GovInsider

SPECIAL REPORTS

Cybersecurity Champions 2025

COMMUNITY PARTNERS:

Republic of Estonia
Information System Authority

MINISTRY OF POST AND TELECOMMUNICATIONS, CAMBODIA

FOREWORD

GovInsider is proud to launch our inaugural Public Sector Cybersecurity Champions report, which features officials at the forefront of the war against cybercriminals.

As the world becomes increasingly digitally connected, the value of data has skyrocketed, with many referring to it as the new oil that fuels the global economy.

A new kind of never-ending war is waged in the shadows: Cyberattacks which attempt to either steal data or disable access for profit or political goals.

If cybercrime were an economy, it would rank as the third largest globally, with its projected costs (due to cyberattacks) to reach US$9.5 trillion (S$12.17 trillion) annually by 2025.

Recently, Interpol dismantled more than 20,000 malicious IP addresses or domains that have been linked to 69 information-stealing malware variants. Around the same time, Singapore took down 1,000 IP addresses that were linked to cybercrime.

These two incidents are just but a sample of the continuous ongoing war against cybercrime.

An increasingly digitalised public sector makes it a juicy target for cybercriminals. According to estimates, the sector is the third most targeted vertical by nation-state actors.

Government cybersecurity experts, often working behind the scenes, are fighting a relentless war against cybercriminals to keep us and our confidential information safe.

Celebrating the champions

To celebrate these heroes without capes, GovInsider has published its inaugural Public Sector Cybersecurity Champions 2025 report.

The report features around two dozen public sector officials from Canada, Germany, Estonia, Singapore, Malaysia, Indonesia, Thailand, Cambodia, Australia and the US.

These champions share their concerns, hopes, and most importantly what they are doing to keep their governments safe.

While priorities and levels of digitalisation differ across the countries covered, the concerns shared remain largely the same, showing how global cyber threats are.

New threat vectors, lack of trained manpower and increasing involvement of organised crime and actors backed by nation-states orchestrating these attacks were some of the top concerns.

Artificial intelligence (AI) is viewed both as a threat and possibly one of the best tools in cyber defence, particularly to bridge the manpower gap with automation.

Another major point comes from the interviews: the passion for the job that all the nominees share, and that they would choose cybersecurity again, given the chance to rewind the clock.

To them, it's not just a career but public service.

Notably, despite significant underrepresentation of women in cybersecurity, they represent more than 50 per cent of those featured, showcasing their growing influence within the field!

We are grateful to all our nominated champions for taking the time to respond to our questions.

We would also like to thank and acknowledge our community partners, Estonia's Information System Authority of Estonia (RIA) and Cambodia's Ministry of Post and Telecommunications (MPTC) for their support in making this report possible.

Meet the Cybersecurity Champions 2025

Click the individual names to access their stories

Australia

- **Lieutenant General Michelle McGuinness,** National Security Coordinator, Department of Home Affairs

Cambodia

- **H.E. Sam Sethserey,** Director General of the General Department of the ICT Department, Ministry of Post and Telecommunications (MPTC)

Canada

- **Joanna Murphy,** Director General, Canada Sovereign Technology Strategy, Chief Technology Office Branch, Shared Services Canada

Estonia

- **Liina Areng,** Director of EU CyberNet, Information System Authority (RIA)

Germany

- **Carsten Meywirth,** Director Cyberdivision, Federal Criminal Police Office (Bundeskriminalamt)

Indonesia

- **Istiqomah,** Head of Cybersecurity Incident Response Team (CSIRT) & Personal Data Protection (PDP), Ministry of Health
- **Wahyu Ahadi Rouzi,** Chief Digital and Information Technology, Indonesia State Electricity Corporation PLN (PT PLN)

INTERPOL

- **Cristiana Nador,** Policy Analyst, Cybercrime Directorate

Malaysia

- **Mohamed Kheirulnaim,** Head of Incident Response and Cyber Threat Intelligence, National Cyber Coordination & Command Centre (NC4), National Cyber Security Agency (NACSA)

Singapore

- **Angela Wu,** Director, Threat Intelligence and Response, Connectivity Cybersecurity & Resilience Group, Infocomm Media Development Authority (IMDA)
- **Beverly Sim,** Senior Manager, Cyber Operations & Technologies, Cyber Security Office, Synapxe
- **Chan Yew Weng,** Agency Chief Information Security Officer (ACISO), National Library Board (NLB)
- **Eric Wong,** Director, Cyber Operations & Technologies, Cyber Security Office, Synapxe
- **Lee Chee Hwan,** Deputy Director, SingHealth CISO Office
- **Leonard Ong,** Director, Sector Governance - Risk & Sector Governance, Synapxe
- **Lim Ee Lin,** Deputy Director, CISO & Governance, Agency Chief Information Security Officer, Home Team Science & Technology Agency (HTX)
- **Dr Liu Yang,** Executive Director, CyberSG R&D Programme Office

Back to top

Meet the Cybersecurity Champions 2025

Click the individual names to access their stories

Singapore

- **Michaela Chua,** Development Programme Manager, Cybersecurity Programme Centre, Defence Science and Technology Agency (DSTA)
- **Syam Gumpalli,** Director, Cyber Risk Management & Services, Cyber Security Office, Synapxe
- **Tan E-Seon Reggie,** Director (Cybersecurity and ICT Governance), Ministry of Home Affairs (MHA)
- **Tan Shui-Min,** Chief Information Technology Officer, National University of Singapore (NUS)

Thailand

- **Amorn Chomchoey,** Secretary-General, Nation Cyber Security Committee, National Cyber Security Agency (NCSA)
- **Saichon Saelee,** Director of Cyber Coordination Department, National Cyber Security Agency (NCSA)

United States

- **Mandy Andress,** Chief Information Security Officer, Elastic

Back to top

Lieutenant General Michelle McGuinness, National Security Coordinator, Department of Home Affairs, Australia

By **Si Ying Thian** | June 26, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

The role of the National Cyber Security Coordinator is to coordinate Australia's strategic response to cyber-security threats, opportunities and challenges.

My office coordinates the whole-of-government response to significant cyber incidents, working closely with operationally independent technical, law enforcement, and regulatory agencies, and coordinating whole of economy consequence management.

I also have responsibility for overseeing the delivery of the 2023-2030 Australian Cyber Security Strategy to help improve Australia's cyber resilience, and drive whole of nation cybersecurity awareness, education and prevention.

2. As we look towards the future of cyber and its impact on national security at a global scale, what does effective security collaboration at an international level look like?

Australia remains deeply invested in building strong international partnerships – an acknowledgment that cybersecurity is borderless. The threats we face, and the opportunities available are shared.

Continued international collaboration is critical as we seek to uphold global cyber standards and together leverage the immense opportunities of secure global commons.

We have refocused Australia's cyber cooperation and capacity building efforts to be more targeted, impactful and sustainable, enabling our partners in the Pacific and Southeast Asia to better prevent cyber incidents and recover quickly when they occur.

Australia is also a founding member of the Counter Ransomware Initiative (CRI) and co-chairs the International Counter Ransomware Task Force with Lithuania. Both efforts demonstrate the importance of international collaboration on the global ransomware challenges.

Our participation in the Quad Senior Cyber Group also demonstrates our commitment to maintaining an Indo-Pacific that is inclusive, resilient and equipped to detect and deter cyberattacks.

Back to top

I see a future where Australia continues to drive global cooperation to develop common standards and effectively prevent, deter and respond to cyber-security challenges, making us all more secure.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the cyber-security scene globally?

Cybercrime is insidious, increasing in scale and sophistication globally.

In Australia, we continue to face a deteriorating cyber threat environment, with the Australian Signals Directorate's Annual Cyber Threat Report 2023-24 advising that a cybercrime is reported every six minutes.

This is consistent with global reporting, which highlight cyber incidents as the top global business risk for the fourth year running.

We are also witnessing an increase in state actors conducting malicious cyber activities. Under the 2023-30 Australian Cyber Security Strategy, Australia will continue to uphold international law and the agreed framework for responsible state behaviour.

We will impose a cost on those responsible for cyber incidents, including making public attributions and imposing sanctions when we have sufficient evidence and it is in our national interests to do so.

4. We are currently watching the emergence of AI-driven cyberwarfare where hackers and professionals are using AI tools for both attack and defend. How can industry and government harness this occurrence to improve their own security measures?

Cybersecurity is a critical thread in almost all aspects of our economy.

AI offers incredible opportunities and great potential to drive economic efficiency, but will almost certainly exacerbate existing and future national security risks.

The Australian Government is providing practical guidance through Voluntary AI Safety Standards, supporting businesses to adopt AI safely and responsibly, as well as continuing to develop mandatory guardrails for the use of AI in high-risk settings.

We are also engaging internationally to ensure the global governance of AI strengthens safe and responsible practices internationally, reflecting our democratic values and respect for human rights.

Wherever technology offers us creative and innovative solutions, we know we need to identify and mitigate new risks. We must ensure our technology is secure by design.

Technology underpins our critical infrastructure and delivers the essential services that are the foundation of our economy, security and sovereignty; while supporting the standard of living we have all come to expect.

5. When looking to improve whole-of-country cybersecurity posture, what has been the biggest vulnerability and how have you responded to this?

As we continue to build our digital economy, we must translate our strong physical culture into a strong cybersecurity culture.

Our 2023-30 Australian Cyber Security Strategy is our foundational national response to cybersecurity uplift and addresses cybersecurity posture across six layers, we call shields.

These shields are focused on: Strong businesses and citizens; Safe technology; World-class threat sharing and block; Protected critical infrastructure; Sovereign capabilities; and Resilient region and global leadership.

There are still things that every Australian can do, to make us all more cyber secure and we continue to invest in these initiatives.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your role in facilitating the Plan B approach and why it is important?

Australia has strong regulation requiring critical infrastructure to maintain cybersecurity incident response plans.

A large part of my role is exercising these plans and collaborating across the economy to ensure we are sharing best practice and lessons learnt.

When the worst happens, we collaborate across the Australian Government to support impacted entities through the provision of a highly coordinated response, seeking to minimise harm and ensure victim entities are resilient & bounce back rapidly.

This includes convening all sectors of the economy required to ensure broader consequences are minimised and harms are mitigated to the greatest extent possible.

7. Looking into the future, what are your hopes for development of the cyber industry?

Developing our cyber workforce and partnering with industry are top priorities.

A key goal under the Strategy, is for Australia to have a flourishing cyber industry.

Only through focused collaboration between industry and government, can we tackle some of the toughest cybersecurity problems and harness the opportunities presented by technologies like AI and quantum computing.

8. Reflecting on your leadership experience across defence and cyber, what advice can you give us?

The rapid pace of change – of both threats and technology – means that cybersecurity must be about collaboration and not competition.

Cybersecurity is national security, economic stability and prosperity. Governments cannot do this alone. Strong and trusted public-private partnerships are critical.

And while we need a sector that is collaborative, creative, innovative, agile and diverse, like most challenges, it also requires strong leadership.

Leaders at every level need to drive informed decisions around priorities, risk and resources. It's also an incredibly demanding field.

We need leaders to not only drive uplift and capability, but to promote the support culture and structures than protect and grow our workforce.

9. Can you explain the importance of professionalising the cyber industry?

Growing and professionalising the cyber industry is critical for building a resilient and trusted digital future.

As cyber threats become more complex, we need a workforce that is not only sufficiently sized but also skilled and accountable.

Australia is making significant investments in growing and professionalising the cybersecurity industry Introducing clear pathways and consistent standards removes barrier and fosters growth of through both horizontal and vertical avenues.

Professionalisation also helps to attract new talent. The new generation of cyber professionals want to know there's a structured and respected career waiting for them, where they can achieve their full potential.

It's the responsibility of both Government and industry to endorse a career in cyber as vital to national security and our way of life.

10. We often see lower numbers of women entering the cyber workforce. How can the cyber community break down barriers to entry to engage more demographics of the population in the workforce globally?

Diversity in the workplace is vital to building a responsive, creative, innovative, and future-ready workforce.

We must ensure the narrative and culture across the cyber field is right. There is nothing inherently exclusive or masculine about cybersecurity and we must ensure that those entering the workforce or looking to change fields understand the pathways available to them, and that all who seek to serve in the field have the opportunity to reach their full potential.

To that end, we are working closely with industry to ensure we can attract, grow and retain a workforce that's not only capable but varied in perspective. This includes increasing employment of women and First Nations people.

H.E. Sam Sethserey, Director General of the General Department of the ICT Department, Ministry of Post and Telecommunications (MPTC), Cambodia

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I am the Director General of the General Department of ICT (GDICT) under the Ministry of Post and Telecommunications (MPTC) of Cambodia. MPTC oversees and regulate the country's Post, Telecom and ICT sector; and support the government in digital transformation.

GDICT is mandated to governance and regulate the ICT sector and promote digital startups, and participate in the implementation of cybersecurity protection for MPTC.

Moreover, GDICT manages CamCERT which acts as a government lead in implementing ICT security strategy and a contact point for handling Cybersecurity incident reported in Cambodia.

GDICT has expanded its capabilities to aligned with "Cambodia Digital Economy and Society Policy Framework 2021-2035", which handles Cybersecurity implementation, Cybersecurity Awareness Campaign, Cybersecurity Protection, Law and Regulation and Policy Frameworks.

2. What kind of cyber threats does your organisation face on a regular basis?

I think every ministries and organisations should be asking themselves this question regularly because as we can see cyber threats are no longer rare events, they are happening every day.

One of the most common attacks is DDoS (Distributed Denial of Service) Attacks which is an attack technique used by attackers to overwhelm online services and take them offline.

In addition, we can see the rise of AI which could enhance phishing attack to trick users to input sensitive information. Another concern is the illegal use of satellite internet services, which serve illegal activities such as online gambling and online scams.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Back to top

There are many threats and challenges in the public sector cybersecurity scene globally.

One of the biggest threats is supply chain attacks because most public sectors rely on third-party software and services, so if a vendor is compromised (e.g., SolarWinds attack), attackers could compromise the entire ICT infrastructure or gain access to critical systems.

Another cyber threat, spear phishing or Business Email Compromise (BEC), is an effective technique used to aim for a specific target within the public sector and with the help of AI makes it very easy to fall into a victim of this kind of attack.

The last one is geopolitical cyberwarfare and disinformation which is used by most nation state adversaries aiming to disrupt, cause chaos, steal secrets, or erode public trust of one's country. For example, we are seeing more operations where attackers breach a system, then leak or manipulate information for political or social influence.

Some key challenges in cybersecurity protection for public sectors include the requirement of significant investment for implementing cybersecurity protection and monitoring, limited user awareness, and inconsistent security standards and information sharing across agencies.

4. What are some of the biggest cybersecurity challenges faced by Cambodia?

Cambodia is currently facing key cybersecurity challenges, notably a shortage of skilled professionals, limited funding and resources, and limited public awareness. We anticipate that the forthcoming Cybersecurity Law will help address these issues.

5. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

We are seeing more and more of AI-driven cyberwarfare. It is a double-edged sword. The scale, speed, and sophistication of both attacks and defences are being transformed. AI can be used as a weapon and a shield in cybersecurity.

From the perspective of attackers, AI has helped them tremendously in launching a sophisticated phishing campaign that can generate convincing phishing emails, texts, or even voice deepfakes that are hyper-personalised using data scraped from social media.

Moreover, AI tools can help attackers to perform automated reconnaissance by scanning and profiling a company's entire attack surface in minutes (something that used to take humans hours or days). More dangerously, AI tools enable even small attacker groups to access advanced capabilities that used to be reserved for nation state adversaries.

On the other hand, I believe Cybersecurity professionals are also levering AI as a powerful defence tool. One important area is the ability to detect threats and monitor anomalies faster and more accurately to identify a potential breach.

For example, in sectors like banking, AI systems are catching abnormal transactions/potential fraud much faster than humans can. At the same time, cybersecurity professionals can design an automated incident response where AI can isolate infected devices, shut down suspicious processes, and notify the right people instantly.

It is also important to mention that AI can identify vulnerabilities in code and help organisations to prioritise what systems are more at risk and which threats are the most likely to be exploited.

The rise of AI-driven cyberwarfare is not speculative; it is already unfolding in practice.

Thus, we should be proactive, act urgently and collaboratively to share knowledge and best practices across the region and globally, and to develop regional or international norms and agreements on AI use in cyber operations, including "red lines".

6. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A team sport in Cybersecurity is very important because let's face it, no organisation, ministry, agency, or business could operate by themselves.

Governments, private companies, infrastructure providers, and even individuals are interconnected, often through shared systems, data, and supply chains. A vulnerability in one sector (e.g. healthcare or energy) can ripple across the entire country, so if one entity does not train, get ready, or does not show up to the game, everyone loses.

