification documentation	• Conducting complex reverse engineering and on-site security assessments • Exercising judgement to determine whether findings are genuinely exploitable • Reviewing software designs, source code and deployments for security implications • Advising development teams on penetration-testing needs • Improving testing methodologies for novel or complex threats	• Testing AI models for prompt-injection, jailbreak and adversarial-ML weaknesses • Assessing AI-specific attack surfaces and misuse risks • Evaluating AI model, application and supply-chain security exposure • Validating AI-generated test cases and findings • Conducting security testing of AI systems before deployment	AI should be treated more like a junior pentester. It can perform significant parts of testing, but its outputs still need to be verified and triaged by an experienced practitioner. The analyst increasingly becomes the validator and expert-in-the-loop, determining whether AI-generated findings are valid, exploitable and meaningful. The analyst will also steer AI-assisted testing, deciding what and how to test, setting and enforcing appropriate boundaries and guardrails, guiding AI towards promising attack paths, and taking over where deeper expertise is required. They will also ensure that AI-assisted testing is conducted safely and does not cause unintended harm to the systems under test.
VAPT Manager *Vulnerability Assessment and Penetration Testing*	• Establishing test metrics and benchmarks against best practice • Drafting testing policies, governance procedures and methodologies • Building frameworks and dashboards for VAPT reporting • Consolidating complex test-data and root-cause analysis • Drafting stakeholder communications of testing outcomes	• Setting the strategy and scope for security testing • Exercising judgement on escalated testing issues and risks • Recommending strategic changes to address emerging threats • Validating and approving final test results • Leading improvements to testing methodologies and capabilities	• Setting scope and assurance requirements for AI security testing • Leading AI red-teaming and adversarial-testing programmes • Establishing AI-specific testing methodologies and security protocols • Assessing AI supply-chain and model-security risks within testing engagements	AI can automate much of the traditional project-management work such as consolidating results, tracking metrics and drafting reports. The manager continues to require the underlying VAPT expertise to validate AI-generated findings and serve as a credible escalation point. A new responsibility is governance of AI-enabled testing, defining when and where AI can be used and what level of human oversight is required. This includes decisions around approved AI/LLM providers, data sensitivity and deployment models, including when local or on-premise LLMs may be necessary.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Forensic Investigator *Forensics Investigation*	• Scanning systems and supporting the retrieval and processing of data from storage and devices • Supporting the extraction, processing and decryption of threat data from affected systems • Correlating and analysing evidence against threat databases and threat intelligence to support classification • Performing attack path and root cause analysis to identify how attackers gained access and moved through affected systems • Discovering new indicators of compromise (IOCs) and tools, techniques and procedures (TTPs) • Drafting investigative reports of findings and conclusions • Updating the threat database from investigation findings • Identifying relevant artefacts, patterns and relationships across large volumes of evidence	• Determining the root cause of security incidents • Distilling the key insights and impact from the evidence • Providing forensic findings to support incident containment and remediation • Documenting attack impact with affected stakeholders • Advising stakeholders on mitigation strategies • Defining investigative scope, questions and hypotheses • Assessing the quality, relevance and context of evidence • Maintaining evidence integrity and chain of custody • Defending investigative conclusions during audits, regulatory reviews or legal proceedings	• Orchestrating AI-assisted investigation across different stages of the investigative workflow • Validating AI-assisted evidence processing and investigative outputs • Recognising hallucinations, errors, biases and limitations in AI-generated findings • Preserving the provenance and integrity of AI-derived evidence • Applying AI securely to forensic analysis where appropriate • Independently verifying AI-generated findings against source evidence • Understanding appropriate AI use cases and when AI should not be relied upon • Protecting the confidentiality, privacy and access controls of forensic data when using AI tools	AI can augment the processing, correlation and analysis of large volumes of digital evidence, enabling forensic investigators to work more efficiently and at greater scale. The investigator continues to require forensic expertise and judgement to examine and interpret evidence, determine root cause, maintain evidential integrity and ensure that investigative findings and conclusions are robust and defensible.
