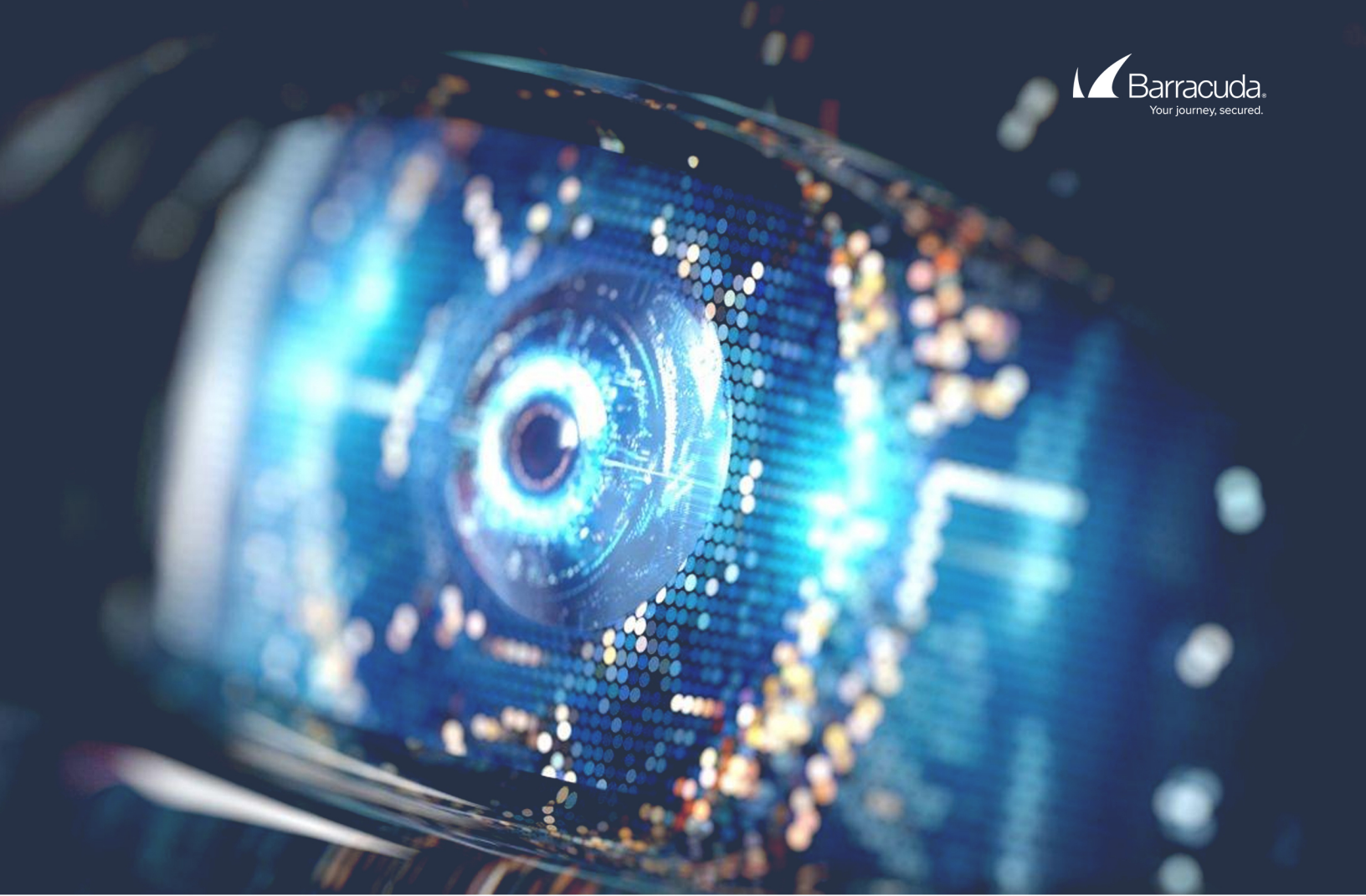


Cybersecurity in the Age of AI

The new 'AI versus AI'
frontier in cyber-defence



Cybersecurity in the Age of AI

The new 'AI versus AI' frontier in cyber-defence

The science and application of artificial intelligence (AI) has been around for decades, but with generative AI (GenAI) chatbots having been made publicly accessible since late 2022, we are now witnessing the gradual democratisation of the technology to consumers and public/private sectors worldwide.