We must ensure we can work as a group to come up with a way to share threat intelligence across agencies, find unified response strategies, create common frameworks and standards, have interagency training and exercises.

As cyber threats, such as ransomware, espionage, critical infrastructure attacks, do not respect borders or bureaucracies, it needs everyone's efforts and involvement.

Ranging from private sector (often owns the critical infrastructure), academia and research (innovation, talent development), media (public awareness) to citizens (cyber hygiene and reporting), everyone has a role and responsibility and the more integrated the effort, the stronger the posture.

7. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

The idea of Plan B in Cybersecurity is crucial.

The assumption that a breach is inevitable; not if but when, has become a foundational mindset for modern cyber strategy. One important thing is to have a resilience strategy in place because it is not just about reacting to a breach, but it is about resilience, recovery, and continuity.

It's a part of the strategy that answers: "When the attackers get in, how do we limit damage, respond fast, and keep critical systems alive?". In Cambodia, we have a lot of cross-border cybersecurity collaborations; especially, "JICA project Cyber Resilience Project by JICA, Japan".

Having a strong plan B means we are well prepared by having critical plans in place such as Incident Response Plan (IRP), Business Continuity & Disaster Recovery (BC/DR), Threat Intelligence and Detection, Communication Plan.

Having firewalls, encryption, and strong access controls are important, but just like buildings still have fire exits and evacuation plans despite sprinkler systems, cyber defences need contingency thinking.

Plan B is not failure - it's preparedness. So having a robust, realistic Plan B is not optional, it's essential and it is a strategic asset.

8. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

Probably impossible, a dream scenario: an unlimited budget for cyber defence.

Having layered security architecture such as Zero Trust model and segmentation & micro-segmentation; plus, top-notch security technologies like AI-driven Extended Detection & Response (XDR) platforms that correlate data across endpoints, networks, clouds, and applications is very important.

Moreover, having a strong red team to constantly simulate attacks to find gaps and improve security posture and threat hunting team to actively search for advanced persistent threats.

Lastly, I would spend the budget on hiring elite cybersecurity experts, threat hunters, red teamers, and blue teamers and provide continuous advanced training in threat intelligence, incident response, and offensive tactics.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

The global shortage of qualified cybersecurity professionals is a serious issue.

According to the 2024 ISC2 Cybersecurity Workforce Study, the demand for cybersecurity professionals has surged, resulting in a workforce gap of about 4.8 million unfilled positions. I think one thing we can do about it is to incentivise cybersecurity careers.

Following "Cambodia's pentagonal strategy and Digital Economy and Society Policy Framework 2021-2035", Cybersecurity contains two Sub-Tracks, covering five occupations in Cambodia digital skill development roadmap 2024-2035. This shows the need for cybersecurity in the future, though it can attract more people into the field.

Moreover, the government should encourage students to study cybersecurity/digital skills by providing scholarships and student loans. Second is to continue to expand education and training. Case in point, MPTC will launch Cambodia National Cybersecurity Competition event in May to find the winners and equip them with training and get them ready for ASEAN Round & ASEAN Cyber SEA Game in Thailand.

Cambodia has two universities that provide degree related to Cybersecurity such as American University of Phnom Penh (Cyber Security BSc & Master of Laws in Cybersecurity) and De Montfort University Cambodia (Cyber Security BSc).

In conclusion, we cannot forget about global collaboration and public-private partnerships.

It is essential to have a platform cybersecurity knowledge sharing platform among governments, academia, and private companies to collaborate and share best practices (e.g., ISC2 Cambodia Chapter).

In addition to international training programmes, countries can establish exchange programmes to train cybersecurity professionals across borders (e.g., ASEAN-Japan Cybersecurity Capacity Building Centre - AJCCBC).

GOVINSIDER CYBERSECURITY CHAMPIONS 2025

Joanna Murphy, Director General, Canada Sovereign Technology Strategy, Chief Technology Office Branch, Shared Services Canada

By **Amit Roy Choudhury** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I am responsible for developing a Canadian Sovereign Technology Strategy to foster resilient and secure IT systems and boost made-in-Canada digital capabilities to promote economic growth. The goal of the strategy is to protect Canadian data and intellectual property rights, enabling innovators and researchers to pursue groundbreaking research and production, ultimately delivering Canadian-made solutions.

2. What kind of cyber threats does your organisation face on a regular basis?

Canada faces state-sponsored network attacks that utilise online information campaigns to influence public opinion and target critical infrastructure, pre-positioning for possible future destructive cyber operations. Ransomware is the top cybercrime threat facing Canada's critical infrastructure.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The public sector supports the smooth operations of a country's government. State-sponsored actors seek to disrupt governments. The biggest challenge lies with exploiting human weaknesses (e.g. phishing scams, social engineering), and exploiting vulnerabilities such as unpatched systems or weak passwords.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Absolutely. AI is making it easier for more actors to carry out cyber threat activity. AI is also making cyber threat activities faster and more precise. In the same way, cyber tooling is becoming more sophisticated by using AI to fine-tune orchestration and understand undesirable patterns. AI will also allow us to replace human repetitive tasks in incident response, allowing cyber experts to focus their efforts on treating sophisticated attacks.

5. Cybersecurity is often described as a team sport, whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

In Canada, we have a risk-based, whole-of-government approach to enable a resilient cybersecurity posture and effectively respond to and recover from cyber events on time. Shared Services Canada, the Treasury Board of Canada Secretariat Office of the Chief Information Officer, and the Communications Security Establishment all work together to protect government systems.

This whole-of-government approach is critical because we need to be laser-focused to protect Canadians who rely on public institutions like the Government of Canada to deliver important programmes and services.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

We must always be ready to respond to a breach. It is a certainty, so the job of the cybersecurity professional is to lessen the impact when it happens by adding layers of defence, protecting critical data and systems, and having a robust cyber event response and communication process.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

I would invest in implementing quantum-secure cryptography throughout our network and systems, complete our zero-trust architecture network to minimise attack surfaces and improve threat detection, develop AI-powered systems for threat detection and prediction and AI to streamline incident response - all the while having an eye on building a sovereign Canadian technology stack.

8. What brought you to this profession, and what do you love the most in your job, and what would you like to improve?

My introduction to cybersecurity was in implementing a public key infrastructure in the Government of Canada. I loved the idea that you could use math (cryptography) and technology (key infrastructure) to protect sensitive information and manage risk. What I love most about my job is finding technology solutions to protect Canadians (our democratic institutions, our personal information, and our peaceful lives).

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

AI is transforming the labour market. The World Economic Forum anticipates a net loss of 14 million jobs globally by 2027, with 83 million positions eliminated and 69 million new ones created. There is an opportunity in reskilling and upskilling to help fill the cybersecurity skills shortage.

10. If you had a chance to restart your career from scratch, would you still want to be a cybersecurity professional and why?

Technology has always played a main part in my career journey, whether it was in IT consulting, IT audit, running a cybersecurity programme, or now building a sovereign Canadian technology strategy. Cybersecurity should be and will become a part of everyone's job. If I had a chance to restart my career, I wouldn't change a thing!

Liina Areng, Director of EU CyberNet, Information System Authority (RIA), Estonia

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I am leading EU CyberNet, a project funded by the European Union and implemented by the Estonian Information System Authority.

Project was established five years ago to bridge cyber capacity gaps among EU partner countries while also strengthening EU's own expertise and coordination for providing external capacity building support.

EU CyberNet brings together cybersecurity experts, key organisations and EU initiatives to foster more comprehensive approach to cybersecurity.

2. What kind of cyber threats does your organisation face on a regular basis?

EU CyberNet is, first and foremost, a project dedicated to strengthening the capacities of European Union partner countries to address and respond to the growing spectrum of cyber threats.

From commonplace phishing schemes targeting individuals and organisations to sophisticated, state-sponsored attacks against critical national infrastructure, the range and impact of cyber incidents are expanding rapidly.

Rather than focusing on internal or European challenges, EU CyberNet works externally - sharing expertise, building communities and supporting the development of resilient cyber ecosystems worldwide.

The project mobilises European experts and institutions to assist countries in improving their cyber resilience, whether through policy development, regulatory advisory support or hands-on technical training.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Back to top

Public sector faces, indeed, a multitude of cyber threats. However, the greatest challenges are structural: limited funding often hinders investments into cybersecurity, while reliance on external or third-party providers may increase risks.

Additionally, in an interconnected world a breach here may have a cascading spillover there across governments and sectors.

Addressing these challenges requires sustained investments, stronger public-private collaboration, and a shift towards proactive cybersecurity strategies that puts resilience in priority, threat intelligence sharing and capacity building at all levels.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Of course this is the case. AI-driven cyberwarfare is no longer a distant threat, it is already part of today's threat landscape. We are increasingly witnessing a paradoxal digital battlefield of machine vs machine.

Both attackers and defenders are leveraging AI for automation, efficiency and scale, but AI is only as effective as the humans directing it. At the moment, AI remains a tool not an autonomous force working without human input.

The challenge lies in how to use AI smartly and responsibly, and by the end of day, AI should enhance our defences not replace our critical thinking and strategic guidance.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A wholistic cybersecurity posture is essential because cybersecurity is only as strong and effective as its weakest link. Governments, businesses and society must work together to protect critical infrastructure, public services and digital economy.

Imagine, just a breach in one government agency can compromise an entire government. However, cybersecurity does not recognise borders – neither institutional nor geographical. Threats emerge and spread globally, making national security dependant on international cooperation.

Strengthening cybersecurity requires unified approach at home and close collaboration with international partners, ensuring resilience against threats that no country can tackle alone.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Resilience is the key: prepare and prevent. The real questions is not if a breach happens, but when it happens. The ability to bounce back defines true strength of organisational cybersecurity.

Plan B in this case may even be multiple backup plans to fall back on with clear incident response protocols, reliable backup systems and recovery strategy. Organisations must be ready to detect, contain and recover quickly while minimising damage.

Regular exercises, cross-sectoral and international coordination and learning from past incidents helps to build capacity and resilience when systems are put to test.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

Throwing money at cybersecurity won't guarantee cyber defence. It's about strategy and people, not about getting the latest tools and gadgets.

Technology is important, but without skilled people to manage, understand, analyse and respond, even the best systems money can buy fall into inefficiency.

Cyber resilience starts with human capability: the real challenge is attracting diverse talent, training and retaining skilled professionals, because no amount of funding can instantly create expertise.

Technology matters, but defence is built on skilled people working together. Thus, budgets must be spent smartly for lasting impact.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

Like many Estonians of my generation, my path into cybersecurity was shaped by the 2007 large-scale cyberattacks on Estonia.

At the time, I was starting as a diplomat in NATO, and my portfolio unexpectedly expanded to include a "cyber package". That twist of fate turned into a wonderful career opportunity, as I was fortunate to contribute to the development of NATO's first-ever cyber defence policy.

Once you enter this field, it's hard to leave. Cybersecurity is exciting, complex, constantly evolving and never boring, offers continuous opportunities to learn and develop.

What I particularly love about my job is internationality. Through helping to build cyber capacity, you get to appreciate vastly different experiences, pathfinders and enthusiastic leaders, countries that are leapfrogging in their digital development.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Addressing global shortage of qualified labour requires both short- and long-term solutions.

In the short term, upskilling and reskilling professionals from related fields and professions can help fill critical gaps. Long-term success, on the other hand, depends on the education system, especially early education.

Digitally aware citizens can be raised by putting focus on digital skills and integrating cyber matters into curricula as well as supporting hobby education like coding club, robotics or cyber competitions.

These can spark interest and help to identify talent early. Importantly, we must take conscious effort to engage girls and women – by providing relatable role models, suitable learning environments and targeted campaigns – to ensure that we include full potential of our collective talent, including the other 50 per cent of the brain pool.

Developing strong cyber workforce requires continuous learning opportunities and a culture that encourages curiosity and problem-solving from a young age.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

I have always wanted to be a doctor - saving lives - but I'm not emotionally strong enough for that kind of heroism. So instead, I ended up in cybersecurity - where I may not save lives, but I like to think I help change them. It's digital first aid :)

Carsten Meywirth, Director Cyberdivision, Federal Criminal Police Office (Bundeskriminalamt), Germany

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I'm the Head of the Cybercrime department with the rank of a Director at the German Federal Criminal Police Office.

We conduct our own investigations, work closely with the police authorities of the German federal states and coordinate the national and international cooperation of the German criminal investigation offices.

2. What kind of cyber threats does your organisation face on a regular basis?

We focus on the prosecution of serious cybercrimes directed against information technology systems, but also target the administrators of criminal trading platforms on the internet and the darknet.

Our aim is to identify and arrest the criminals. Along the way, we deprive them of their digital infrastructures and assets, secure evidence and help to prevent further crimes from succeeding.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Within the scope of our responsibilities, ransomware attacks regularly cause the greatest damage to victims.

Ransoms are calculated on the basis of the presumed or scouted ability to pay and initially appear to be a more attractive option in view of the sometimes massive loss of business and revenue.

Unfortunately, however, this is sometimes followed by further extortion, sometimes under threat of the publication of previously leaked confidential data. Phishing remains one of the main attack vectors for more serious crimes.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI tools also enable attackers to create more convincing spam emails or to carry out much more far-reaching fraudulent activities.

Everyone needs to be aware of these risks, which is why broad awareness campaigns at all levels seem sensible.

At the same time, AI also offers great potential for both law enforcement and the detection of anomalies in IT systems, which should be leveraged.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

Cybersecurity is definitely a task for society as a whole. The private and public sectors must work together as closely as possible and make their contributions. This was critical to the success of many of our operations.

Comprehensive, self-responsible prevention should also be part of any cybersecurity strategy. And above all, cybercrime is almost always international. Perpetrators, victims and the infrastructures that connect them are often spread across continents.

That's why we rely on close cooperation with our partners around the world.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Preparation is mandatory.

Every organisation should have clearly structured, carefully reviewed and continuously updated crisis plans. This starts with simple questions about who can be contacted and who is responsible in the event of possible cyber incidents.

In Germany, we have set up specialised central cybercrime contact points of the German police for companies, which we believe is a success story.

And, of course, everyone should make regular backups of their important data.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

We are not dreaming the dream of unlimited resources, because every nation must use taxpayers' money responsibly.

Of course, human resources are a bottleneck as we would like to be able to run more investigations in parallel.

On the other hand, non-monetary resources such as legal options can also be very valuable for law enforcement authorities.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I became a police officer out of deep conviction and passion, because I want to make a contribution to our constitutional state. This is still enormously fulfilling for me. I can't imagine a better job.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

We rely heavily on our own training and knowledge management in order to multiply the outstanding skills that can be found in our ranks as comprehensively as possible.

Our team is made up of people who are passionate about what they do and this intrinsic motivation can move mountains.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Yes, as I can't imagine a more exciting and dynamic sector.

Istiqomah, Head of Cybersecurity Incident Response Team (CSIRT) & Personal Data Protection (PDP), Ministry of Health, Indonesia

By **Mochamad Azhar** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As Head of the Cybersecurity Incident Response Team (CSIRT) and Personal Data Protection (PDP), I collaborate with the infrastructure team to manage cybersecurity for systems within the Ministry of Health environment.

This team is supported by a Security Operations Centre (SOC) that continuously monitors cybersecurity 24 hours a day.

This team is under the Centre for Data and Information Technology (Pusdatin) and acts as the coordinator for cybersecurity management within the Ministry of Health and the healthcare sector.

Pusdatin also coordinates with the National Cybersecurity Agency (BSSN), the National Intelligence Agency (BIN), and the Ministry of Communication and Digital Affairs (Komdigi) in managing and enhancing cybersecurity capabilities.

2. What kind of cyber threats does your organisation face on a regular basis?

In the past year, the most common cyber threats to the Ministry of Health environment were malware infections (69.6 per cent), data leaks (26.6 per cent), and defacement (1.9 per cent).

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The biggest threats and challenges in cybersecurity are social engineering, which are attacks that exploit human weaknesses.

Humans are the weakest link in cybersecurity. Human negligence and lack of awareness can open security gaps in even the most robust defence systems. This is especially true in the public sector, which prioritises public service.

Back to top

Another challenge is balancing the convenience of public services with the fulfilment of security standards. In some cases, security measures are perceived as slowing down and complicating service processes.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI is an evolving technology that can be positive when used properly. Conversely, AI can also be negative when used for malicious purposes.

Both hackers and security professionals can utilise AI technology. In its implementation, the use of AI requires ethical guidelines to ensure that it is used responsibly for the common good and does not harm others.

The Ministry can incorporate these ethical guidelines into regulations aimed at ensuring that AI is used properly, beneficially, and does not harm others.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

It is very important to have an ideal cybersecurity posture. We must know what strengths we have, both in terms of policy and controls established in several aspects related to security to protect data and information assets.

