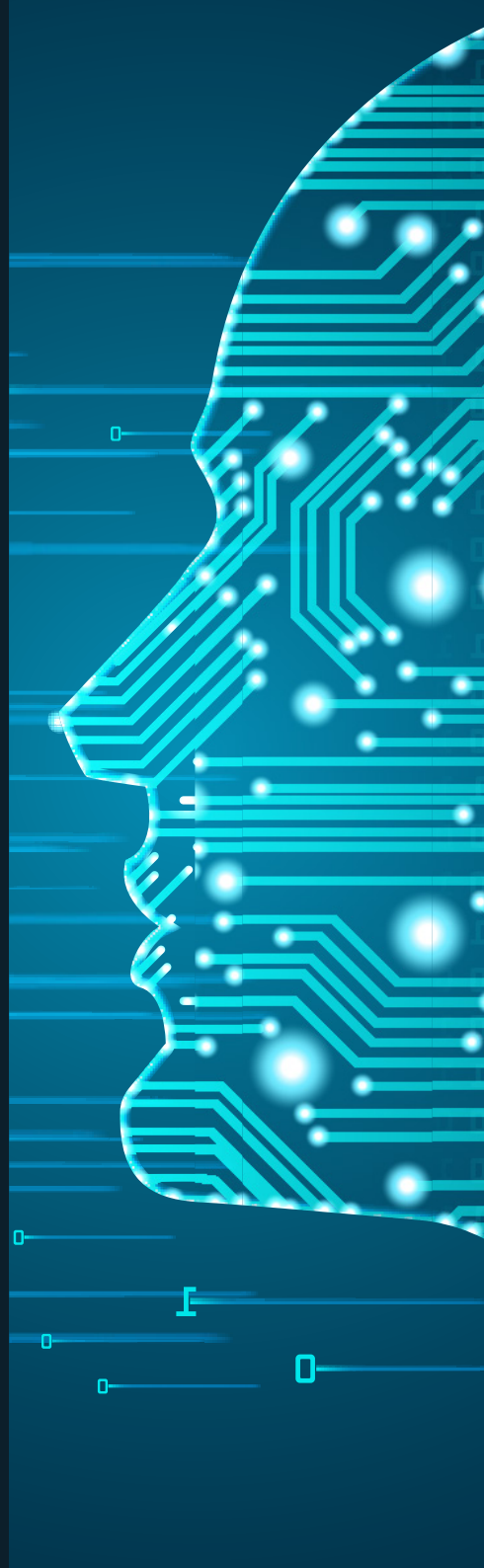
WHITEPAPER | APRIL 2023

CYBERSECURITY LEADERS' FORUM

Building cyber resilience and leveraging cyber governance



Infosys® | InnovationAus.com
PUBLIC POLICY AND BUSINESS INNOVATION

Introduction

Given the frequency and variety of increasing cyber-attacks, it is imperative to progress beyond cybersecurity towards building cyber resilience and leveraging cyber governance, to thwart attackers before they strike.

Apart from being proactive, cyber resilience differs from the old approach by accepting that security incidents are inevitable. With that acceptance, it focuses on improving detection, alertness and response in those situations.

Large enterprises are protecting customers, citizens and assets with artificial intelligence, robotic process automation and the Internet of Things in threat assessments.

Organisations are building robust risk management frameworks and prioritising cyber investments to meet their objectives against a heightened threat landscape.

Corrie McLeod, Publisher of InnovationAus.com, led a discussion between a senior group of chief information security peers from industry and government around building cyber resilience strategies and leveraging cyber governance frameworks to bolster board-level program support.

Vishal Salvi, Senior Vice President, Chief Information Security Officer, and Head of the Cyber Security Practice at Infosys discussed global trends and insights. Vishal leads a team of more than 4,000 cybersecurity professionals at Infosys, a company which employs 345,000 people globally.

Attendees

Ben Willis, CTO at MadeComfy

David Sandell, CEO and Managing Director at CI-ISAC

Derek Chen, CISO at Toll Global Express

Doug Hammond, CISO at Uniting

Mark Smink, Executive Director, Head of Global Cyber Governance Risk and Compliance at JLL

Rajinder Rathor, Cyber Security - Practice Lead at Infosys

Richard Williams, CIO at MoneyMe

Vikas Tatwani, Associate Vice President & Head - APJ (Cloud, Infrastructure & Security Services) at Infosys

Vishal Salvi, the Senior Vice President, Chief Information Security Officer, and Head of the Cyber Security Practice at Infosys

Moderator – **Corrie McLeod**, Publisher, InnovationAus.com

Closing the skills gap

In terms of closing the widening skills gap and how to address it, creating more proactive and simplified cyber-risk reporting and governance systems and supply-chain security is imperative.

Australia has a well-documented shortage of cyber skills, and this is across both government and the private sector. This in part is due to the fact that the spectre of cyber should be viewed as society-wide. Every industry has a role to play to evangelise, draft and nurture talent.

In this respect, education about cybersecurity needs to start early, where risk needs are taught and understood via technological training to democratise it. At a tertiary level, certain cybersecurity and/or cyber resilience standards should be mandatory for practitioners of IT careers.

In practice, the adoption of automation technology continues to surge. How useful is it to address the cyber skills shortage and how are organisations maximising their available human skills? Are there unintended consequences that we need to be mindful of?