While earlier GenAI chatbots had failed in various ways, OpenAI's ChatGPT with GPT3.5-Turbo and GPT4.0 Large Language Models became an overnight phenomenon, capturing the world's imagination around what is possible when it comes to this technology.

This potential has not been lost on cybercriminals, who much like everyone else are swiftly recognising the potential of Gen AI, realising that by combining it with other types of AI, such as machine learning and neural networks, it's possible to strike more targets faster, more evasively, and with better accuracy. Cyber defenders will need to respond in kind — so it is going to be an all-out AI-versus-AI arms race out there.

The question is, how will the AI-driven cyber war affect the global threat landscape in general, and the Asia-Pacific region in particular? What are the standout threats faced by organisations today, and how are defenders employing AI in response? When will the technocrats and leaders in AI development come up with a concrete plan to address AI weaponization and potential abuse and even the achievement of machine sentience?

These and other burning questions will be addressed in this Special Report, which features insights from Barracuda Networks; from cybersecurity experts interviewed by **CybersecAsia.net** over the past year and from the security leaders attending **Barracuda Networks'** industry roundtable event in October 2023.

Tackling escalating cyber threats in the Age of AI

Technological innovation drawing on AI is unfolding at an unprecedented pace, and business and society find themselves contending with the challenge of escalating cyber threats. The integration of artificial intelligence into various facets of our lives brings significant benefits but also presents a formidable playground for malicious actors. As our reliance on AI-based interconnected digital systems deepens, so will the sophistication of cyber threats, leveraging the capabilities of AI for nefarious purposes. Tackling this will demand a concerted effort from cybersecurity experts, policymakers, and technologists to devise adaptive strategies that not only defend against current threats but also anticipate and pre-emptively address the evolving landscape of malicious activities fuelled by the power of artificial intelligence. In this dynamic environment, the pursuit of effective cybersecurity measures becomes paramount for safeguarding the integrity, privacy, and functionality of our digital ecosystems.

As identified by Barracuda Networks' former Chief Technology Officer, Fleming Shi, there are 5 key trends and threats contributing to the urgency of this situation, including:

- 1. An explosion in data generation and the required protection of that data:** The world will need to protect at least 200 Zettabytes of data within the next three years.
- 2. Unprecedented levels of cybercrime and digital fraud:** The global cost of cybercrime is expected to reach \$10.5 trillion by 2025, up from \$6 trillion in 2021.
- 3. Huge investments are needed to address growing cybercriminal and state-sponsored offensives:** For the period 2021–2025, around US\$1.75 trillion will have been spent to address cyber threats: a figure that has so far proved to be ineffective for stemming the explosive rise of malicious digital activities.
- 4. A narrowing digital divide that will see more vulnerable users come online:** 75% of the world's human population, aged 6 and older, will soon be able to access the digital world, ready to be exposed to social engineering, scams, criminal campaigns, fraud and the hazards of the Dark Web.
- 5. The lagging supply of global cyber talent pools:** In 2023, the cybersecurity workforce gap reached a record high, with 4 million professionals needed to adequately safeguard digital assets.

(statistics source: Cybersecurity Ventures, 2023 ISC2 Cybersecurity Workforce Study)

Fighting AI with AI

As the relentless evolution of technology continues, a new battleground is emerging within the realm of cybersecurity—a virtual arena where cybercriminals equipped with advanced artificial intelligence face off against cybersecurity defenders wielding their own AI-driven tools. This clash of algorithms introduces a complex and dynamic dimension to the ongoing struggle for digital security. This paradigm shift in the cybersecurity landscape transforms the traditional cat-and-mouse game into a high-stakes duel of algorithms, where the outcomes hold profound implications for the security of our increasingly interconnected digital world.