The stronger the cybersecurity posture, the more prepared we will be to face cybersecurity threats.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Zero trust is a security approach that assumes that nothing is inherently secure by default. Everything has potential risks that must be managed, both before and during an incident.

We must start by identifying potential risks and incidents that may arise from the assets we manage. Next, we must develop a mitigation plan in the event of a security incident, considering various situations and conditions, and simulate them so that when an incident does occur, services do not come to a complete halt, and we can minimise the resulting losses.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

In addition to purchasing the latest and best technology tools, it is equally important to invest in people, whether they are security managers, application managers, or users.

No matter how advanced the security tools are, they still require humans with strong analytical skills and sensitivity to manage security. The same applies to applications supported by strict security systems. If users lack understanding in maintaining access and protecting their assets, then security defences may be rendered ineffective.

Therefore, in addition to purchasing the most advanced technology, unlimited budgets will also be used to enhance the capabilities of security managers and increase awareness among application users.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

Security is an effort to protect what is valuable not only for oneself but also for others. Maintaining security means safeguarding the interests of many parties.

Equally important is how we can help others understand the importance of protecting data from potential cyber threats. Because even the slightest negligence can potentially lead to significant threats.

The skills I want to improve further are identifying and mitigating potential risks (risk management), as well as advocating and raising awareness about information and cybersecurity.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

In the face of increasing threats, coordination with other cyber incident response agencies and the establishment of a cybersecurity communication forum comprising experts and practitioners are essential for exchanging experiences. Experience is the easiest knowledge to learn and can be directly implemented.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Yes. Because managing cybersecurity indirectly also safeguards data security. In the healthcare field, data is extremely important, so safeguarding data means we are helping to protect patient safety.

GOVINSIDER CYBERSECURITY CHAMPIONS 2025

Wahyu Ahadi Rouzi, Chief of Digital & Information Technology, Indonesia State Electricity Corporation PLN (PT PLN), Indonesia

By **Mochamad Azhar** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As Chief Digital & Information Technology at State Electricity Company (PT PLN), I am responsible for the strategy and operations of information technology systems to support electricity supply throughout Indonesia.

This includes developing a five-year Information Technology Master Plan (ITMP), creating applications, purchasing laptops, and securing information technology systems, which within our organisation is more commonly referred to as "kamsiber" (an abbreviation for cybersecurity).

This responsibility requires me to ensure that the national electricity system operates efficiently, reliably, and is protected from cyber threats. Furthermore, under Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure, the electricity sector is classified as the most critical sector, as failures in the electricity sector can lead to systemic failures in other sectors.

2. What kind of cyber threats does your organisation face on a regular basis?

Based on data from our Security Operations Centre (SOC), active and passive scanning often ranks first among cybersecurity events. Although these cybersecurity events do not necessarily pose a threat, they could be reconnaissance, which is the first step in a cyberattack.

Phishing attacks and human error are the most common threats we encounter. It cannot be denied that the weakness of all systems lies in human factors, so human-driven threats will always pose a threat to cybersecurity over time.

Are there other types of threats at PLN?

Of course, for a company of PLN's scale, there are always individuals who attempt to launch ransomware attacks, DDoS (Distributed Denial of Service) attacks, exploit vulnerabilities, leak data, and steal identities. However, in terms of numbers, these are still outweighed by phishing attacks.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Cybersecurity in the public sector faces two main challenges, not only in Indonesia but worldwide.

From external sources: 1) The increasing number of attacks based on AI, which makes attacks more sophisticated and increasingly difficult to detect; 2) The computational capacity of quantum computing, which threatens current encryption technology like a child's toy that can be easily cracked in minutes.

From internal sources: 1) The difficulty of eliminating dependence on legacy systems, which often lack modern security features; 2) The paradigm of an organisation or company that views cybersecurity as a cost rather than an investment in risk mitigation.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

It is undeniable that the use of AI in the cybersecurity landscape is increasing, with hackers using AI to automate the search for security gaps and exploit vulnerabilities, including deepfakes to increase the success of phishing attacks.

If hackers are using AI, then defence mechanisms must also be equipped with AI, such as the use of Extended Detection & Response (XDR) systems to detect network anomalies based on activity, including other methods such as Zero-Trust Network Architecture (ZTNA) and User and Entity Behaviour Analytics (UEBA).

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

PLN can be divided into at least four major business processes: power generation, transmission, distribution, and retail. Power generation in western Java can only be felt by people in Bali if there is good teamwork between these four business processes to distribute electricity, ensure a stable load, and deliver it to customers.

With such a long supply chain, only teamwork can ensure the electricity system operates smoothly.

The same applies to a country, but on a much larger scale. For instance, vulnerabilities in the electricity sector can lead to disruptions in economic, social, educational, and even health activities in a region. Therefore, a mature national cybersecurity posture is of utmost importance.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

No system is 100 per cent secure. With this in mind, planning aspects ranging from mitigation to remediation become important. Mitigation efforts include security-by-design system planning, application security testing, and the use of security devices for detection and prevention.

Almost all cybersecurity solutions offered serve to mitigate cyber incidents. However, if a network breach has occurred, it falls under the category of an incident (even a critical incident), which requires remediation efforts.

One of the most effective methods is system recovery from backups. However, it is not limited to recovery from backups but also includes the Business Continuity Plan (BCP) that each organisation has defined.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

Interesting question. Of course, I would equip the entire office network and all employee endpoints (work devices) with the latest AI-based solution to detect suspicious activity with all features enabled, along with an automated response system.

Trend-wise, this solution can reduce the risk of cyberattacks by up to 85 per cent. If outside the system, it is mandatory to provide comprehensive cybersecurity training or certification to all employees, as well as explore subscribing to cyber insurance for PLN and all our subsidiaries.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I started my career long before cybersecurity became a major issue. However, as times have changed, cybersecurity has become a crucial factor for business continuity and even national security, especially in the electricity sector.

What I enjoy most about this work is the challenge of continuously evolving to respond to evolving threats. I aim to continuously enhance the resilience and reliability of systems at PLN to remain relevant and robust in the face of threats and negative abuse cases.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Increasing the number of employees who have received formal education and certification related to cybersecurity is a major driving force. In addition, the development of cybersecurity communities also plays an important role in building capacity and knowledge informally.

Policy, investment, and research are also key determinants, making collaboration between the government, industry, academia, and cybersecurity service providers crucial.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

If my career were to start over from the beginning, it seems that the demands of the times would likely lead me down this same path. Cybersecurity is not only a rapidly growing field but also has a significant impact on business and national resilience. Its dynamic challenges make this work consistently intriguing, and I wish to continue contributing to building a stronger digital defence.

Cristiana Nador, Policy Analyst, Cybercrime Directorate, INTERPOL

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I serve as a Policy Analyst at INTERPOL's Cybercrime Directorate, where I support strategic initiatives that guide global efforts to combat both cyber-dependent and cyber-enabled crime.

My role blends operational coordination, institutional strategy, and multilateral engagement. I contribute to shaping INTERPOL's global narrative on cybercrime, advising on international frameworks, and building cross-sectoral partnerships.

For those less familiar with INTERPOL, we are the world's largest international police organisation, connecting law enforcement agencies from 196 member countries through secure channels to share intelligence, coordinate operations, and combat transnational crime.

As we mark our 102nd anniversary, we look forward to continuing this mission for many years to come.

2. What kind of cyber threats does your organisation face on a regular basis?

We work with a vast array of threats ranging from cyber-dependent crimes - like malware campaigns, DDoS attacks, and ransomware - to cyber-enabled crimes, including human trafficking, financial fraud, and environmental crimes facilitated through digital means.

INTERPOL regularly detects and addresses coordinated cyber operations focused on the most pressing cyberthreats targeting member countries.

We respond to these challenges by mobilising intelligence through the I-24/7 network, coordinating multi-country operations, and collaborating with partners across law enforcement, the private sector, and international organisations.

Our work is grounded in trusted, sustained collaboration with industry actors - who provide essential threat information as well as technical insight - and multilateral partners, civil society, and academia, helping to turn critical cyber intelligence into operational impact.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Phishing and Business Email Compromise continue to be top entry points for attacks, now amplified by AI.

The emergence of Phishing-as-a-Service and deepfake-driven scams make it harder for public institutions to defend against deception at scale.

Cyberattacks on public infrastructure also remain a major concern, especially in regions with low cyber resilience. The real challenge lies in turning threat intelligence into action and bridging the trust gap - both across sectors and between countries with varying levels of cyber maturity.

This is where partnerships like those fostered through mechanisms like the Cyber Atlas and the Open-ended Working Group on the security and use of ICTs play a crucial role in building shared situational awareness and collective response.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI is not a new battlefield - it is a magnifier. It enhances the precision, scale, and efficiency of cyberattacks, but also equips defenders with predictive tools.

At INTERPOL, we focus on how AI is enabling known threats to evolve: sextortion scams are growing through synthetic images; ransomware variants are spreading faster; and phishing campaigns are more tailored than ever.

We are developing new projects to address AI-driven threats, with an emphasis on crimes that disproportionately affect vulnerable populations. This includes efforts to embed gender-responsive approaches and human rights safeguards into prevention and enforcement.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

The cyber threat landscape is inherently transnational, requiring a whole-of-globe approach.

INTERPOL promotes this through secure communication tools like the I-24/7 network, international legal frameworks such as the Budapest Convention and the UN Convention against Cybercrime, and strong alliances between law enforcement and the private sector.

At the same time, we recognise the importance of regional identities and how they shape cooperation and policing practices. That's why we operate through a desk model - embedding local officers who serve as vital connectors between global strategy and regional realities.

Public-private cooperation is indispensable. Partnerships with cybersecurity firms, infrastructure operators, platform providers, and policy networks like the World Economic Forum and the Paris Peace Forum offer not only technical knowledge but also early warning capabilities and broader visibility into emerging threats.

True resilience requires inclusive, interoperable, and sustained partnerships across borders and sectors.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Resilience begins before a breach. A robust Plan B means investing in segmentation, preserving critical functions, and planning communications. It also means being able to quickly engage with trusted partners - national and international - for technical support, legal guidance, and public messaging.

Through INTERPOL-coordinated operations, we've seen that the speed of response and strength of cross-border collaboration often determine whether a breach is swiftly contained or spirals into a broader crisis.

In this context, our partnerships under the Gateway Initiative play a vital role, improving the effectiveness of cyber operations and investigations.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

I would prioritise capacity building in underserved regions, ensuring equitable access not only to forensic tools and intelligence-sharing platforms but, critically, to sustained cyber training.

Providing tools without the training to use them effectively has repeatedly proven insufficient - skills development must be at the core of any long-term strategy.

I would also expand the scope of public–private partnerships to develop real-time detection systems and invest in secure-by-design infrastructure that anticipates both cyber-dependent and cyber-enabled threats.

We welcome collaboration with partners who share these goals and are interested in co-developing impactful, forward-looking projects with us. If you're one of them, reach us out to CD.FIND@interpol.int

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

With a foundation in political science, law, and international security, I was drawn to cybercrime because it is where global governance, human rights, and law enforcement intersect in real time.

What I love most is the collaborative spirit: working with cyber investigators one day and advising multilateral negotiations the next.

I would like to see more integration of environmental lenses into cyber policy work, and stronger recognition of how digital threats intersect with broader public safety and development agendas.

As future conflicts are increasingly shaped by access to natural resources, and as we rely more heavily on technology to monitor and secure them, the potential impact of cyberattacks on environmental systems and human security becomes even more critical.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

We must redefine what a cybersecurity professional looks like. This means opening the field to diverse disciplines, breaking down stereotypes, and removing structural barriers for women and marginalised communities.

Initiatives that combine education, mentorship, and international cooperation - like those supported under the INTERPOL Global Cybercrime Expert Group - are key to expanding the talent pipeline in meaningful, inclusive ways.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Yes - because cybersecurity today is about more than technology. It's about diplomacy, justice, and protecting fundamental rights in an increasingly digital society. It's about understanding risk, building resilience, and shaping the future of safety in ways that matter for people and planet alike.

That said, my plan B would probably involve becoming a yoga instructor on an eco-conscious farm in rural Iceland. Still focused on peace and balance, just through a different kind of firewall.

Mohamed Kheirulnaim, Head of Incident Response and Cyber Threat Intelligence, National Cyber Coordination & Command Centre (NC4), National Cyber Security Agency (NACSA), Malaysia

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As Senior Assistant Director at the National Cyber Coordination and Command Centre (NC4), National Cyber Security Agency (NACSA) Malaysia, I oversee a multidisciplinary team that collects, analyses and disseminates cyber threat intelligence for both government bodies and national critical information infrastructure (NCII) entities.

We draw upon internal and external sources to convert raw information into actionable insights, guiding national early-warning systems, incident response and strategic planning.

NC4 itself functions as the country's nerve centre for cyber coordination: we maintain 24/7 situational awareness of high-impact events and facilitate seamless collaboration between agencies under NACSA's mandate stated in Cyber Security Act 2024 to protect Malaysia's cyberspace.

2. Which broad categories of cyber threats (e.g. nation-state, organised cybercrime, insider risk) does NACSA prioritise in its strategic planning, and how does that inform your threat-assessment framework?

We view adversaries as three overarching groups: sophisticated nation-state actors whose stealthy operations often target strategic assets; organised cybercrime syndicates focused on financial gain through ransomware campaigns, data exfiltration and fraud; and insider or opportunistic threats ranging from well-meaning but negligent staff to "script kiddies".

By mapping each category against our established risk framework, we ensure that the characteristic tactics, techniques and procedures of each group inform our priority settings, intelligence-collection requirements and the allocation of defensive resources.

Back to top

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Globally, the public sector grapples with the vulnerability of ageing systems that struggle to meet evolving security demands, resource constraints in terms of skilled personnel and research budgets that hamper proactive resilience measures, and entrenched inter-agency silos that impede rapid information-sharing and coordinated response.

Overcoming these challenges demands concerted efforts to modernise technology platforms, reform governance structures to incentivise collaboration, and establish interoperable channels for threat intelligence exchange.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI in cyber operations presents a double-edged sword: adversaries can harness machine-speed automation for phishing, deep-fake social engineering and adaptive malware, while defenders leverage AI-enabled anomaly detection, predictive modelling and autonomous triage to distinguish genuine threats from background noise.

In the coming years, I expect AI-vs-AI confrontations to become the norm, pitting our algorithmic defences against adversarial-learning techniques.

Success will depend on robust AI governance, continuous validation of our models and a steadfast commitment to staying ahead of malicious innovations.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A unified posture is indispensable because cyber adversaries do not respect bureaucratic boundaries nor the lines drawn on a map.

By adopting a Whole-of-Nation (WoN) approach, we guarantee seamless incident response, consistent enforcement of policies and centralised fusion of threat intelligence.

Through shared standards, a joint situational-awareness platform and collaborative exercises, we eliminate blind spots, accelerate decision-making and raise the operational cost for any actor seeking to exploit gaps between agencies.

6. How does Malaysia's resilience strategy ensure continuity of critical services in the event of a major cyber incident, without compromising operational security?

Malaysia's resilience strategy ensures continuity of critical services through proactive coordinated national planning, sector-specific code of practice, and business continuity practices to address potential service disruptions.

It prioritises organisational readiness via layered defences and isolated redundancies, while strategic-level crisis simulations with key sectors test coordination and decision-making without disclosing sensitive operational details.

This approach safeguards essential functions while maintaining operational security and institutional trust.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

My foremost investment would be in people rather than platforms. Trust doesn't begin in boardrooms; it's built when the right people are empowered to grow, lead, and stay committed.

It begins when talented individuals with integrity choose to stay and grow as knowledge especially tacit knowledge is the most valuable asset for a country.

I would therefore prioritise recruiting and nurturing individuals of exceptional aptitude and dedication, focusing on quality over quantity through specialised fellowships, mentorship schemes and bespoke simulation academies.

Talent in cybersecurity is not like building Lego bricks, where parts can be interchangeable; it's more like assembling Gunpla; every piece has its unique fitting, and the Gundam model kit cannot stand tall if the leg has yet to be assembled.

Only after we have established this cadre of world-class cyber defenders with great tacid knowledge would I allocate resources to next-generation telemetry, advanced AI/ML research and initiatives to strengthen our technology sovereignty.

After all, the most sophisticated tools are powerless in unprepared hands.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

In the public service, it's common that we don't get to choose our specialisation. Our postings depend on agency needs and available vacancies.

I found myself assigned to the cybersecurity domain early in my government career and have since learnt a variety of tradecraft, from incident response to threat actor profiling. Over the years, I gravitated towards threat intelligence because I discovered a genuine passion for uncovering adversaries' methods and translating those findings into protective measures.

What I enjoy most is the combination of technical challenge and public-service purpose; each investigation feels like a complex puzzle that directly contributes to national cyber resilience.