Forensic Investigation Manager *Forensics Investigation*	• Drafting digital-forensic investigation policies and standards • Correlating forensic incident trends and patterns across cases • Mapping the tactics, techniques and procedures used • Consolidating evidence and causal analysis • Drafting investigation and threat-mitigation reports • Synthesising findings across multiple investigations to identify recurring patterns, relationships and pervasive issues	• Setting the forensic investigation strategy • Determining investigative scope, priorities and lines of inquiry • Leading investigations and coordinating forensic teams • Ensuring evidence integrity and determining causal conclusions from analysis • Challenging and validating significant AI-assisted findings against underlying evidence • Presenting findings in legal proceedings and to leadership • Advising senior management on major security risks	• Governing the provenance and integrity of AI-derived forensic evidence • Setting controls for the use of AI in forensic investigations • Monitoring AI performance, bias, accuracy and compliance risks • Assessing and independently validating the reliability and limitations of AI-assisted analysis • Establishing processes for defensible use of AI-derived findings • Managing confidentiality, privacy and access-control risks when forensic evidence is processed using AI	AI can augment the correlation of evidence and incident trends, analysis and preparation of investigation materials, enabling forensic investigation teams to work more efficiently and at greater scale. The manager continues to require forensic expertise and judgement to set investigative direction, evaluate findings, ensure evidential integrity and stand behind conclusions presented to leadership or in legal proceedings. As AI adoption grows, this also includes overseeing the appropriate use of AI in forensic investigations and ensuring AI-assisted findings remain reliable and defensible.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Incident Investigator *Incident Response*	• Collecting, analysing and storing threat intelligence • Analysing past attacks to draw insights • Analysing incident data and drafting incident reports • Scrutinising systems for vulnerabilities • Proposing mitigation techniques and countermeasures	• Exercising judgement during live incident response • Coordinating the recovery of contained incidents • Adapting incident-response techniques to novel or complex situations • Validating AI-recommended containment actions before execution • Recommending measures to strengthen system resilience	• Using AI tools to support incident investigation and response • Assessing the reliability and limitations of AI-generated incident analysis • Validating AI-generated containment and recovery recommendations • Using AI securely when handling sensitive incident and threat data	AI can support threat-information analysis, incident analysis and the development of response recommendations. The investigator continues to require the underlying incident-response competencies to validate AI-generated recommendations, exercise judgement during live incidents and determine appropriate containment and recovery actions.
Incident Investigation Manager *Incident Response*	• Optimising analytics and detection models to identify potentially malicious activities • Drafting contingency and disaster-recovery plans • Consolidating and analysing risks and exposures to support decision-making • Drafting IR policies, standards and processes • Generating threat-analysis inputs for security and design teams • Correlating incident, threat and vulnerability information across multiple sources to identify emerging patterns and systemic risks	• Setting incident-response strategy and standards • Advising senior management on major security risks • Governing threat-intel sharing with partners and law enforcement • Directing remediation and preventive measures to reduce likelihood and impact of future incidents • Making command decisions during high-stakes incidents • Evaluating and approving significant AI-generated response recommendations before operational execution	• Integrating AI-related cybersecurity risks into incident-response strategy • Establishing AI incident-response and vulnerability-disclosure processes • Defining controls for the use of AI in incident analysis and response • Monitoring AI performance, bias, accuracy and compliance risks • Assessing the reliability, limitations and operational risks of AI-generated incident analysis and response recommendations • Overseeing response to incidents involving AI systems	AI can support detection analysis, risk consolidation and the development of contingency and incident-response plans, enabling incident-response activities to be managed more efficiently and at greater scale. The manager continues to require incident-response expertise and judgement to set response direction, direct remediation and make command decisions during major incidents. As AI adoption grows, this also includes overseeing AI-enabled response capabilities and ensuring AI-related scenarios are appropriately addressed in incident-response processes.
Threat Analysis Manager *Threat Analysis*	• Continuously tracking the dark web and other external sources for threats and significant issues • Researching new and existing threats to IT systems according to the organisation's risk profile • Correlating threats against the database to classify them • Running attack simulations (e.g. ASM, BAS) to gauge threat impact • Monitoring and reporting changes in threat tactics	• Assessing and attributing potential attacker groups • Prioritising and rating threats by severity and potential impact • Taking appropriate action according to threat assessment • Assessing hostile intent and providing timely warnings • Exercising judgement to identify novel threats • Advising on security policy and controls for at-risk assets • Producing intelligence reports to document threat analysis, key findings and recommended actions	• Understanding and anticipating adversarial-ML threats and AI-enabled attack scenarios • Identifying AI-generated or manipulated content that may pose a security threat • Assessing the limitations and reliability of AI-generated threat intelligence • Understanding threats to AI models, training data and supply chains, including model poisoning, which could impact AI-supported threat analysis • Understanding AI-related risks and how adversaries can leverage AI across the attack chain to enhance their capabilities (e.g. evade detection or accelerate attacks) • Conceptualising and overseeing agentic orchestration of threat actor profile creation, horizon scanning, etc.	AI increasingly monitors for external threats, identifies and connects potential threats, and runs attack simulations, allowing teams to process much larger volumes of threat information and assess the impact on the organisation based on its risk profile. The role continues to require threat-analysis expertise and judgement to interpret and contextualise threat information, assess attribution, severity and hostile intent, and identify novel threats. Attribution, in particular, requires not only technical analysis, but also an understanding of geopolitical context and adversary tradecraft - areas where AI may not yet perform consistently or reliably.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Senior Security Engineer/ Security Engineer *Security Design and Engineering*	• Drafting security controls in line with guidelines • Documenting system design, operation and outputs • Researching modern security architectures and best practice • Scanning systems for strengths and weaknesses • Automating security infrastructure and processes	• Validating AI-generated designs against production systems • Resolving issues in implementing new security systems • Testing and evaluating new security technologies • Running disaster-recovery drills and simulation tests • Recommending products and procedures to enhance the design	• Implementing security measures to protect AI models • Deploying AI guardrails and moderation controls • Securing generative AI application development • Configuring AI security testing and monitoring • Securing the AI supply chain and development environment • Hardening AI deployment infrastructure and protecting model and data assets	AI can support security analysis, configuration review, research, automation and the development of controls and documentation, enabling security engineers to work more efficiently. The engineer continues to require security engineering expertise and judgement to design and implement effective security measures, resolve implementation issues and ensure that security controls operate as intended in real-world environments. As AI adoption grows, this also includes securing AI systems, models, deployment infrastructure and supply chains.