The 'AI versus AI' battlefield

In the left-hand corner are the 'bad actors': such as lone cybercriminals, organised crime rings, and groups of highly motivated cyber mercenaries for hire by state-run or commercial agencies.	In the right-hand corner are the 'good actors', whose aim is to use AI to automate processes and solve pressing problems; improve world productivity and sustainability and do good in general.
Unique Advantages ✓ Previously leaked data provides sources of intelligence which are now feeding the attacker's data scientists. ✓ Cybercriminals don't consider themselves bound by international laws and restrictions. ✓ Their intentions can transcend mere financial motives to cross geopolitical, economic, social, personal, racial, religious and other causes. ✓ Some operate in the dark cyber-underworld in lean teams and broad networks of state-sponsored and/or mercenary groups, always a few steps ahead of lawful and law-bound crime busters. ✓ The succession and contingency planning of the groups behind some threats necessitates sustainable and resilient operations even when part or all of operations are busted or disrupted. ✓ When captured or exposed, state-sponsored cyber threat actors may enjoy discretely exercised diplomatic immunity and invisible legal privileges, rendering them as sustainable sources of cyber threat even when they are in custody. ✓ When AI is abused by driven, talented and organised criminal minds, its impact could be multiplied in every aspect. ✓ The most fearsome cybercriminal networks have the advantage of agility, focus, (sometimes state-sponsored) funding and geographically diverse operations to always stay ahead of the good actors or at least possess ways to slow them down.	Rules-based Disadvantages ✓ Even specialised crime-buster agencies are delayed by (justifiable) bureaucracy due to possible political ramifications. ✓ Global talent droughts persist in producing insufficient good actors to tackle the cyber war on equal footing. ✓ Bound by rules-based orders, respect for human rights and complex multi-agency dynamics, there is a common perception that even the best crime-busters cannot spend as much time and energy on winning as their lawless counterparts. ✓ There appears to be more complexity and unpredictability in succession and contingency planning. ✓ Lack of similar unity and immunity on a global scale, considering the diversity of national interests and subtle rivalry among so many governmental and commercial entities struggling to collaborate for a common global goal. Attrition remains high. ✓ If AI adoption is hesitant, fragmented and bogged down by distrust worldwide, the technology will always harbour weaknesses and unpredictable exploits. ✓ The most fearsome crime-busting networks may enjoy special legal waivers, funding and benefits to keep up with the bad actors, but they remain bogged down by disadvantages that criminals don't encounter or can evade.

This table indicates that the AI vs. AI fight is not a one-sided war. We have a fighting chance if we learn from history and act now. The good actors outnumber the malicious forces, and with the right global unity in place, the outcome of the AI war is still not set.

To narrow the gap, we need to address the aforementioned cyber threats and trends urgently; cut the lifelines and supplies of the bad actors, and boost our own preemptive-strike and counterattack capabilities. With AI development under watchful control, its adoption and widespread benefits will gain societal trust and lead to stronger cyber resilience in the following ways:

Cyber protection

With the various aspects of AI such as machine learning, large language models, intelligent automation and natural language-based processing, defenders can offer:

1. More targeted and personalised security awareness training.
2. More efficient and focused analyses of huge amounts of threat data.
3. Fast correlation of signals across multiple attack surfaces to detect and halt attacks effectively and pre-emptively.
4. More accurate reports and analyses of data and network traffic for enhanced system observability.

Broader range of protection capabilities:

Against attacks involving account credentials, network compromise, lateral movement, data exfiltration, ransom demands.