Moving forward, I aim to improve my ability to communicate these technical insights at the executive level, ensuring that our strategic recommendations resonate with policymakers and secure the resources needed to stay ahead of emerging threats.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Addressing the talent gap demands incorporating general cybersecurity awareness and foundational concepts into STEM education policies from secondary education onwards to build a future pipeline.

It also requires forging public-private partnerships that offer graduates hands-on rotations in security operations centres, and delivering modular, on-demand certifications to upskill mid-career IT professionals, enabling them to pivot into cybersecurity roles without restarting their careers entirely.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Honestly, probably not! *laugh*.

The adrenaline rush that comes with tracking threat activity in real time at three in the morning is unparalleled, but every time I walk past my PS5 and see it gathering dust, I'm reminded that life's too short not to finish the latest exclusive!

Nonetheless, knowing what I know now, I'd still choose a field that never sleeps, just so I could put off hunting Arch-Tempered Rey Dau in Monster Hunter: Wilds for a little less time.

Angela Wu, Director, Threat Intelligence and Response, Connectivity Cybersecurity & Resilience Group, Infocomm Media Development Authority (IMDA), Singapore

By **Amit Roy Choudhury** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the Head of Department for the Threat Intelligence and Response (TIR) division at the Infocomm Media Development Authority (IMDA), I oversee three teams: Cyber Threat Intelligence, Digital Forensics & Incident Response, and Security Engineering.

My team's primary focus is on protecting Singapore's Infocomm & Media sector from cybersecurity threats. We serve as the frontline defence, working with operators to prevent and mitigate these potential cyber threats.

2. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing, and identity theft) in the public sector cybersecurity scene globally?

Based on our observations, there are some trends relevant to the Infocomm & Media sector:

- Attacks targeting network infrastructure devices such as firewalls, routers, and virtual private network systems. These attacks often exploit system flaws – including zero-day vulnerabilities – to gain full access or establish persistent backdoors. As these are proprietary systems, standard cybersecurity operations teams face significant difficulties in detecting potential compromises as they cannot effectively run traditional malware indicators of compromise searches or deploy standard Endpoint Detection Response (EDR) solutions.

- Threats against central management platforms that handle virtual machines. These platforms often suffer from multiple vulnerabilities: inadequate network segregation, weak privileged access management, lack of EDR capabilities, and susceptibility to both known vulnerabilities and zero-day attacks. When these platforms are compromised, threat actors can move laterally

between virtual machines managed on the same platform.

- Ransomware and DDoS (Distributed Denial of Service) attacks. Organisations that haven't properly deployed and configured EDR systems are particularly vulnerable to ransomware attacks. For DDoS attacks, while implementing countermeasures are crucial, it's equally important to proactively test at-risk systems to ensure they can withstand such attacks.

3. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI technology is being leveraged by threat actors in several concerning ways.

AI-powered tools are now capable of generating massive volumes of sophisticated phishing content. These are not the obvious, error-riddled phishing attempts of the past — instead, they are grammatically perfect, unique, and highly convincing messages.

Additionally, we're seeing an increase in deepfake videos being deployed in scam operations, with AI making these increasingly difficult to distinguish from genuine content. These AI-generated materials are often used as vehicles for malware delivery.

Given that these attacks typically target large numbers of individual email accounts, organisations need to implement a two-pronged approach. First, there must be regular employee awareness and education about these evolving threats. Second, organisations need to develop and maintain robust process controls that can effectively validate authorised requests and prevent fraudulent transactions.

One effective mitigation strategy we've identified is proactive communication. When organisations promptly notify their customers about emerging threats and publish details of current phishing attempts and scams on their corporate websites, it significantly helps reduce the potential impact on both customers and suppliers.

4. What brought you to this profession and what do you love the most in your job and what would you like to improve?

My journey into cybersecurity was driven by a deep fascination with the constantly evolving nature of cyber threats. What drew me to this field was the challenge of developing and implementing preventive measures against new and emerging risks, as well as finding ways to address the potential impacts of these attacks.

What I find most fulfilling in my role is the opportunity to design and deploy preventive measures and detection systems that effectively counter high-risk threats. I enjoy the challenge of implementing security solutions that maintain their effectiveness while having minimal operational impact on our customers' day-to-day operations. This balance between security and usability is crucial in our field.

Looking ahead, I see one key area for improvement in our industry: the need for better information sharing and collaboration. I hope to see organisations become more open to sharing their experiences with cyber incidents and threats. Currently, there's often hesitation or reluctance to discuss security incidents due to fear or shame.

However, if organisations could overcome these barriers and collaborate more openly with other organisations and government agencies, it would create valuable learning opportunities for the entire cybersecurity community. Such sharing of lessons learned could help other organisations implement more effective preventive measures and reduce their risk of experiencing similar incidents.

5. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Yes, I would still choose to be a cybersecurity professional. I find genuine enjoyment in studying and countering the evolving nature of threats targeting internet connected or standalone devices — as long it contains a processor.

What makes cybersecurity particularly appealing is its versatility as a career. Since organisations worldwide use similar brands, systems, hardware, and software, the skills are highly transferable across different sectors. The main difference lies in how security incidents impact different organisations and their customers differently, which has allowed me to build a lifelong career where I can continuously learn and apply my knowledge across multiple countries and contexts.

Beverly Sim, Senior Manager, Cyber Operations & Technologies, Cyber Security Office, Synapxe, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As Singapore's national HealthTech agency, Synapxe creates intelligent technological solutions to improve the health of millions of people in Singapore. Within Synapxe, I lead the Proactive Threat Defence team under the Cyber Security Office.

We provide early warning to public healthcare on cyber threats and take proactive measures to strengthen our cybersecurity posture.

This includes strategic threat analysis, examining phishing attacks within the sector, and alerting on potential vectors of attack to support the fine-tuning of defences.

2. What kind of cyber threats does your organisation face on a regular basis?

Healthcare organisations across the globe are considered soft cyberattack targets due to their high public visibility, significant reliance on technology and data, use of legacy systems, as well as limited resources and focus on patient care.

Singapore's public healthcare institutions (PHIs) are similarly considered attractive targets for cyber espionage, cybercriminals, and other threats, including advanced phishing techniques, impersonation, ransomware and supply chain vulnerabilities.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Supply chain attacks pose a significant threat to the public sector due to the reliance on a diverse range of third-party vendors and cloud service providers.

Attackers exploit the trust relationships between organisations and their vendors, targeting vulnerabilities in these external entities to gain access to networks.

Back to top

The challenge with maintaining visibility and control over the security practices of all third-party vendors also exacerbates the threat posed by supply chain attacks.

In addition, identity theft has grown significantly with the widespread use of info stealers, Adversary-in-the-Middle (AitM) attacks, as well as quishing (QR code phishing) attacks to trick users into providing their credentials.

Many successful breaches in the last year have been from the misuse of stolen credentials to gain access into victim networks.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Cyberwarfare has traditionally depended on human-driven attacks, characterised by small but highly technical teams manually crafting malicious code, exploiting vulnerabilities, and conducting reconnaissance.

However, we have entered an era of AI-driven cyberwarfare, where AI acts as a force multiplier — both in offence and defence.

Threat actors are increasingly harnessing the power of AI to scale their attacks. In dark web forums, cybercriminals are exchanging knowledge on how to exploit legitimate LLMs like ChatGPT to distribute malicious content.

These attackers are using LLMs to generate highly personalised phishing content with remarkable accuracy using just a few prompts.

Additionally, AI is enabling the automation of vulnerability discovery and exploitation, and it helps simulate human behaviour to bypass authentication or outsmart security systems.

On the defensive front, AI has become essential to any reputable cybersecurity solution.

It plays a crucial role in threat and anomaly detection, enabling real-time identification of anomalies across large volumes of logs and network traffic. Notable blue team experts have also leveraged LLMs to develop plugins, such as DFIR-GPT (by Josh Lemon) and Cybersecurity Guardian.

These plugins, built on top of ChatGPT, are specially targeted to provide blue team members with accurate technical advice in Digital Forensics and Incident Response (DFIR).

5. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

In public healthcare, while investing heavily in a "defence-in-depth" strategy, we are also highly cognisant of the need to plan for any potential breach of our networks.

To instil confidence in the sector's ability to safely and effectively continue delivering core services during breach resolution, our plans go beyond technical recovery; it also focuses on resilience and mission continuity as well.

Such a plan needs to encompass all facets of an entity including IT, cyber, business units, corporate communications, operations, management and clinical staff.

It needs to incorporate business continuity plans at every level, for example, in healthcare, from determining what clinicians need to maintain patient care to bringing up backup systems that can continue to support operations.

Furthermore, it is important to include internal and external communication, as well as coordination throughout the entity during the incident. We take our plans seriously and conduct regular exercises with key stakeholders in public healthcare.

6. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

An unlimited budget for cyber defence is unlikely and should not be anticipated.

To build a strong cyber defence programme, it is important to first invest in the right people – those who possess strong technical skills in the cyber domain and a commitment to integrity.

I believe it is important to speak truth to power, highlight blind spots, call out underinvestment in areas with gaps, and raise alarms about issues that put the organisation at risk.

With the right people, we would then be able to allocate our budget wisely to focus on the areas that matter most to the organisation.

7. What brought you to this profession and what do you love the most in your job and what would you like to improve?

Stuxnet, a sophisticated computer worm discovered in 2010, was when I witnessed for the first time how cyber threats in the digital realm could manifest as tangible real-world impact. This intersection of technology, strategy, and national security was fascinating and alarming.

Since then, the rapid digitalisation of networks across various industries, including initiatives like Smart Nation Singapore, Smart Health, and the extension of remote healthcare monitoring solutions to homes, has spurred innovation while simultaneously heightened risks.

This evolution has led to a growing demand for cybersecurity professionals.

What I love the most about my job is the opportunity to collaborate with the cybersecurity professionals at Synapxe, who bring diverse backgrounds and varied experiences to the table.

The moments when we unite to brainstorm ways to tackle cybersecurity challenges not only inspire me but also reinforce my commitment to our shared mission, even in the face of adversity.

Communication, collaboration and cross-functional sharing between the cybersecurity teams in Synapxe and our stakeholders across public healthcare is crucial to achieving strong cybersecurity.

By enhancing communication and collaboration, we can build the trust that is essential to assure our stakeholders that cybersecurity is an enabler rather than a barrier to business.

Establishing this trust and mutual understanding during peacetime will be invaluable when we encounter different situations at work.

8. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Cybersecurity plays a crucial role in safeguarding people, businesses, and even nations from cyber threats.

The purpose and mission of defending against these threats, which can disrupt lives, should be communicated more frequently by role models. Their influence can inspire the younger generation to pursue careers in cybersecurity, inspiring them to make a difference in this field.

To expand the cyber talent pipeline, we can start by creating awareness and fostering interest in cybersecurity among children at an early age. Engaging them through diverse modes (computer games, animation, movies, television shows) that depict cyber hacking and network attacks can spark curiosity and entice them to delve deeper into the field.

Implementing school programmes that introduce students to the diverse opportunities within cybersecurity can also be beneficial.

In addition, I have noticed that hands-on experiences can greatly cultivate interest in cybersecurity. Activities such as hackathons, capture-the-flag competitions, and internships offer practical exposure to real-world challenges, significantly enhancing engagement in the cyber domain.

These initiatives not only educate but can also encourage students to explore careers in cybersecurity.

9. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

I would still choose to be a cybersecurity professional because the field is constantly evolving and intellectually stimulating.

Every day brings a new challenge — whether it is new technologies, emerging threats, or evolving attacker techniques.

There will always be new attacker techniques to examine and analyse. Concerns over whether these techniques could be used against public healthcare drive us to assess their impact on the networks and systems we protect.

Moreover, cybersecurity offers diverse opportunities, from blue team roles such as security monitoring, incident response, forensics, threat hunting and intelligence, to red team roles including penetration testing, security validations and red team operations.

With so much to do and learn, there is never a dull moment in cybersecurity.

Chan Yew Weng, Agency Chief Information Security Officer (ACISO), National Library Board (NLB), Singapore

By **Amit Roy Choudhury** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the National Library Board (NLB)'s Agency Chief Information Security Officer (ACISO), I manage NLB's cybersecurity team and all related agency cybersecurity matters. NLB nurtures Readers for Life, Learning Communities and a Knowledgeable Nation by promoting reading, learning and discovery through our network of 28 libraries across Singapore, the National Library and the National Archives of Singapore.

2. What kind of cyber threats does your organisation face on a regular basis?

Like every organisation that is tech-enabled and connected, NLB faces cybersecurity probes, incidents and active threats. These include phishing, scam e-mails and messages, active cybersecurity threats, malware threats, and cybersecurity reconnaissance probes on our networks and services.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

In cybersecurity, the consensus among all cybersecurity professionals is overwhelmingly that the human element is the weakest link. Hence the biggest cybersecurity threats that we face today usually pertain to scams and phishing attempts through e-mails and messages that target users.

All it takes is one person, even someone who is tech-savvy, to inadvertently run unauthorised processes and/or unwittingly introducing unverified files into systems. We need everyone to be vigilant all the time. No one, not even the tech-savvy, can afford to be complacent with cybersecurity.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Yes, AI has increasingly become a double-edged

sword for cybersecurity. On one hand, we are seeing prevalent use of AI to generate scams and phishing messages and in creating vocal and/or video deepfakes which makes it difficult for users to distinguish the authenticity of information/communications received.

On the other hand, cybersecurity professionals leverage AI for data analytics, monitoring and filtering of the massive amounts of data that is collected by the organisation. With AI to augment our operations, we are better positioned to identify and thwart potential attacks in a timely manner.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

Sharing of information and resources is vital. With more information at hand, we will be better placed to identify and find indicators of compromise in a timely manner rather than guessing at what to look out for.

Hence the whole-of-government or country approach, in terms of information sharing is helpful in these circumstances.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

As is often said, it is not a matter of if but a matter of when. We need to prepare for the worst and hope for the best. NLB regularly conducts drills such as tabletop and recovery exercises where we test the effectiveness of our cybersecurity recovery plans should a breach occur.

Over the years, our recovery plans, exercises and drills have evolved to address emerging challenges like ransomware and scams, ensuring our readiness against the dynamic nature of cybersecurity threats.

However, cybersecurity is evolving at such a pace that whatever plans that are in place today might not be effective against new and evolving threats. That is why it is also important for everyone in this space to stay updated and vigilant on emerging cybersecurity challenges and adapt accordingly.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

I would make use of the budget in two ways. First, the main priority is to target user awareness and education since our people is our first line of defence.

Next, it would be the enforcement of basic cybersecurity hygiene (in terms of simple things like the principle of least privilege, baselining and hardening of systems, utilising Multi-factor authentication in systems and networks, etc).

In my opinion, a sophisticated cybersecurity toolset will increase the quality of telemetry gathered but it is not such an essential element on Day 1. Getting the fundamentals right matters more.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I was first given the opportunity to work in this field in the early days where cybersecurity was just in its infancy where security was often an afterthought.

It gave me the opportunity to learn and understand where cybersecurity needed to be implemented and was most important and effective (i.e. from the Network to Applications and now the Cloud).

To my mentors in my previous agencies, I am forever grateful for the opportunity!

What motivated me then and now, is still to create a safe environment where everyone has access to the learning and discovery of our resources and services.

I believe that providing this safe and level playing field is essential - when people feel secure using our systems, they can focus on what truly matters: learning, discovering, and growing at their own pace.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

This has been a challenge from the beginning since the cybersecurity field first emerged. Singapore has been trying to expand the talent pool of cybersecurity professionals through various training and education programmes.

As we have progressed, I am encouraged to see that cybersecurity awareness is becoming part of the broader IT culture.

The majority of IT professionals now have basic cybersecurity knowledge ingrained in them. This shift has made collaboration between cybersecurity professionals and other IT fields more effective and efficient.

Also the emergence of AI has helped to augment some of the more mundane tasks in the industry. By automating routine tasks like alert monitoring and data analysis, cybersecurity professionals can dedicate more time to critical activities like risk assessment and developing mitigation strategies, rather than getting bogged down by repetitive monitoring tasks.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

On a personal belief and mission basis, yes, I would still want to consider cybersecurity as a career. There are fundamental challenges that I believe I can help tackle and influence in cybersecurity.

However, the pace of change in cybersecurity and AI are relentless, and a lot is expected from the cybersecurity team. Therefore, I cannot overstress the importance of having a good team in place to ensure that the organisation achieve its goals. At the end of the day, while the work can be intense at times, the sense of purpose and fulfilment I get from it makes it all worthwhile.

Eric Wong, Director, Cyber Operations & Technologies, Cyber Security Office, Synapxe, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

The national HealthTech agency, Synapxe, bolsters the local public healthcare sector by providing secure and reliable digital systems. This support empowers healthcare professionals to deliver safe care while ensuring that patients can access services with confidence.