Security Architect *Security Design and Engineering*	• Drafting architecture diagrams, roadmaps and implementation plans • Analysing current architecture for weaknesses and gaps • Designing standard configurations and patterns • Researching emerging technologies and market trends • Drafting architecture requirements and documentation • Analysing large amount of data from monitoring to proposed risk and gaps from data points and trend	• Designing novel architectures for complex environments • Leading business-architecture governance and standards • Approving exceptions and recommendations to standards • Advising senior management on emerging-technology adoption • Acting as a security expert across application, data and network design • Validating policy exception and proposed control measures from a system-of-systems perspective to determine residual risk	• Developing advanced AI security protocols • Architecting guardrails into AI systems • Governing ethical AI system design • Setting enterprise AI risk-management frameworks • Designing secure-by-design AI systems across the lifecycle • Governing AI supply-chain and deployment-infrastructure security • Architecting SBD with a deep understanding of system boundaries of agentic AI configuration • Ability to understand the intrinsic process and threats invoked by AI	AI can support architecture analysis, research, design development and documentation, enabling security architects to explore options and develop architectures more efficiently. The architect continues to require security architecture expertise and judgement to design secure architectures, address complex requirements, govern standards and make architecture and technology decisions. As AI adoption grows, this also includes designing for the security of AI systems and addressing risks across AI infrastructure and supply chains.

Cyber role	What AI can support *What parts of the existing work can AI augment, perform or significantly accelerate? List is illustrative and non-exhaustive*	What requires human judgement & oversight *What still requires professional judgement, contextual understanding, validation or accountability?*	Additional competencies required in an AI-enabled environment *What does the professional now need to know/do to use AI effectively in this role?*	How the work changes *What is the practical effect on the workflow, such as greater speed, scale, iteration or human-in-the-loop validation?*
Chief Information Security Officer *Executive*	• Gathering, synthesising and correlating security information and threat intel • Performing initial analysis and identifying patterns • Developing scenarios and insights to support risk and remediation prioritisation • Automated compliance monitoring • Drafting cybersecurity strategy, policies and frameworks • Establishing and tracking cybersecurity KPIs and effectiveness metrics • Consolidating cybersecurity risk-assessment frameworks	• Owning the organisation's cybersecurity vision and strategy • Framing the problem, challenging assumptions and conclusions, and contextualising AI-generated analysis • Determining the materiality of risks and findings, setting priorities and deciding where action and resources are required • Providing leadership, building organisational trust, shaping security behaviours and influencing stakeholders • Making risk-based decisions and accepting accountability for residual security risk • Exercising judgement on escalation, communications and acceptable risk during major cyber incidents • Maintaining sufficient cybersecurity depth to recognise when AI-generated analysis may be wrong or incomplete	• Understanding AI-specific cybersecurity risks and controls, assessing their security implications, and critically challenging technical advice • AI-enabled critical thinking and judgement, including the ability to challenge assumptions, identify limitations and uncertainty, and critically assess AI-generated analysis • AI-enabled security assurance, including understanding the coverage, limitations, reliability and effectiveness of AI-enabled security capabilities and where independent validation or human oversight is required • AI supply-chain and concentration-risk management, including understanding dependencies on models, cloud platforms, datasets, APIs and other underlying services • Leading an AI-enabled cybersecurity function, including understanding where AI can appropriately augment threat modelling, vulnerability management, threat hunting, detection, remediation and security operations • Understanding AI lifecycle risk management, translating AI-related cyber risks to business implications, decision-making and trade-offs for senior management • Good understanding of the interaction and relationship between identities, system, cloud and AI to ascertain business risk. Reshaping the dialogue of trust and assurance of system design thinking in association with business risk at board level.	AI can enhance the CISO's ability to oversee complex cybersecurity environments by consolidating risk information, improving situational awareness and informing strategic decisions. The CISO retains intellectual ownership and accountability for cybersecurity analysis and decisions. The CISO increasingly leads a hybrid human-AI cybersecurity function, while contributing to cross-functional AI governance and enabling secure AI adoption. Organisational influence, trust-building and trusted advice to senior management remain critical. The CISO's core mandate remains largely unchanged, but expands to address the cybersecurity implications of AI and oversee its responsible use within the cyber function.

CSA SINGAPORE
Cyber Security Agency of Singapore