Cyber talent training and skills force development

Generative AI can enhance training content, boost trainee performance, enhance training retention, reinforce on-the-job training efficacy, and encourage continual learning of cyber defence skills and tactics.

When coupled with AI-powered SASE architecture, AI continually improves key cybersecurity parameters

While Secure Access Service Edge solutions form a good foundation for cyber resilience in the age of advanced AI threats, a best-in-case SASE solution would incorporate cutting-edge AI that:

- Enables strong protection of remote and hybrid work activities.
- Strengthens security posture and reduces known and unknown risks.
- Improves system performance and reliability as compared to non-AI-enhanced solutions.
- Reduces complexity and simplifies cybersecurity management.
- Reduces dependence on specialised in-house resources.
- Reduces the Total Cost of Ownership (TCO) and improves return on investments.
- Identifies the 'needle in the haystack' and delivers efficiency with automation in a heavily distributed network infrastructure that exposes users, devices, and data to threat actors.
- Identifies misconfiguration and blind spots in security postures where only AI models can identify and remediate at machine speed to remove the threat.
- Using natural language to retrieve crucial information needed in triggering actionable alerts.
- AI can speed up detection with AI inferences on user behaviour to accelerate Zero Trust based access controls.
- All of the benefits of AI with SASE will create efficiency and savings for TCO.

When coupled with comprehensive XDR+24/7 SOC integrated solutions, cutting-edge AI can reduce cyber incident resolution time

Best-in-class XDR solutions, such as those from Barracuda, can reduce the resolution times for the following incidents from months or weeks down to mere hours.

How long does it typically take for resolution		
	Without XDR	With XDR
Typical BEC resolution (gateway only)	1 – 2 months	1 – 2 hours
Identity theft resolution	3 – 4 weeks	1 – 2 hours
Malware infection resolution	3 – 4 weeks	~ 1 hour
Insider threats resolution	3 – 6 months	~ 4 hours
Extortion resolution without XDR	Variable	> 24 hours

AI cybersecurity leaders can stay ahead of the generative AI maturity curve to help keep AI-empowered cyber threats in check:

- Strengthen software development security practises as well as secure Cloud and API usage
- Perform real-time detection and blocking of suspicious URLs in all forms of corporate communications and social engineering contexts
- Engage governments and the community in safeguarding all aspects of ethical AI use

In the other corner of the ring, the bad actors have all forms of AI at their disposal. The technology can improve their capabilities in terms of scale and speed of attack, evasiveness, and efficacy in discovering vulnerabilities and potential exploits in target systems. Therefore, we have to find ways to emulate the bad actors. On a grander scale, the world should recognise that in addition to human greed, the historical lack of global peace, equality and unity is what often drives good people to turn to criminal activity.

Is AI being put to optimal use in cyber defence?

All of the benefits that cybercriminals gain with AI are meant to exploit the current weak links in cybersecurity involving:

- Organisational ignorance, misunderstanding and complacency in strengthening and maintaining a best-in-class security posture.
- Continued use of legacy systems and complex infrastructures with little or no room left for upgrading and futureproofing.
- Non-holistic and fragmented threat detection and response, coupled with weak links in cloud configuration, software supply chain security and risk management.
- Organisational misconceptions and unrealistic expectations when juggling the benefits of AI-driven productivity and cybersecurity solutions — leading to the lack of cybersecurity-first corporate culture and vulnerability to human-linked errors in cyber vigilance.
- Inappropriate selection and choice of the most appropriate AI-empowered digital transformation and cybersecurity solutions for the organisation's unique needs — leading to non-optimal implementation of IT investments, as well as human error in the usage and training of employees for optimal returns on investments and risk elimination.

Cybercriminals and state-sponsored threat actors know and understand the motivations and factors causing the abovementioned weak links to exist and resist mitigation. Therefore, in the AI-powered fight, good actors need to address the two sets of threats covered in this Special Report so far:

1. Every aspect of the Top 5 threats that risk plunging the world into an escalating cyber war, with AI likely to give lawless opponents the upper hand.
2. The 5 weak links in AI adoption, implementation and culture that compromise the full potential of AI-defence and impede efforts to correct systemic errors and management indecision.