As the Director of Cyber Operations & Technologies at Synapxe, I lead a multi-disciplinary team of over 100 specialists dedicated to safeguarding our public healthcare institutions from cyber threats. We work round the clock to detect, prevent, and respond to potential cyberattacks.

Our team also analyses global trends — examining attackers' tactics, operational methods, and emerging risks — to ensure we stay one step ahead. We regularly test and enhance our systems to ensure that they remain resilient and ready.

Additionally, we plan strategic investments to keep our defences strong and future-ready.

Beyond my day job, I also serve as President of the ISC2 Singapore Chapter, where I contribute to growing and supporting the wider cybersecurity community in Singapore.

2. What kind of cyber threats does your organisation face on a regular basis?

The cyber threat landscape is constantly evolving. Globally, we are witnessing an increase in ransomware, advanced persistent threats (APTs), sophisticated phishing scams, and supply chain attacks.

In Singapore, the Cyber Security Agency of Singapore (CSA) consistently identifies ransomware and phishing as top concerns, along with the rising threats to essential services and critical infrastructure.

The healthcare sector is particularly vulnerable. In the United States, the 2024 Change Healthcare ransomware attack disrupted medical services nationwide and affected over 100 million individuals.

Such incidents highlight a growing global trend: healthcare systems are attractive targets due to their sensitive data, complex environments, and the critical nature of their services.

At Synapxe, we proactively address these challenges by closely monitoring global and local threat developments, strengthening our defences, and investing in the right mix of people, processes, and technology to protect Singapore's public healthcare sector.

This ensures that healthcare professionals can deliver care with confidence and that patients can trust the systems that support them.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

One of the most significant challenges globally is that public sector systems are high-value targets.

They contain sensitive citizen data, deliver essential services, and often operate within large, complex digital environments, making them attractive to both cybercriminals and state-linked attackers.

At the network layer, attackers seek out weaknesses like unpatched systems or misconfigured infrastructure to infiltrate and navigate through systems undetected.

However, the more pressing and growing threat today lies in the human element — phishing, scams, and identity theft — where attackers circumvent technology altogether and deceive people instead.

A notable example is the 2024 incident involving UK engineering firm Arup, where scammers employed deepfake technology to impersonate the company's CFO and other executives in a video call.

An employee in the Hong Kong office was misled into transferring US$25 million (S$32.1 million) to fraudulent accounts. This incident underscores the increasing sophistication and danger of scams, particularly with AI-powered tools now accessible to cybercriminals.

In the public sector, where services must remain open and accessible, the challenge is finding the right balance between usability and security.

That's why strong identity protection, layered defences, awareness training, and proactive monitoring are more important than ever.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

We truly seem to be entering a high-tech game of chess, with both sides utilising super-powered AI assistants.

Picture your favorite action movie, but instead of spies and lasers, it features hackers with chatbots and defenders with AI copilots.

In the past, a hacker might spend hours crafting a convincing phishing email. Now, they can simply prompt an AI to generate one instantly — complete with perfect grammar, multiple languages, and even tailored to your LinkedIn profile. It is quite alarming, right?

However, here is the twist: cybersecurity professionals also have AI on their side. While hackers attempt to infiltrate, AI defenders are analysing billions of data points, detecting unusual behaviour, and raising alarms — often before a human even realises something is amiss.

Both sides are equipping themselves with faster, smarter tools, but ultimately, it still comes down to who has the better strategy, the sharper team, and the most vigilance.

So yes, we are in an AI-powered cyber arms race.

But the good guys have powerful allies too — and they are not backing down anytime soon.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

While it is often said that a system is only as strong as its weakest link, I prefer to focus on the strength that arises from unity.

Cybersecurity is truly a team sport, and when we collaborate effectively, our collective strength can overcome individual weaknesses.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

I don't view it as a Plan B; it is Plan A.

In my younger days as Scout, our motto was "Be Prepared" and that mindset has stayed with me. In cybersecurity, it's not a question of "IF" an incident will occur, but "WHEN". Thus, preparation is not a backup plan — it is the primary strategy. It is about building resilience and ensuring we can recover quickly.

The role of cybersecurity is to restore business operations, minimise downtime, and maintain trust. In today's interconnected world, cyber threats disregard boundaries, targeting individuals, organisations, and nations alike.

Adversaries often collaborate on the dark web, sharing tools and intelligence.

To combat this, we must adopt a whole-of-government and whole-of-country approach, where public agencies, private sectors, professional associations, and individuals work together, sharing information and resources.

By building a cohesive cybersecurity ecosystem, we enhance our collective resilience, ensuring that our defences are robust and adaptive against evolving threats.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

Regardless of whether resources are limited or abundant, the fundamental pillars remain the same: people, processes, and technology.

People should always be our top priority. We need to attract talent and provide continuous training to stay ahead of evolving threats. Investing in our team's development ensures we have the expertise to tackle emerging challenges.

Furthermore, we must remember that security should be an enabler, not a barrier. This means investing in seamless security solutions that enhance user experience rather than impede it.

By integrating intuitive tools and fostering a culture of security awareness, we can protect our systems without compromising usability.

Ultimately, it is about cultivating a secure environment where innovation can flourish and users feel empowered rather than restricted.

8. What brought you to this profession?

My journey into cybersecurity began in the 1980s during my primary school years, where I developed a fascination with computers and coding.

This passion deepened throughout secondary school and junior college, where I dedicated countless hours to exploring programming and understanding systems operations.

Influences from cyber-themed movies like Hackers (1995) also played a significant role, showcasing the captivating of hacking and digital exploration.

I was also intrigued by the exploits of Kevin Mitnick, the legendary hacker from the late '80s and early '90s, who infiltrated major corporations and government networks — not just through code, but also via clever social engineering.

This sparked my curiosity about not only how systems functioned worked, but also how they could be secured.

That curiosity drove me to pursue a Bachelor of Engineering in Electrical and Electronic Engineering, specialising in computing, followed by a Master of Science in Information Assurance in 2006, which, fun fact, was the term used before "cybersecurity" became the more popular label for the field.

My journey has been shaped by curiosity, and I am grateful it has led me to this point.

9. What do you love the most in your job?

There is so much to love, but if I had to choose, it is the hands-on tinkering and problem-solving that truly energises me.

Whether analysing a cyber incident, testing a new detection method, or figuring
out how to harden our defences, I enjoy rolling up my sleeves and diving into the technicalities.

Even more than that, it is the people I have the privilege to work with. I am fortunate to be surrounded by a passionate and talented team that is mission-driven, collaborative, and fun to work with.

Tackling challenging problems together and knowing that our efforts contribute to the protection of the public healthcare system makes the work all the more meaningful.

10. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

The cybersecurity talent shortage is a pressing global challenge. According to the World Economic Forum's Global Cybersecurity Outlook 2025, the cyber skills gap increased by 8 per cent in 2024, with two-thirds of organisations experiencing moderate to critical talent shortages.

Moreover, only 14 per cent expressed confidence in capabilities of their current teams.

Additionally, a key challenge is the misconception that cybersecurity is exclusively for individuals with deep technical expertise. In reality, the field encompasses a wide range of roles, including policy development, risk management, and user education.

Promoting diversity is essential; while Singapore has made strides, women still represent less than half of the tech workforce, highlighting significant opportunities to enhance their participation in cybersecurity roles.

To bridge the talent gap, we need to invest in comprehensive training and education programmes. This includes integrating cybersecurity into school curricula, offering scholarships, and providing accessible certification courses.

In Singapore, the Skills Pathway for Cybersecurity. This initiativelaunched by the Singapore Computer Society with 13 founding employers including Synapxe, offers structured training and certifications for aspiring professionals.

This initiative provides clear guidance for individuals entering the field, supported by industry-recognised certifications and opportunities for internships and job interviews.

On a global scale, collaboration among governments, educational institutions, the private sector, and professional associations is crucial to develop a robust pipeline of cybersecurity talent.

By demystifying the field and providing clear pathways for entry and advancement, we can attract a diverse range of individuals to this vital profession.

11. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

110 per cent yes! Getting paid to do something I love, why not? Also, I get to say things like "I work in cyber" at parties, which sounds cool – even if no one truly understands what it entails.

On a serious note, it is incredibly rewarding to protect critical systems and help others navigate the digital world safely. Plus, there is always something new to learn which keeps the job exciting.

Lee Chee Hwan, Deputy Director, SingHealth CISO Office, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

The Cybersecurity Office oversees the cybersecurity programme for SingHealth, and our goal is to ensure the security and resilience of healthcare IT systems, medical technology and devices, and operational technology systems.

We also aim to strengthen cybersecurity awareness amongst our users, making sure that operational security processes across the different teams in SingHealth and our IT partner, Synapxe, are functioning properly.

2. What kind of cyber threats does your organisation face on a regular basis?

Many experts have identified the healthcare sector as one of the most targeted sectors by cybersecurity threat actors. This is because patient data is a highly valuable resource and the level of reliance on IT systems is very extensive amongst hospitals.

Many of these threats have been successfully defended and neutralised through technical security measures and the vigilance and awareness of our staff. The skills and expertise of our IT partner, Synapxe, and their vendors have also contributed significantly.

These threats could easily have materialised into ransomware attacks leading to IT systems disruptions, theft of patient data and impact to business operations. Ransomware attacks are the top threat faced by healthcare organisations around the world today and has been so for the past five years or so.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Over the past few years, SingHealth, as part of the public healthcare family, has made significant investments to enhance and strengthen technical measures to protect against cyberattacks.

Despite these investments, one of the most challenging and difficult threats that we still need to be deal is from social engineering attacks via phishing emails and SMSes, due to its volume and fast evolving nature.

We are extremely mindful and cognisant that a single phishing link on an email could lead to a threat actor getting a foothold on our networks and thus lead to ransomware and other attacks.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Reports and expert opinions seem to indicate that AI tools have been increasingly used as a supplementary aid to threat actors in helping them carry out cyberattacks.

For example, using GenAI to help craft convincing phishing emails or to help develop scripts for carrying out port scans to identify vulnerabilities.

But the positive side is that AI can also help strengthen cyber defences, and many cybersecurity vendors have been working hard to include AI-assisted technology to help with cybersecurity detection, monitoring and response capabilities.

We expect this trend to continue and improve in the near and medium term.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

In cybersecurity, the attackers are often described as having an asymmetric advantage as they are able to pick their targets, time their attacks and have access to threat intelligence sharing amongst the threat actor community.

Given the inherent disadvantage of defenders, it is therefore critical to adopt an united approach to cyber defence from all public healthcare institutions. Everyone has a part to play and every institution works as one to defend against threats.

No one can guarantee that a cyberattack will not happen, but working together helps to reduce the risks, even from the weakest link.

In SingHealth, we place a lot of emphasis and focus on staff education and awareness efforts to ensure that everyone exercises vigilance and actively engages in safe cyber and data security practices.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Defence, prevention and awareness are important in cyber defence. However, resilience and recovery are also equally important.

A crucial part of any modern cybersecurity programme includes regular exercises to test readiness and resilience against cyberattacks.

The Plan B is to always be prepared that cyberattacks can and will occur, and to develop contingencies to deal with it, from crisis communications, to data and systems restoration processes, etc.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

In reality, there is no such thing as an unlimited budget, especially so in technology and cybersecurity. Regardless of the amount, all IT and cyber practitioners need to adopt a prudent, balanced and practical approach towards cyber defence spending.

The approach needs to be holistic, covering not just technical measures but also including training and awareness, as well as conducting of business continuity exercises to test and practice readiness and response.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I got into this profession by chance after starting in a consulting firm with zero background in cybersecurity. I enjoy meeting different people from various industries to understand their challenges, constraints and attitudes towards cybersecurity, which provides me an indication of how the nature cybersecurity can develop in the future.

I would like to improve the attitudes that many have about cybersecurity by correcting the misconception that cybersecurity is not only the responsibility of cybersecurity professionals but of everyone.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

It's a very complicated issue and we hope that with time, the situation will improve as the job market evolves and suitably skilled IT practitioners make the switch to the cybersecurity domain.

The Cyber Security Agency of Singapore has been working hard to deal with the cyber talent shortage, but it will still take a number of years before we see the results.

In the meantime, as a public healthcare organisation, SingHealth, together with our partner Synapxe, has invested in training to prepare and uplift staff who are keen to make the transition to cybersecurity. This is a win-win situation for both SingHealth and our staff.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Of course. Cybersecurity cuts across all skillsets and all domains, and with the ever-changing digital landscape and more organisations gearing towards digitalisation, it's a non-stop learning journey!

Leonard Ong, Director, Sector Governance - Risk & Sector Governance, Synapxe, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the Director for Sector Governance in Risk & Sector Governance (RSG) for Singapore's national HealthTech agency Synapxe, I lead several key areas covering public healthcare sector.

This includes Policy, Control and Compliance; Governance and Data Protection; Capability Development and Readiness; and Enterprise Risk Management and GRC System.

My team collaborates closely with various key stakeholders across Singapore's Ministry of Health (MOH), Cyber Security Agency (CSA), Health Science Authority (HSA), public healthcare institutions and the industry ecosystem, to increase cyber risk posture and maturity, drive efficiency and enable innovations in the sector.

For example, in 2024, Cyber Security Labelling Scheme for Medical Device [CLS(MD)] was formally launched during the Singapore International Cyber Week. This "first-in-the-world" multi-levelled CLS(MD) seeks to improve medical device security by incentivising manufacturers to adopt a security-by-design approach.

It will enable consumers and healthcare providers to make more informed decisions about the security of such devices prior to purchase and usage.

The CLS (MD) team had received the Dare to Do Award (Special Mention) for its Medical Device Oversight Comittee Programme during GovInsider's Festival of Innovation 2025

2. What kind of cyber threats does your organisation face on a regular basis?

Generally, the healthcare sector has been one of, if not the most, targeted sector in recent years.

Healthcare organisations worldwide are facing similar threats that have been widely reported in recent incidents, such as sophisticated phishing campaigns, ransomware, targeted social engineering, and attempts to exploit vulnerabilities in their systems.

The sensitive and valuable nature of healthcare data makes it a prime target for the threat actors, but together, we can strengthen our defences and protect our sector.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Globally, the healthcare sector faces significant threats from increasingly sophisticated, AI-driven cyberattacks like advanced phishing techniques, impersonation, ransomware targeting essential services, and supply chain vulnerabilities.

Challenges include dealing with legacy infrastructure that is inherently vulnerable, budgetary constraints that limit cybersecurity investments, and an expanding digital landscape that broadens the attack surface.

Additionally, balancing robust cybersecurity with the delivery of seamless population-centric digital health services adds complexity to governance and risk management practices.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

We are undoubtedly entering an era where AI significantly influences both cybersecurity threats and defences.

Adversaries increasingly leverage AI to automate and amplify their attacks through sophisticated deepfake campaigns and the rapid exploitation of vulnerabilities.

Conversely, defenders are harnessing AI for enhanced threat detection, predictive analytics, and automated response.

This dynamic creates a perpetual race that necessitates continual innovation, transparent, ethical use of AI tools, and robust defences that can adapt and respond swiftly.

5. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Having a well-articulated post-breach recovery plan is as crucial as preventive measures.

Effective cybersecurity requires acknowledging that breaches are possible, and therefore, planning for resilience is paramount.

A good approach involves rapid containment measures, eradication, detailed investigations, structured recovery operations, transparent stakeholder communications, and capturing actionable lessons learned.

Regular simulations, tabletop exercises, and drills are essential for testing and refining these plans, ensuring the resilience and continuity of critical services.

6. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

In reality, public healthcare organisations will never have an unlimited cybersecurity budget. Hence, it is imperative to ensure the prudent and strategic use of resources.

Even if budget constraints were not a concern, our priorities would still focus on critical areas that provide the highest return on investment. This includes:

- Modernising healthcare systems to reduce vulnerabilities
- Enhancing AI-driven threat detection and response capabilities
- Strengthening cyber readiness through realistic red-teaming exercises and robust cyber range training environments
- Promoting cybersecurity workforce development, education, and awareness initiatives
- Ensuring that secure-by-design principles are embedded across all new technology implementations

Ultimately, responsible and targeted investment in cybersecurity protects public trust and enhances the resilience of critical healthcare services.

7. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

The global shortage in cybersecurity talent calls for a multifaceted strategy which includes:

1. Integrating cybersecurity education and awareness initiatives early-on in schools
2. Implementing robust reskilling programmes aimed at mid-career professionals transitioning into cybersecurity roles
3. Promoting diversity by encouraging individuals from various backgrounds, including technology, communications, and analytics
4. Expanding internship programmes, mentorship opportunities, and continuous professional development through pre-defined skill pathways
5. Creating inclusive, adaptive, and supportive learning environments to cultivate and sustain a capable cybersecurity workforce
6. Continuously investing in upskilling and reskilling while collaborating with service providers to complement our needs
7. Automating work to allow the workforce to focus on higher-value activities

8. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

I would undoubtedly choose the same field again. In this era of Industry 4.0 (the Fourth Industrial Revolution), cybersecurity is essential in enabling digital transformation and preserving digital trust.