In the next two pages, we will examine the various aspects of addressing the two sets of threats that industry decision makers have personally faced and conquered with the right evangelism and technology.

The AI vs AI frontier in cyber defence

In October 2023, a roundtable discussion was held in Singapore on the topic of “Cybersecurity in the age of AI”. Organised and hosted by CybersecAsia and Barracuda Networks, the roundtable aimed to discuss the democratisation of AI among consumers and businesses in Asia; its impact on the threat landscape in this region, including the standout threats organisations face today, and how defenders are employing AI in defence.

Hosted by Fleming Shi, former Chief Technology Officer, Barracuda Networks and moderated by Victor Ng, Editor in Chief, CybersecAsia, the roundtable was attended by 14 IT security decision makers from Singapore-based firms across a wide range of industries, including (in alphabetical order) Adval Tech Holdings, Bayonics International, Bilcare Singapore, Containers Printers, Dou Yee International, JP Morgan, Meranti Power, National University Health System (NUHS), Navig8 Asia, Schneider Electric, Starhub, Tai Cheong Steamship & Co., and The Hour Glass.

In exploring the top threats of the current cybersecurity landscape and the non-optimal adoption of AI and automation, some key insights, opinions and conclusions were gathered from the participants.

- **It's an AI vs AI arms race out there**

Artificial intelligence (AI) has been around for decades, but with the public introduction of generative AI models in late 2023, we are witnessing the democratisation of AI among consumers and businesses in the region. AI is transforming the world of cybersecurity and the likely evolution of the threat landscape at a remarkable pace. Combining the power of machine learning, neural networks and generative AI, cybercriminals are now able to strike faster and with better accuracy. Cyber-defenders need to respond in kind – so it's an AI-versus-AI arms race out there.

- **Weak links in AI adoption and implementation need to be addressed**

With cumulative financial losses from cyberattacks projected to reach US\$10.5tn by 2025, global investments in cybersecurity need to measure up to avoid giving bad actors the upper hand. Participants agreed that financial losses are likely to continue unless weak links in AI adoption and implementation are addressed.

- **Lack of visibility continues to undermine security efforts**

Many of the roundtable participants noted that their IT and research teams were often unaware of how many APIs were running in the cloud at any one time. This is a signal that observability, as compared to strong network visibility, is still an Achilles heel for many organisations with supposedly modern cybersecurity infrastructures. Roundtable participants unanimously agreed that AI, when implemented optimally and used in a cybersecurity-first corporate culture, would lead to superior observability and as a result — superior cyber readiness and resilience.

- **The skills gap is felt**

The 2023 ISC2 Cybersecurity Workforce Study, highlights that when it comes to the global cybersecurity workforce, demand is still outpacing the supply. Roundtable participants acknowledged feeling this constraint themselves, whilst acknowledging that the intersection of AI and cybersecurity requires a specialised skill set. They also agreed that a lack of cyber talent in this region undermines the region's cyber resilience, and in particular, the ability of small-to-medium-sized enterprises to establish cybersecurity best practises and teams. The concept of CISO-as-a-Service was briefly tabled as a potential short-term measure while economic strain limits manpower investments. There was a general consensus however that CISO-as-a-Service requires highly specialised consultants with industry-specific knowledge, so may not be applicable to all industries or scenarios.

- **Shying away from AI is not the answer**

While the potential trajectory of AI is uncertain, the roundtable participants agreed that shying away from AI adoption is not the answer. They acknowledged that such a reluctance could have severe consequences for business and diminish the prospects of the good actors winning the AI war. As one of the fastest-growing regions globally, characterised by extensive connectivity and rapid technological adoption, Asia-Pacific is a prime target for cyber terrorism. The region faces significant economic risks if cyber resilience standards were to decline.

- **The C-Suite needs to be persuaded to invest**

While participants acknowledged the benefits of AI-driven productivity and cybersecurity solutions, they noted that investing in AI is not cheap, and returns on investments need to be high enough and come with a level of certainty to justify management-board approvals. For SMEs, participants agreed that the key consideration is often lack of budget – with or without management board support. CISOs at the roundtable concluded that citing convincing case studies of financial damages and business collapse resulting from cyberattacks was the only practical way to convince upper management to allocate the funds necessary to address top cybersecurity threats.

- **More public / private collaboration is necessary**

As cyber threats continue to escalate, increased collaboration between the public and private sectors will be crucial. By pooling resources, expertise and intelligence we can enhance our collective ability to anticipate, mitigate, and respond to cyber threats.

- **Business priorities come first**

In a debate over whether IT/cybersecurity considerations should dictate business IT investment decisions or if broader business priorities should take precedence, the panel unanimously agreed that the latter should be the guiding principle for IT/cybersecurity investments. This consensus arises from the acknowledgement that the viability of the business is paramount, as cybersecurity becomes inconsequential if the foundational integrity of the business is compromised.



Top 10 takeaways

While both defenders and attackers continue to leverage AI technologies, we are at a point where attackers may be on the verge of gaining an advantage unless significant action is taken. The proponents of ethical AI find themselves trailing in the development, deployment and use of AI, with the potential for an even wider gap given the current landscape of super-inflation, geopolitical hacktivism, and state-sponsored cyber warfare.

In order to narrow this gap and take the lead in the AI race, it's clear we need to:

1. Galvanise the public and private sectors in recognising that the bad actors are currently winning the AI race in order to boost critical resources through increased collaboration, stricter regulations, and more funding to counteract opponents' advantages.
2. Address top cyber threats by increasing funding and support of public awareness programmes, cyber education and certification, whilst tightening cyber resilience policies to mandate a security-first culture at all levels of society.
3. Address key weaknesses in AI adoption, implementation and culture. Given the resounding concern by AI pioneers that there is a strong potential of AI going rogue or being weaponised in future, the principles of ethical AI use and restrictions should be ironed out and enshrined in all AI development globally. This will ensure that cautious trust in AI will be nurtured worldwide, leading to accelerated adoption and implementation to counter
4. The above factors will require time to take root. In the meantime, organisations should observe cybersecurity best practises and take a Zero Trust, security-first approach in every aspect of their operations.
5. As technology and optimal use of AI narrows the digital divide and drives financial inclusion, the world must be even more committed to protecting the new entrants to the digital world, as they could easily be a new vector for threat actors to exploit.
6. Even when organisations "follow the book" on cybersecurity, SecOps, DevSecOps and AI best practises, human factors can still be exploited to poke holes in the system defences at the most inopportune times. This human factor is one of the key points of weakness that threat actors constantly seek out — with or without AI. Similarly, cyber defenders need to constantly review all end points with full visibility (observability) on a single-pane-of-glass and use AI to pull multiple signals together to enhance pre-emptive cyber defence.
7. When points of attacks meet with failure, cybercriminals may resort to deep fakes, impersonation, brute-force attacks, and supply-chain weak links. AI-powered SASE, managed XDR with round-the-clock SOC, and the TINA Tunnel, are promising ways to address such vectors automatically and alert defenders (using large language models of billions of cyber incident cases to filter alerts and avoid causing unnecessary alert fatigue) for prompt intervention.
8. When defences still give way, a well-implemented best-in-class AI-powered cybersecurity XDR solution can prove useful in drastically reducing recovery time, blast radii, amount of data/funds lost, and increasing the speed of data restoration and resumption of services.
9. Recognise that SMEs and MSMEs need the most help as they form the bulk of supply chains to all other organisations. With their limited funding and cyber talent, they are low hanging fruit for AI-empowered cyber threat actors. Their cybersecurity is the lynchpin of a whole-of-national community approach to staying cyber resilient.
10. The unanimous all-encompassing conclusion of the roundtable panel is that the dictates of basic business/organisational survival supersede all other considerations. If a business cannot stay relevant survive competition and cyberattacks, then no amount of IT investments can salvage it. Therefore, businesses of all sizes should strive to leverage IT and AI to boost competitiveness, survivability and sustainability. The side benefit is that this enhanced level of technology adoption (while an technologically-lagging business is still viable) predisposes any organisation to easier implementation of optimal AI cybersecurity along the way.