This makes the profession incredibly rewarding and purpose-driven, which I deeply value and enjoy.

Having worked in the healthcare sector for over a decade, I find fulfilment in knowing that we can make a difference by improving health outcomes through better and more modern healthcare services.

Lim Ee Lin, Deputy Director, CISO & Governance, Agency Chief Information Security Officer, Home Team Science & Technology Agency (HTX), Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I serve as the Deputy Director (CISO & Governance) and concurrently as the Agency Chief Information Security Officer (ACISO) for the Home Team Science and Technology Agency (HTX).

HTX's core mission is to empower the Home Team with cutting-edge science and technology solutions to enhance Singapore's homeland security. We support frontline operations across law enforcement, emergency services, border control, and civil defence.

As the ACISO, I am responsible for overseeing HTX's overall cybersecurity strategy, governance, and operational resilience. This includes leading the development of security policies, driving secure-by-design practices across critical projects, managing cyber risks, and ensuring incident readiness.

I work closely with senior leadership and operational stakeholders to ensure our systems remain robust against evolving cyber threats, while enabling innovation and transformation in support of national security outcomes.

2. What kind of cyber threats does your organisation face on a regular basis?

As an agency supporting national homeland security, we operate in a high-threat environment.

We are routinely targeted by phishing campaigns, malware, credential theft, and attacks on exposed services.

Beyond these, we face advanced persistent threats (APTs), including those potentially linked to state-sponsored actors. Given the critical nature of our work, even a small compromise can have cascading effects on public safety operations - making continuous vigilance and layered defences imperative.

Back to top

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The public sector globally is under growing pressure from both cybercriminals and geopolitical threat actors.

Key challenges include widespread phishing and impersonation campaigns, ransomware targeting public services, and identity theft. Legacy IT infrastructure, fragmented system ownership, and the increasing digitalisation of citizen services all introduce vulnerabilities.

In the context of homeland security, the stakes are particularly high - where operational downtime or data breaches can directly affect national safety and public trust.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI is undoubtedly reshaping the cyber battlefield. Threat actors are exploiting AI for automated reconnaissance, deepfake-driven social engineering, and advanced malware that can adapt to environments.

Conversely, defenders are leveraging AI for faster detection, behavioural analysis, and predictive defence.

However, AI must be deployed responsibly - augmented with human oversight, robust governance, and clear ethical frameworks - especially when it pertains to mission-critical homeland security systems.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

It is absolutely essential.

Homeland security relies on a tightly interwoven ecosystem of agencies, systems, and operations. An aligned and coordinated homeland security cybersecurity posture ensures coherence in policies, incident response strategies, capability development, and threat intelligence sharing across government.

Extending this to a whole-of-country approach - by engaging critical infrastructure operators, academia, industry partners, and the wider community - further reinforces our collective resilience.

Cyber defence must be a shared national responsibility, much like homeland defence itself, with every stakeholder playing an active and accountable role.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

A breach is not just a possibility - we have to be ready for it. Our Plan B centres around resilience and containment.

This includes predefined response playbooks, clearly assigned roles, secure backup environments, and communications protocols.

In a homeland security context, response speed and operational continuity are paramount. Post-incident reviews and simulations help institutionalise learning, making the organisation stronger with every challenge.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

I would prioritise three areas: (1) Enhancing detection and response capabilities, particularly those powered by real-time intelligence and AI; (2) Investing in cyber talent—through structured career pathways, upskilling programmes, and domain-specific training in homeland security technologies; and (3) Advancing secure-by-design practices through R&D in emerging technologies such as quantum-safe encryption, zero trust architecture, and cyber-physical systems resilience.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I was drawn to cybersecurity by the opportunity to serve the public interest while engaging in intellectually challenging work.

What I value most is the clarity of mission - contributing to Singapore's safety through the invisible shield of cyber defence.

Every threat countered, every system hardened, has a real-world impact. I would like to further enhance how cybersecurity is integrated into upstream technology development - embedding security early, not as an afterthought.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Addressing this shortage requires both structural and mindset change. We need to spark interest in cybersecurity from an early age - through engaging education, gamified learning experiences, and meaningful exposure to real-world applications.

Stronger partnerships with Institutes of Higher Learning (IHLs), such as universities and polytechnics, are vital to ensure that curricula remain aligned with evolving national and industry needs.

Support for mid-career transitions is also key, with mentorship, upskilling programmes, and diverse role pathways that welcome professionals from adjacent fields.

Just as importantly, we must challenge outdated perceptions - cybersecurity is not a male-dominated field by nature, and we must intentionally create space for diverse talent to thrive.

In the context of homeland security, where systems are increasingly technology-driven and complex, cultivating domain-specialised cyber professionals will be critical to building sustainable capabilities.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Absolutely.

My journey in cybersecurity has always been fuelled by passion - a genuine fascination with how systems work, how threats evolve, and how we can outpace them to protect what matters.

It's a field that challenges me intellectually while allowing me to contribute meaningfully to something larger than myself: the safety and resilience of our nation.

The dynamic nature of this work, coupled with its real-world impact, keeps me energised and inspired every day. If I had to start all over again, I'd still choose this path - without hesitation.

Dr Liu Yang, Executive Director, CyberSG R&D Programme Office, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

Prof Liu Yang is a Full Professor at Nanyang Technological University (NTU) and serve as the Executive Director of Cyber Security Research Centre @ NTU, as well as the Executive Director of CyberSG R&D Programme Office (CRPO).

His expertise spans cybersecurity, software engineering, and artificial intelligence, with research focused on bridging the gap between theoretical foundations and practical applications in programme analysis, data analytics, and AI-driven security solutions.

Having published over 600 papers in top-tier conferences and journals and received 30+ best paper awards, Prof Liu is leading several major research initiatives, including Cysren, Trustworthy AI in NTU (TAICeN), CREATE Center with ICL on medical device security and CyberSG R&D Programme Office (CRPO).

The CyberSG R&D Programme Office (CRPO) is a national cybersecurity research and development centre based in Nanyang Technological University (NTU) Singapore. It was established by the Cyber Security Agency of Singapore (CSA) in September 2023, with S$62 million in funding.

CRPO spearheads the translation of research prototypes into usable products and services for both the national security agencies and industry. It facilitates the commercialisation of cybersecurity technologies, positioning Singapore as a global leader in cybersecurity innovation and implementation.

2. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Cybersecurity is a constant tug-of-war between attackers and defenders.

The rise of AI, advancements in operational technology, and shifts in human behavior and lifestyles have redefined the cybersecurity landscape, introducing new complexities and vulnerabilities.

The resulting technical threats that define today's challenges can be categorised into the following areas:

First, Social Engineering. Things like phishing, scams, and impersonation are getting more advanced, especially with AI making fake emails, voices, and videos more convincing. These attacks target people, not just systems.

Second, Legacy Systems. A lot of government systems still run on old technology that's hard to update. These systems often lack basic protections and are easy targets for attackers.

Third, Supply Chain Risk. Public agencies use a lot of third-party and open-source software. If one part of that supply chain has a hidden vulnerability, it can impact everything else connected to it.

Fourth, AI-Powered Attacks. Attackers are starting to use AI to find weak spots faster and to make their attacks more adaptive. Defenders don't always have the tools to keep up at the same pace.

Fifth, Insider Threats. Mistakes or intentional misuse by people inside an organisation, like lost credentials or unauthorised access, can lead to serious breaches, and they're often hard to detect.

Sixth, Long-Term Intrusions. Some attacks aren't just quick hits - they're slow, quiet, and focused on staying hidden for months. These persistent threats can cause long-term damage if not caught early.

Cybersecurity considerations in the public sector are influenced by the complexity of governmental networks and the large volume of sensitive data they manage.

These factors present distinct security challenges and shape the potential consequences of cyber threats, affecting areas such as national security, public trust, and institutional stability.

3. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI Innovations has indeed transformed Cybersecurity from knowledge adaptation into insights generation and advanced methodological development.

In my recent panel discussion at the STACKx Cybersecurity 2025, I highlighted these three key areas that we should take note of:

Automated Discovery: AI-driven systems can autonomously identify novel attack vectors and defence mechanisms, enhancing the ability to detect threats in real time.

This allows organisations to detect threats in real time, reduce dwell time, and prioritise risks based on context. For example, AI models can analyse massive volumes of logs and traffic data to flag suspicious behaviours that traditional rule-based systems would miss.

Adversarial Simulation Battles: AI-powered techniques that simulate adversarial scenarios to refine both offensive and defensive cybersecurity strategies, enabling organisations to anticipate and counter sophisticated threats.

These simulations allow defenders to test how well their systems hold up under various threat models, including zero-day scenarios or advanced persistent threats. By automating red-teaming and scenario planning, AI helps refine both offensive and defensive tactics with greater accuracy and speed.

Attack and Defence Frameworks: AI-enhanced methodologies that strengthen security postures by proactively adjusting to evolving cyber threats.

We're also seeing the emergence of AI-enhanced security frameworks that can adapt on the fly. These frameworks combine behavior analysis, predictive modeling, and automated policy enforcement to respond to evolving threats in real time.

Rather than waiting for patches or alerts, these systems proactively adjust configurations, block malicious behavior, and even isolate affected components to prevent spread.

The core challenge is that cyberwarfare is becoming a high-speed arms race - whoever wields AI more effectively gains the advantage. Governments, businesses, and individuals must invest in AI-driven security to keep up, while policymakers regulate AI tools to prevent misuse.

4. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A whole-of-government or whole-of-country cybersecurity posture is crucial in today's hyperconnected world. Cybersecurity extends beyond just the technology; it is a coordinated and shared responsibility for all to build up the resilience of the nation.

Cybersecurity defence operates as an interconnected loop, where various stakeholders must remain aware of their roles in sustaining security and resilience. Any weakness within this framework, whether technical, procedural, or human, can compromise the entire framework.

As part of this ecosystem, CRPO seeks to bolster the R&D of cutting-edge technologies and increase collaborations between agencies, industry and public - private partnerships to commercialise these cybersecurity technologies and reinforces its commitment to build innovation-driven resilience of the ecosystem.

5. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Yes, the shortage of cybersecurity professionals is a serious global issue, and addressing it will require coordinated efforts across multiple stakeholders.

First, governments and educational institutions can help broaden the talent pipeline. That means updating curricula, funding scholarships, and creating programmes that welcome people from diverse backgrounds - not just computer science majors.

It's also about raising awareness early on, even at the high school level, that cybersecurity is a viable and meaningful career path.

Second, training providers and industry leaders need to focus more on practical, hands-on learning. Certifications, bootcamps, and real-world simulations are far more effective than theory-heavy courses alone.

Companies can also provide internships or apprenticeships that help people build experience before entering the workforce.

Third, employers play a big role in encouraging mid-career transitions. People in IT, software engineering, or networking already have a strong foundation, they just need support to pivot into security roles.

That might mean offering internal reskilling programmes, mentoring, or flexible certification support.

Fourth, technology vendors and cybersecurity firms can help by continuing to build tools that automate routine tasks, like threat detection, log analysis, or patch management. That allows smaller teams to work more efficiently and reduces the pressure caused by staff shortages.

Finally, everyone in the ecosystem, from educators to employers to policymakers, needs to work on changing the image of cybersecurity. It's not just about technical hacking skills.

It's about protecting real-world systems that affect lives, economies, and national stability. Framing cybersecurity as a high-impact, purpose-driven field can attract a more diverse and motivated workforce.

Michaela Chua, Development Programme Manager, Cybersecurity Programme Centre, Defence Science and Technology Agency (DSTA), Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I am currently a Development Programme Manager in Defence Science and Technology Agency's (DSTA) Cybersecurity Programme Centre, where I leverage deep kernel technologies to develop highly specialised cyber solutions to enhance digital defence for Singapore's MINDEF and the SAF.

I lead software development teams to develop custom in-house solutions focused on protecting defence systems and networks through encryption.

2. What kind of cyber threats does your organisation face on a regular basis?

In today's highly contested and fast-evolving cyber landscape, threats are not only wide-ranging and constant but also deliberate and increasingly sophisticated.

Thus, our cyber defence strategy involves leveraging best-of breed commercially-off-the-shelf (COTS) cybersecurity products to safeguard our networks. Increasingly, we notice that adversaries are also targeting some of the well-known COTS products.

It became clear to us that we need to develop bespoke, in-house solutions purpose-built to address the growing threat in the cyberspace. That's why DSTA invests in developing our own capabilities.

It's part of how we stay agile, adaptable and ready for new emerging threats.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The rapid advancement of emerging technologies like Artificial Intelligence (AI) and quantum computing introduces new and complex risks to the cyber landscape.

Back to top

We may be approaching a point where quantum computing could challenge the systems we currently rely on to keep our data secure.

Encryption standards protecting the most sensitive systems today may, in time, be compromised, continually challenging us to rethink and redesign how we defend our digital infrastructure for the future.

Public sector organisations globally may face similar risks as custodians of massive troves of personal, financial, and mission-critical data.

A quantum-capable adversary could, in theory, access this information on an unprecedented scale, threatening national security, eroding public trust, and disrupting essential services.

Many of these organisations could still be relying on legacy systems that are not originally designed to withstand quantum threats, making the transition to quantum-safe standards not only essential, but also urgent and highly complex.

In DSTA, we develop solutions with these challenges in mind, guided by strong systems thinking, close collaboration across teams and a drive to build future-ready capabilities.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI has rapidly become a double-edged sword in cyberwarfare. On one hand, it powers advanced defence mechanisms that can detect anomalies, predict attack patterns, and automate threat mitigation at machine speed.

On the other, adversaries are using AI to develop sophisticated malware, automate phishing campaigns, and identify system vulnerabilities faster than ever before.

This AI-versus-AI battlefield will become the norm, where both hackers and defenders deploy adaptive algorithms in a continuous cycle of attack and response.

It will no longer just be about keeping up. In DSTA, we are moving towards setting a clear operational framework that ensures AI tools are used wisely, transparently, and effectively within our defence infrastructure.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

Within the public sector, this means engaging with partners across government, industry, and academia, not just locally but internationally, to share threat intelligence and strengthen collective defences.

Equally important is the mutual sharing of cybersecurity solutions and capabilities within the broader government ecosystem.

By sharing our in-house cyber capabilities within WOG, we also streamlined our efforts and accelerate the capability growth across agencies. And more importantly, we reap the benefits of raising the collective cyber maturity of the public sector.

Given our limited talent pool, I believe that there is immense value in ensuring our locally-developed innovations are not siloed and only through active collaboration can we close the gaps that adversaries seek to exploit.

At DSTA, we believe that a unified approach is key to building resilient systems that can withstand increasingly complex cyber threats.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

For a defence organisation like DSTA, we take every near-miss incident as an opportunity to coordinate and improve our operational response between various teams.

Teams such as Incident Response, Threat Hunting, Red and Infrastructure teams also work together to frequently test and refine our incident response playbooks and ensure everyone understands their role when systems go down.

These exercises are extremely crucial in sharpening the effectiveness of our response and recovery mea-

sures. Ultimately, the real test of our cyber maturity is not whether we can avoid every attack, but how effectively we respond, recover, and restore trust.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

If I'm given an unlimited budget for cyber defence, I would adopt a transformative approach that considers both today's threats and tomorrow's possibilities – a mindset we embrace in DSTA.

With additional resources, we can scale up our efforts in investing in people by focusing on developing strong cyber teams through continuous education, real-world simulations, and nation-wide collaboration.

While technology plays a critical role, skilled and adaptive professionals remain an essential line of defence.

There is also the need to spend on modernising one's infrastructure, where necessary, to better prepare for future threats.

This might involve deploying quantum-resistant encryption, implementing advanced zero-trust architectures, and designing systems with resilience in mind – building on the foundation that DSTA has already laid.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

What brought me to join DSTA in championing cybersecurity for the nation was a passion for problem-solving in high-stakes environments and the opportunity to develop deep technical skillsets.

Cybersecurity is one of the few professions where one can continuously be learning – whether its mastering encryption standards, understanding network architecture, or staying ahead of the latest attack vectors.

DSTA has a strong learning culture where we regularly share knowledge through lectures and courses, exchange perspectives and support one another's growth. Everyone is always so ready to share their knowledge and experiences.

This field requires a blend of theoretical knowledge and hands-on technical expertise, so we constantly spar ideas and help each other, making it an attractive and ideal environment for those who thrive on complexity and innovation.

Personally, I strive to develop not just technical proficiency, but also greater strategic thinking, leadership skills, and the ability to communicate complex risks in accessible terms. And my organisation places strong emphasis in nurturing such skills among the staff too.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

In my view, we should aim to change the perception of cybersecurity, where it is not just a technical field for specialists but a domain critical to every aspect of modern society.

Recognising the need for diversity can certainly help us to attract a wider, more dynamic pool of professionals to meet the growing demand.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

If I had the chance to restart my career from scratch, I would still choose to be a defence cyber warrior without hesitation.

Few careers offer the unique concoction of intellectual stimulation, societal impact, and continuous discovery that cybersecurity provides. Every day, there is something new to learn and new ways to collaborate with brilliant minds across disciplines.

More importantly, the opportunity to make a tangible difference in protecting our national interests while operating on the frontlines of technological innovation is incredibly fulfilling.

It's something I've found deeply meaningful in my journey with DSTA.

Syam Gumpalli, Director, Cyber Risk Management & Services, Cyber Security Office, Synapxe, Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

Synapxe is Singapore's national HealthTech agency inspiring tomorrow's health. As the Cyber Risk Management and Services Lead, I provide Chief Information Security Officer (CISO) services to public healthcare entities.

My role involves developing and implementing strategic programmes aimed at enhancing cyber resilience, strengthening cybersecurity governance and importantly, promoting cybersecurity awareness among staff and stakeholders.

I also lead a team of Technology Information Security Officers (TISOs) to manage cyber risks for public healthcare ICT systems, ensuring compliance with Security-by-Design principles.

I also oversee efforts to proactively identify and address security vulnerabilities within our public healthcare technology ecosystem.

2. What kind of cyber threats does your organisation face on a regular basis?

We face and address various cyber threats prevalent in the healthcare sector, including ransomware, phishing, scams, advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and supply chain vulnerabilities.

Our comprehensive security strategy incorporates multiple layers of defence to mitigate these persistent risks, ensuring a resilient HealthTech environment for Singapore.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Globally, public sector cybersecurity is facing significant challenges, such as state-sponsored attacks and ransomware targeting critical infrastructure. These threats are further complicated by the presence of legacy systems.

Back to top

Supply chain attacks and human-layered threats, including sophisticated, AI-driven phishing scams targeting citizen data, are also a concern. Other key challenges include budget limitations, skills shortage and insufficient employee awareness.

To effectively address these multifaceted issues, it is crucial to implement coordinated, well-funded and proactive strategies to strengthen public sector resilience worldwide.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

We are entering an era of AI-driven cyberwarfare, where attackers utilise AI for automated reconnaissance and sophisticated attacks, such as phishing and polymorphic malware, which can overwhelm traditional defences with speed and scale.

On the defensive front, AI provides powerful advantages by analysing vast datasets in real-time for anomaly and threat detection, automating intelligence, enhancing vulnerability management, and implementing adaptive controls.

The future of cybersecurity will be shaped by this AI arms race, making developing and deploying advanced AI tools crucial for both offence and defence.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

Fragmented national cybersecurity efforts create exploitable vulnerabilities. Adopting a unified, whole-of-nation approach facilitates the development of a cohesive, layered defence by leveraging shared intelligence, disseminating best practices, and coordinating responses.

This approach is crucial in reducing weak links and strengthening the entire digital ecosystem. It also promotes widespread cybersecurity awareness and responsibility, reducing weak links while enhancing overall digital resilience.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

In today's cybersecurity landscape, while prevention is crucial, it may not always hold up against sophisticated threats, making a comprehensive "Plan B" essential.

This proactive strategy would encompass a well-tested incident response plan, robust backup and recovery systems, network segmentation, and data loss prevention measures.

Additionally, business continuity and disaster recovery plans are essential for operational resilience beyond IT, alongside effective clear communication and post-incident analysis.

All in all, investing in resilience is key to achieving long-term security and business continuity.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

Regardless of budget, my priority would be to establish a proactive and intelligent security ecosystem that enhances threat intelligence through AI and expert insights.

I would revamp the infrastructure by implementing zero-trust principles, advanced tools, as well as Security Orchestration, Automation, and Response (SOAR) systems. At the same time, it is also essential to invest in top talent and integrate security through DevSecOps.

Beyond prevention, I would focus on building resilience by implementing immutable backups, expanding the scope of the Disaster Recovery Plan, and ensuring redundancy.

A proactive security awareness programme, coupled with strategic research partnerships, are also essential for fostering a dynamic and adaptive defence that ensures long-term security and operational integrity.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

My journey into cybersecurity was profoundly shaped by my former boss 12 years ago, who inspired me to pursue this field and led me to discover its potential for making a meaningful impact in protecting critical systems and data.

What I love most about my job is the deep sense of purpose that comes from safeguarding organisations and individuals against cyber threats. This work is not just a job, but a mission to contribute to a safer digital environment. It is incredibly rewarding to know that my efforts help prevent breaches, protect sensitive information, and foster trust in technology.

Looking ahead, I hope to see a greater emphasis on how security can actively contribute to business

goals and innovation, evolving beyond its traditional role as a purely preventative function to becoming a business enabler.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

The global shortage of qualified cybersecurity professionals presents a significant challenge demanding multifaceted solutions.

First, investing in education and training programmes across various levels, from schools to vocational centres, is crucial for developing a robust talent pipeline. Upskilling existing IT professionals can also help bridge the immediate skills gap.

Additionally, public-private partnerships are vital for creating innovative training and certification programmes, while incentives like scholarships can attract more students to the field.

Addressing this shortage also requires promoting diversity and inclusion to engage underrepresented groups, while leveraging automation and AI for routine tasks can free up existing professionals to tackle more complex challenges.

Finally, raising public awareness about cybersecurity careers and providing early exposure in schools can inspire future professionals.

Tan E-Seon Reggie, Director (Cybersecurity and ICT Governance), Ministry of Home Affairs (MHA), Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the Director overseeing Cybersecurity & ICT Governance and concurrently serving as the Ministry-level Chief Information Security Officer (CISO) for the Ministry of Home Affairs, Singapore, I help to shape and enforce cybersecurity policies, standards, and guidelines to ensure that the Home Team's digital infrastructure and operations remain secure, resilient, and future-ready.

A key part of my role also involves enabling our Home Team departments to adopt innovation securely. We also work closely with both public and private sector partners to enhance national cyber resilience and align with broader whole-of-government digital and cybersecurity objectives.

The Ministry of Home Affairs consists of MHA Headquarters, seven Home Team departments and three statutory boards, known collectively as the Home Team. The Home Team works round the clock to keep Singapore safe and secure.

2. What kind of cyber threats does your organisation face on a regular basis?

Scams, phishing, and identity theft continue to be prevalent, given the high Internet penetration in Singapore and greater use of social media, smartphones and e-commerce. It is becoming harder to protect citizens from criminal activities happening online.

There is also a greater risk given that more of our government services are being transacted online, which increases the attack surface. We also face emerging threats such as supply chain vulnerabilities and AI-powered cyberattacks.

Our Home Team CISOs have to step up our cyber leadership to address these multifaceted security risks while balancing it with accessibility and innovation — ensuring digital services are easy to use while remaining well-protected.

3. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

We're already seeing AI influencing both sides of the cybersecurity battlefield. Malicious actors use AI for large-scale phishing, automated reconnaissance, and even deepfake campaigns.

On the other hand, defenders like us are deploying AI for anomaly detection, behavioural analytics, and automating incident response. To stay ahead, it is critical to invest in AI-driven tools while retaining strong human expertise and ethical oversight.

4. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

Cybersecurity absolutely requires a collective effort.

A whole-of-government approach ensures alignment of standards, resource sharing, and coordinated responses across the different sectors.

The digital ecosystem is only as strong as its weakest node - so it's essential to ensure that every agency, supplier, and individual understands their role and is equipped to play it effectively.

5. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

The reality is that breaches are inevitable, so resilience is key.

A robust Plan B includes well-tested incident response plans, real-time monitoring, rapid detection and containment measures, and a strong disaster recovery plan. Regular cyber drills and tabletop exercises will prepare the staff for various scenarios, and ensure that teams are prepared to act swiftly to minimise damage.

Resilience is not just about bouncing back but to be able to recover swiftly, with minimal disruption to services that citizens rely on daily.

6. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

There will always be a need to manage resources, ranging from budget and time, to manpower.

Given the increasingly complex digital landscape, I would prioritise predictive threat intelligence platforms, AI-based detection tools, and modernising legacy systems.

I would also give weight to continuous development of our cybersecurity professionals within the organisation - through skills development, advanced training, and nurturing our next generation of cybersecurity leaders.

7. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I was drawn to this role because of its strategic importance and dynamic challenges.

What excites me is the opportunity to solve complex problems that have real-world impact. I particularly enjoy mentoring future cyber leaders and supporting innovation within secure parameters.

One area I think has room for improvement is inter-agency coordination, especially in areas like information sharing and incident escalation. This is because early sensemaking will allow us to respond to the threat more effectively.

8. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

The shortage of skilled cybersecurity professionals is real, but it can be addressed with the right strategies.

Our Institutes of Higher Learning have already begun expanding cybersecurity education and certification. We also need to create more industry internships, apprenticeships, and mid-career conversion opportunities.

Encouraging diversity and offering flexible pathways into the field will help grow the cyber workforce.

9. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Without a doubt! Cybersecurity is more than a job - it's a mission.

The challenge of staying ahead of adversaries keeps the job engaging.

Plus, knowing that the work I do helps safeguard public safety and critical infrastructure gives me a strong sense of purpose every single day.

Tan Shui-Min, Chief Information Technology Officer, National University of Singapore (NUS), Singapore

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

NUS is the oldest, largest, and the flagship university of Singapore. We are also one of Asia's leading universities. Ranked 1st in Asia and 8th globally by QS world university ranking.

NUS is known for its comprehensive education system, cutting-edge research, and visionary enterprise.

We are a vibrant university offering a wide range of undergrad, grad and professional degree programmes across a diverse array of disciplines in STEM, humanities, social sciences and the arts.

As the Chief Information Technology Officer (CITO) of the National University of Singapore (NUS), my role goes beyond that of a traditional cybersecurity professional.

I lead the university's digital transformation efforts, which include shaping IT strategy, driving innovation, and ensuring operational resilience across our academic, research and administrative functions.

Cybersecurity is a critical part of this, and my responsibilities include safeguarding NUS's digital assets.

2. What kind of cyber threats does your organisation face on a regular basis?

Our university regularly faces a variety of cyber threats that are common across the higher education sector, for example phishing, malware and so on.

To mitigate these threats, we maintain robust cybersecurity protocols, continuous monitoring, regular training, and incident response plans.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The public sector is a prime target for a wide array of cybersecurity threats due to the sensitive nature of governmental data, the scale of operations, and the potential for widespread disruption.

In particular, Advanced Persistent Threats (APTs) and state-sponsored attacks frequently target organisations in the public sector for espionage, intellectual property theft or to undermine trust.

These attacks are sophisticated, stealthy and persistent. Similarly, critical infrastructure such as utility, transport and health, is also increasingly targeted in geopolitical conflicts, with destructive malware and sabotage.

Addressing these requires a comprehensive, multi-layered approach: robust technical defences, security awareness training for staff, strong identity and access management, regular incident response exercises, and a commitment to continuous improvement and collaboration with external partners.

At NUS, we are advancing on all these fronts, recognising that cybersecurity is not just a technical challenge, but a human and organisational one as well.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

I agree with the statement. Attackers are increasingly leveraging AI to automate and scale their efforts.

For example, AI can help cybercriminals craft more convincing phishing emails, find vulnerabilities in systems more efficiently, and automate the process of probing for weaknesses at a speed and scale that would be impossible for humans alone.

Generative AI can also be used to create fake content or deepfakes that are harder to detect.

On the other hand, cybersecurity professionals have been using AI-powered tools for defence long before ChatGPT came into the scene. These include systems that can detect anomalies in network traffic, identify potential threats in real-time, and automate responses to certain types of attacks.

AI can help sift through vast amounts of data to identify patterns or behaviours that may indicate a cyberattack, allowing for faster and more effective responses.

However, it's important to note that AI is not a silver bullet. While it can enhance both attack and defence, it also introduces new risks - such as adversarial attacks targeting the AI models themselves. Therefore, human expertise and vigilance remain crucial.

Our approach is to combine advanced AI technology with skilled cybersecurity professionals, continuous training, and robust governance.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A whole-of-government or whole-of-country cybersecurity posture is essential in today's highly interconnected IT environment.

Since systems across government agencies, critical infrastructure, businesses, and individuals are all linked, a vulnerability in one area can quickly become a risk to others.

Cyberattackers often exploit the weakest link, moving laterally through networks and across organisational boundaries. This interconnectedness means that no single entity can address the full range of cyber threats alone.

A unified approach to cybersecurity allows for better sharing of threat intelligence, resources, and expertise across different organisations.

When agencies and sectors work together, they can respond to incidents more rapidly and effectively, minimising potential damage. It also helps in developing and enforcing common standards, policies, and best practices, which closes the gaps that attackers might otherwise exploit.

Moreover, public trust depends on the reliability and security of essential services. When the public sector presents a united front against cyber threats, it reassures citizens that their data and services are being protected.

At NUS, we actively participate in national cybersecurity initiatives and embrace collaboration, recognising that only through such collective effort can we build a robust and resilient digital ecosystem.

Cybersecurity truly is a team sport, and success depends on a spirit of partnership across government, industry, academia, and the wider public.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

The reality is that no organisation, however well-defended, is immune to breaches. It is not a matter of "if" but "when", and what matters most is how effectively and quickly one can respond and recover from a cybersecurity breach.

Having a well-defined Plan B, otherwise known as an incident response plan, is essential.

This plan should outline the steps to take immediately after a breach is detected, including isolating affected systems, containing the threat, and preserving evidence for investigation.

Clear communication protocols are vital to inform stakeholders and response teams internally, and to notify affected parties externally when needed.

Equally important is the ability to restore critical operations and data swiftly and securely. This means maintaining robust, regularly tested backup systems and clear procedures for disaster recovery.

After the immediate response, conducting a thorough investigation to understand the root cause, assessing the damage, and learning from the incident is vital for improving defences and preventing future breaches.

At NUS, we place a strong emphasis on preparedness through regular tabletop exercises, continuous improvement of our recovery plans, and fostering a culture where reporting and responding to incidents is timely and coordinated.

Ultimately, this is about building resilience: being able to withstand disruptions, recover quickly, and emerge stronger after an incident. Having the right mindset and preparation are just as important as strong technical defences.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

An unlimited cyber defence budget is a tantalising proposition – much like indulging in unlimited ice cream without gaining weight.

While we prefer not to lay out the exact blueprint of our defences, I would say that under such wishful circumstances, we would certainly take every opportunity to future-proof our infrastructure, invest deeply in intelligence-led capabilities, and ensure our entire university community is equipped to navigate the digital landscape securely.

But as always, it's not just about how much you spend — it's how wisely you invest in people, processes, and technology.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

What brought me to this profession is the path of least resistance. I stumbled upon IT when in my first month in junior college (JC) I had to choose a subject to replace Biology.

I ruled out all other subject options for various reasons and Computer Science was the only one left. I included that as one of my A-level subjects and realised that I was pretty good at coding. So I went on to major in Computer Science in my university years, graduated to become a developer and got swept into the world of technology.

I can't say for sure that there is something or someone that inspired me to stay on in a tech career. It's more like, there's nothing to steer me off a career in tech. So here I am today, still in tech!

What I love most about my job is the opportunity to make a meaningful impact across the university community. Every day brings the chance to create new value through innovation and help shape the digital future of higher education.

I find great satisfaction in working with passionate colleagues and in seeing technology serve as an enabler of excellence.

What I'd like to improve is the way we continue to align digital initiatives with the evolving needs of the University.

While we've made great strides, there's always room to enhance communication, foster greater digital literacy, and build even stronger partnerships across the Institution.

My goal is to ensure technology not only supports but anticipates the needs of our community in a way that's seamless, inclusive, and forward-thinking.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

This requires a multifaceted approach. Firstly, education and training must be expanded and made more accessible.

Universities and institutions can play a key role by offering specialised cybersecurity programmes and integrating relevant skills into their curriculum. Partnerships with industry can ensure that the training is practical and aligned with current needs.

Secondly, there should be greater emphasis on continuous professional development.

Cybersecurity is a rapidly evolving field, so ongoing upskilling through certifications, workshops, and hands-on experience is essential. Organisations can support this by providing learning opportunities and encouraging staff to pursue advanced certifications.

Thirdly, we need to broaden the talent pipeline by encouraging diversity and inclusion in the cybersecurity workforce. This means creating opportunities for women, mid-career professionals, and individuals from non-traditional backgrounds to enter the field.

Outreach programmes, internships, and mentorship

schemes can help attract and retain a more diverse range of talent.