We at CybersecAsia.net and Barracuda Networks hope that this Special Report has provided enough compelling evidence to set you on the right path when it comes to your organisation's responsible AI adoption.

In light of the rapid advancements in artificial intelligence, it is paramount that we take proactive measures to implement policies and regulations aimed at ensuring the safety of AI systems. The potential consequences of unchecked AI development pose significant risks, ranging from privacy breaches to unintended consequences in critical systems. By establishing robust frameworks and ethical guidelines, we can mitigate the potential harm associated with AI technologies. Collaboration between governments, industry stakeholders, and experts is crucial in striking a balance between innovation and safety. Emphasising transparency, accountability, and responsible AI practises will not only safeguard individuals and societies but also foster trust in the continued evolution of artificial intelligence. As we navigate the complex landscape of AI, prioritising safety measures is fundamental to harnessing the benefits of this transformative technology while minimising its associated risks.

We leave you with some thought-provoking quotes:

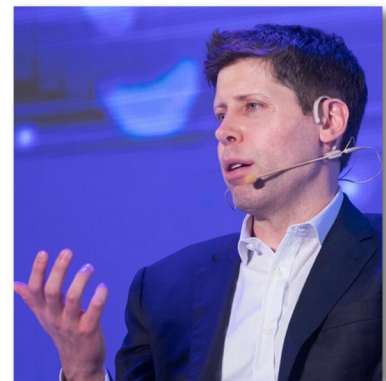


"Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks."

Late Stephen Hawking, Theoretical Physicist

"AI will probably most likely lead to the end of the world, but in the meantime, there'll be great companies."

Sam Altman, Chairman of OpenAI



"Mark my words, AI is far more dangerous than nukes...why do we have no regulatory oversight?"

"AI is a rare case where I think we need to be proactive in regulation than be reactive."

"The biggest issue I see with so-called AI experts is that they think they know more than they do, and they think they are smarter than they actually are...This tends to plague smart people. They define themselves by their intelligence and they don't like the idea that a machine could be way smarter than them, so they discount the idea — which is fundamentally flawed."



Elon Musk, Technologist, inventor, businessman and investor

About Barracuda

At Barracuda, we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.



About CybersecAsia

In the digital economy, with the pressing need to digitally transform, business and technology leaders across the Asia Pacific know that cybersecurity cannot be an afterthought in their transformation journey. However, the cyber-threat landscape is constantly evolving. To help address this critical challenge, CybersecAsia is the region's most trusted source of enterprise cybersecurity information and thought leadership.



About Thinklogic Media Group

Thinklogic is a leading B2B demand-generation company, leveraging Asia Pacific's growing database of enterprise decision-makers. We help enterprises technology solution provides grow by driving demand and awareness through our niche online publications and bespoke marketing methodology. Our tech media sites include Cybersecasia.net, Digiconasia.net and Martechasia.net, which focus on cybersecurity, digital transformation, and marketing technology respectively. Visit us at www.thinklogicmediagroup.com.



Dexter Low

Director of Media and Partnerships

Reinwel Decina

Chief Executive Officer

Iris Carliy Lauron

*Campaign and Operation
Assistant Head*

Victor Ng

Editor-in-Chief

Mae Alagos

Chief Operating Officer

John Kennet Padinit

Graphic Designer