Finally, leveraging technology such as AI and automation can help alleviate some of the resource pressures by automating repetitive tasks, allowing cybersecurity professionals to focus on more complex and strategic challenges.

At NUS, we are committed to strengthening the cybersecurity talent pipeline through our academic programmes, research initiatives, and industry collaborations.

Ultimately, addressing this shortage will take coordinated effort from academia, industry, and government to build a skilled, agile, and diverse cybersecurity workforce for the future.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

If I had the chance to restart my career from scratch, I would absolutely choose to be a CIO again. The role offers a unique blend of leadership, innovation, and problem-solving that keeps every day interesting.

With cybersecurity responsibilities, there's the added challenge and privilege of protecting the university's most valuable digital assets and ensuring a safe environment for learning and research.

It's a role that demands constant learning and adaptation, and that dynamic nature is what makes it both rewarding and fulfilling. It's like having coffee packed with adrenaline each day!

Amorn Chomchoey, Secretary-General, Nation Cyber Security Committee, National Cyber Security Agency (NCSA), Thailand

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the Secretary General of the National Cyber Security Agency (NCSA) in Thailand, I am responsible for leading the strategic direction of the country's cybersecurity initiatives.

My role involves coordinating efforts to secure national critical infrastructure, setting policies that guide both public and private sector cybersecurity activities, and promoting cooperation across all levels of government.

NCSA is dedicated to creating a resilient cybersecurity ecosystem through national preparedness, risk mitigation, and fostering strong international collaborations.

Our mission is to safeguard critical services and data, ensuring the continued safety and growth of Thailand's digital economy.

2. What kind of cyber threats does your organisation face on a regular basis?

NCSA routinely handles a wide range of cyber incidents, with the most frequent involving intrusion attempts, online fraud, and misuse of digital content.

In the most recent reporting period, we responded to over 1,300 cases across various sectors, with education, finance, and government services being the most affected.

We're seeing a sharp rise in both technically driven attacks and socially engineered threats, such as phishing and financial scams. These trends reflect the growing sophistication and scale of cyber threats.

To address them, we focus on proactive monitoring, rapid incident response, and cross-sector collaboration at the national level.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

Globally, we're witnessing a significant rise in both technical and human-centric cyber threats.

From Thailand's experience, intrusion attempts and digital fraud are among the most persistent challenges, particularly in education, finance, and government services.

These incidents often exploit basic security gaps or human error, such as through phishing or social engineering.

Another growing concern is the misuse of information content - ranging from disinformation to data leaks - which can undermine public trust and national stability.

The public sector must address these challenges through greater investment in cyber hygiene, workforce training, and regional cooperation to defend against increasingly coordinated and cross-border attacks.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI will undoubtedly play a pivotal role in both offensive and defensive cyber operations. On one hand, cybercriminals are already using AI to automate attacks, quickly identify vulnerabilities, and scale their efforts.

On the other, cybersecurity professionals can leverage AI to analyse vast amounts of data, detect threats in real-time, and predict potential attacks before they happen.

While AI offers immense potential for improving defences, it also presents challenges, as adversaries can exploit the same tools.

This necessitates a balanced approach, ensuring that AI is used responsibly to enhance cybersecurity while remaining vigilant against its potential misuse.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A whole-of-government and whole-of-country cybersecurity approach is essential for addressing today's multifaceted cyber threats.

The strength of a nation's defence is only as strong as its weakest link, and when sectors fail to collaborate, vulnerabilities can arise.

It is vital for governments, industries, and regulators to align their strategies and work in concert to safeguard critical infrastructure, share threat intelligence, and ensure a coordinated response to incidents.

By unifying efforts across all sectors, we can create a stronger, more resilient cybersecurity ecosystem capable of responding to the ever-growing range of cyber threats.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

From a national standpoint, a cyber incident is not just a technical disruption - it's a test of coordination, leadership, and preparedness.

"Plan B" is not simply about containment and recovery at the system level, but about ensuring that the right governance, communication, and decision-making structures are already in place.

At NCSA, we emphasise incident response frameworks that involve cross-sector coordination, rapid information sharing, and clear public communication. Recovery must include not just restoring operations but reinforcing trust - both within institutions and among citizens.

Post-incident, we focus on systemic improvements, using each breach as a case study to enhance national resilience.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

If resources were no limitation, I would focus on building long-term national cyber resilience - beyond tools and technologies.

This includes strengthening the cybersecurity workforce, investing in early education, supporting local innovation in security solutions, and embedding cybersecurity into every level of digital transformation.

I would also invest in national-level simulation exercises, real-time monitoring infrastructure, and deeper cooperation with international partners.

Most importantly, I would fund sustained public awareness campaigns, because cybersecurity is not

only a technical issue - it is a societal one.

Empowering every sector and citizen to play a role is the true foundation of national defence.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I was drawn to cybersecurity because of its critical importance in today's world and the opportunity to have a direct impact on protecting national security and public trust.

What I love most about my role is the opportunity to work collaboratively with talented individuals from various sectors, solving complex problems and ensuring the country's resilience against cyber threats.

One area I would like to improve is the development of a more agile and adaptable cybersecurity workforce that can respond quickly to the ever-evolving threat landscape.

Continuous training and knowledge sharing are vital in this fast-paced field.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Solving the cybersecurity talent shortage requires coordinated national effort and sustained investment.

We need to develop a clear pipeline - from foundational education to specialised training - so that young people can see cybersecurity as a viable and rewarding career path. This also includes upskilling the existing workforce through hands-on programmmes and certification opportunities.

Collaboration between government, academia, and the private sector is key to ensuring training aligns with real-world challenges.

In parallel, we must foster a culture that values cybersecurity awareness across all professions, making it part of our national mindset, not just a technical domain.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

I believe I would, though I didn't plan for this path from the beginning. Over time, I came to see how important cybersecurity is - not just technically, but in terms of national stability and public confidence.

It's not an easy field, and there's always more work than time. But the ability to support others, respond to real challenges, and keep improving how we protect our systems and people makes it worthwhile.

I don't think any career is perfect, but this one has given me a meaningful sense of responsibility.

Saichon Saelee, Director of Cyber Coordination Department, National Cyber Security Agency (NCSA), Thailand

By **Si Ying Thian** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

As the Director of the Cyber Cooperation Office at the National Cyber Security Agency (NCSA), Thailand, my role involves overseeing both domestic and international cybersecurity coordination.

This includes managing partnerships with international cybersecurity organisations and ensuring Thailand's cybersecurity strategies align with global standards. Domestically, I work to integrate cybersecurity policies and foster collaboration across governmental sectors, private industries, and critical infrastructure.

NCSA is responsible for safeguarding the nation's critical infrastructure, developing cybersecurity policies, improving cybersecurity awareness, and responding to cyber incidents.

We also work globally to strengthen national resilience through cooperation and information sharing.

2. What kind of cyber threats does your organisation face on a regular basis?

NCSA regularly faces various cyber threats, including ransomware, phishing attacks, and exploitation of vulnerabilities in critical infrastructure.

Our focus is on securing the nation's Critical Information Infrastructure (CII). Collaborating with government agencies, regulators, and private sector partners is essential to mitigate risks.

We also face cross-border cyber threats and work internationally to strengthen cybersecurity defence mechanisms, share threat intelligence, and implement joint strategies.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

One of the biggest challenges in the public sector cybersecurity space globally is the increasing

sophistication of cyberattacks, including phishing, ransomware, and identity theft.

As governments and public institutions adopt more digital technologies, their systems become increasingly vulnerable to exploitation by cybercriminals. Another challenge is the need for improved cybersecurity awareness and training for staff at all levels.

Ensuring that critical systems and sensitive data are protected requires a coordinated effort across sectors, better security practices, and a culture of vigilance to mitigate these risks.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

AI is rapidly transforming the cybersecurity landscape, enabling both attackers and defenders to enhance their capabilities.

Hackers use AI to automate attacks, develop more sophisticated phishing schemes, and exploit vulnerabilities faster.

On the defence side, AI is crucial in identifying threats, detecting anomalies, and responding to incidents in real time.

We must ensure responsible use of AI, while continuously adapting our defences to stay ahead of adversaries.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

A whole-of-government and whole-of-country cybersecurity posture is crucial for minimising risks and building resilience against cyber threats.

Cybersecurity is most effective when all sectors - government, critical industries, and regulators - work together to address vulnerabilities and share information.

By fostering collaboration and aligning efforts across all levels, we can ensure that no sector is left behind, reducing the potential for a single point of failure.

This collective approach strengthens the entire system, enhances threat detection, and improves the ability to respond to incidents quickly and effectively.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Having a robust Plan B after a network breach is critical. This plan must include effective incident detection, response, and recovery protocols that involve coordination across government, CII sectors, and regulators.

Once a breach occurs, the focus is on containing the attack, isolating affected systems, and limiting the impact. Communication with stakeholders, including CII providers and regulatory bodies, is essential to restore services quickly and manage public trust.

Post-breach analysis helps identify weaknesses, reinforce security measures, and improve our national response capabilities, ensuring stronger defences moving forward.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

With an unlimited budget, I would focus on enhancing our cybersecurity infrastructure through advanced threat detection systems, AI-driven security tools, and robust training programmes for professionals.

I would prioritise expanding our cybersecurity workforce and improving collaboration between government agencies, regulatory bodies, and critical sectors.

Additionally, strengthening international partnerships and information sharing would be a key investment to address global cyber threats.

The overall goal would be to ensure a more resilient, adaptive cybersecurity posture that can effectively respond to current and emerging challenges.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I didn't set out to work in cybersecurity, but I gradually found myself drawn to it through my interest in policy, coordination, and how technology shapes the world around us.

It can be an intimidating space, especially for women, but I've learned that leadership in this field isn't only about technical expertise. What I enjoy most is working with people - connecting different agencies, cultures, and ideas to move things forward.

If there's something I'd like to keep improving, it's how we make cybersecurity feel more approachable, and how we encourage more women and young professionals to see themselves in this field.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

To overcome the shortage of qualified cybersecurity professionals, we need to invest in education, training, and awareness programmes.

Encouraging individuals to pursue careers in cybersecurity through internships, scholarships, and mentorship programmes can help bridge the skills gap. Additionally, promoting diversity within the field and fostering international collaboration will bring new perspectives and solutions.

Governments, educational institutions, and the private sector must work together to create accessible training opportunities and certifications, ensuring that the next generation of cybersecurity professionals is well-equipped to handle emerging challenges.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Yes, I would still choose to be a cybersecurity professional. The field is ever evolving, offering continuous opportunities for learning and growth.

The ability to contribute to securing critical infrastructure and protecting society from cyber threats is incredibly rewarding.

Cybersecurity remains a vital and impactful area where professionals can make a significant difference in ensuring the resilience and security of digital systems.

The challenges are stimulating, and the work we do has a direct effect on national and global security.

Mandy Andress, Chief Information Security Officer, Elastic, United States

By **Elastic** | June 16, 2025

1. Please give a brief description of your job function as a cybersecurity professional, as well as what your organisation does.

I am the Chief Information Security Officer (CISO) at Elastic, and I lead the charge in fortifying the company's security posture, leveraging nearly three decades of cybersecurity expertise to safeguard the organisation's information, technology, and people.

I share my learnings with other organisations so that we can balance risks and innovation, helping companies grow safely and sustainably.

Elastic is the Search AI company and provides enterprise solutions for search, observability, and security. We are a globally distributed workforce of more than 3,000 employees across 35 countries with a cloud-first approach to infrastructure.

The Elastic Information Security team is organised to address customer trust and enablement, security assurance, threat detection and response, and product security.

2. What kind of cyber threats does your organisation face on a regular basis?

At Elastic, we monitor vast amounts of security data (over 150 TB per day), including over 600 GB of security data from more than 450 thousand Elastic endpoints, to identify threats.

Like other large enterprise organisations, we face increasingly sophisticated phishing and social engineering attacks, amplified by AI, and monitor malware trends, particularly in Linux environments, relevant for companies expanding use of cloud environments that run on Linux.

Our security strategy relies on gaining comprehensive visibility of our data landscape, using tools and practices that provide deeper control and actionable insights to strengthen our security posture.

3. In your view, what are the biggest threats and challenges (be it in the network layer, and/or in areas such as scams, phishing and identity theft) in the public sector cybersecurity scene globally?

The biggest threats facing the public sector include ransomware, identity theft, and data breaches.

Today, public sector organisations are expected to be data-driven, citizen-focused, compliant, and efficient - all while securing critical infrastructure, meeting complex regulatory demands, and navigating the risks posed by emerging technologies like generative AI and machine learning.

Reducing the time to detection and validation of such threats is critical. Elastic provides search analytics capabilities that allow organisations to gain an advantage over cybercriminals by detecting potential fraud across vast volumes of data and keeping evidence searchable for the long term.

At the end of the day, fraud and cyber threats are a data problem. An organisation will need to have full visibility over real-time events and access to data that, in some cases, extends over multiple years to gain the insights as well as evidence to combat threats as and when they appear.

Speed is critical, and with real time data, detection rates can be improved and false positives reduced. Security teams can effectively identify abnormal behaviour and combat fraud by integrating the right information and logs into detection algorithms.

4. Many say that we are entering an age of AI-driven cyberwarfare where both hackers and cybersecurity professionals use AI tools for attack and defence. What is your view?

Cybersecurity is an ongoing battle that's intensified with AI.

Generative AI is a powerful tool, like a 'queen' in chess, capable of shifting the advantage. While bad actors use AI to create sophisticated, error-free phishing attacks highly targeted to their victims, AI also empowers cybersecurity professionals.

A GPT tool deployed responsibly can serve up helpful resources, providing the context needed to help evade potential attacks and facilitate a more effective response to any threats.

Generative AI doesn't just help security professionals make better decisions, it also helps them make faster decisions — with less manual effort. Generative AI can very quickly pull relevant information, best practices, and recommended actions from the collective intelligence of the security field.

Having this comprehensive context allows practitioners to quickly understand the nature of the attack, as well as what respective actions they should take.

5. Cybersecurity is often described as a team sport whereby a network's vulnerability is often defined by its weakest link. In this context, how important is having a whole-of-government or whole-of-country cybersecurity posture?

It is critically important for governments to establish a consistent and enforceable cybersecurity framework across all ministries. Interconnectivity is the cornerstone, aligning individual and agency priorities towards common security goals.

Singapore, for example, can consolidate security services under the leadership of a single CISO.

Such a strategy would enable local government agencies, school districts, state agencies, public colleges and universities, and even the private sector to leverage the same security tools, systems, team, and strategy.

Benefits of whole-of-state security include the centralised budgeting and resources, reduction of duplicative work and tools, and ultimately stronger security and incident response.

Rather than operating in siloes, a unified approach across a country's government will enable cross-agency data sharing.

With shared data, every agency will be equally equipped with the same threat data across the board, to empower cybersecurity protection measures and fraud detection.

6. An often-repeated point in the cybersecurity sector is what your Plan B is after your network is breached. Can you share your point of view on this aspect?

Proactively anticipate and prepare for breaches. Assume an incident will occur and avoid complacency. Develop playbooks and conduct practice scenarios. During any incident, understanding impact and communication are crucial.

7. If your organisation gave you an unlimited budget for cyber defence, what would you spend it on?

I would prioritise resources for Identity and Access Management (IAM).

Given the digital nature of modern business, robust IAM solutions are critical to ensuring secure and efficient user access across all applications, devices, and technologies.

8. What brought you to this profession and what do you love the most in your job and what would you like to improve?

I love that every day is different and brings new challenges. It's never boring! I'm really focused on bringing fresh perspectives to cybersecurity, especially by encouraging individuals from underrepresented backgrounds to join the profession.

9. The lack of qualified cybersecurity professionals is a global problem, how do you think this can be overcome?

Cybersecurity professionals should follow the same line of thinking on diversity in general.

In my view, and from my day-to-day experience as a CISO, a more diverse cybersecurity team is definitely a better cybersecurity team.

To address the lack of qualified cybersecurity professionals, we must broaden our candidate criteria beyond traditional backgrounds, valuing diverse skills and mindsets like curiosity and a passion for learning, not just data science expertise.

Additionally, we need to actively encourage more women to join the field by adjusting our recruitment methods to reach wider audiences, such as partnering with community colleges and specialised recruiters for diverse candidates.

10. If you had a chance to restart your career from scratch, would you still want to be cybersecurity professional and why?

Absolutely. My passion lies in the intersection of technology and business.

I find it fascinating to learn about business operations, technological advancements, and how organisations adopt new technologies.

Security is the unifying element, essential for every company's success, regardless of industry. That first computer my father brought home sparked a lifelong journey in technology for me.

Enjoyed what you've read?

Read our other cybersecurity stories *here*.

GovInsider

Subscribe to GovInsider's email newsletter for the latest updates on public sector innovation

SUBSCRIBE

Follow us for the latest news in government innovation!