The shared services model is the future of this industry. We are no longer managing and imitating large data centres. Everybody is adopting cloud strategy because it's easier to migrate, cost-effective, elastic, portable and transaction based.

Cybersecurity needs to emulate this practice to achieve a network effect – to create a capacity where everybody can use and share these resources.

Ultimately, in terms of the skills shortage, it should not be a case of 'throwing more people at it', but rather allowing artificial intelligence technologies to do what they do best (i.e. efficiently and cost-effectively automate processes). This will not only save time and money, but employ a level of speed and accuracy that is often beyond the realm of human capability.

"There is a misnomer or misconception about cybersecurity that it's rocket science. It is not. It's a very simple problem and solution to understand. It's a question of embracing it, taking accountability, ownership and trying to learn what needs to be done."

– Vishal Salvi, Senior Vice President, Chief Information Security Officer, and Head of the Cyber Security Practice at Infosys

State of compliance

With the state of compliance already so complex, companies are compelled to navigate the future environment and plan ahead; and implement governance frameworks that can be used to reassure boards about resourcing, and to shape business decisions.

In Australia, we hear from cybersecurity leaders that compliance can often be complex, with multiple frameworks to comply with, depending on who your partners and customers are.

From a global perspective, is the industry seeing geographic areas where there has been more consolidation in these frameworks – making it easier for cyber teams to comply and better deploy team resources?

Companies have all these compliance 'hoops' to jump through – but hackers don't have the same restrictions – they can just test and iterate to get the outcomes they want. This creates an extra level of burden in terms of compliance and auditing expectations.

"Since neither data nor the workforce is restricted within enterprise boundaries, security needs to go from being network-centric to become user-centric. Indeed, this is the basic principle of zero-trust architecture (ZTA), which seeks to safeguard users, resources and assets where they are, instead of protecting static perimeters."

– Vishal Salvi, Senior Vice President, Chief Information Security Officer, and Head of the Cyber Security Practice at Infosys

Dynamic change is occurring in this area. Smaller, less resourced companies are often quicker to respond to this need for organisational or two-team change, but they must also budget for compliance costs, which can be challenging.

A solution may be the division of teams into compliance and regulation versus mitigation, if you're resource poor and time poor in a particular cyber area.

Future-proofing is another matter altogether when a company has the finances to do so, regardless of the necessity for dynamic change at a board level. However, questions remain about the veracity of compliance because certifications that companies must adhere to today, they could be in breach of tomorrow.

The regulators will always be behind the industry or risks by two or three years. So, the question remains: where does the industry need to be to negate the risk of cyber breaches while still complying with the regulations?

Reframing challenges and building resilience

Governance strategies that reframe challenges and build resilience must adopt a mindset of not 'punishing the victim', while also ensuring that companies conduct due diligence to thwart attacks.

Beyond protecting a business's vulnerabilities and planning ahead to mitigate risk, cyber frameworks can also be a competitive advantage in the context of environmental, social and governance (ESG).

Australia has seen a flurry of high-profile data breaches — which no doubt is replicated across the world. Given that the reasons for some of these breaches were quite simple, does this indicate that the fragmentation of compliance frameworks means they are no longer working?

Overcoming this challenge comes down to the proactivity versus reactivity of a company. Having an enterprise risk-management structure is all well and good, but how long does the structure take to implement without being outdated or even redundant? This area of effective and flexible risk management needs to be stronger than ever.

CI-ISAC (a not-for-profit organisation that supports and promotes existing legislation and government initiatives that are working to uplift cyber resilience across critical infrastructure sectors) is a fitting example.

Why should the industry come together? Pooling our resources creates a common framework and allows everybody to contribute and consume.

Boards can have all the compliance ticks and approvals in place, but that doesn't mean they are immune to or even combative against the sophistication of hacking techniques.

It's one thing to have the right processes in place, but quite another to employ the skillset to operate and balance the procedural and compliance dichotomy.

This is where CI-ISAC enters the equation to 'provide the governance and trusted, independent, structured set of enabling capabilities to harness the collective power of Australian organisations to work together to defend against cyber attackers'.

"(In light of these high-profile breaches), the conversation is now 'I want to see what you're doing with my data before I give it to you'. And that never happened before."

— Ben Willis, Chief Technology Officer at MadeComfy

Trust and security

Trust and security are a key part of ESG – according to the ESG Radar Report, which Infosys launched this year. These attributes have shifted from 'nice to have' to 'must have', and cyber plays a clear role in both the social and the governance of ESG.

Are boards understanding this, and are there quality discussions taking place about how cyber is further elevated to meet the challenges of ESG? The answer is: yes and no.

The time for execution is upon us. A vast majority of cyber leaders have developed cybersecurity and cyber-resilience strategies, but now it is a matter of putting those plans into action.

Building operational context allows for executive decision-making to act within organisations.

As enterprise workloads increasingly move into the cloud, and the remote work model sustains, the traditional practice of securing the network perimeter is no longer effective.

Given this realisation and the need to often act promptly and abidingly, your cyber strategy needs to align with compliance mandates.

Thus, the data privacy issue is timely in the ESG sphere — and is categorised as conscious bias versus unconscious bias.

Identifying the types of threat sharing helps to overcome the challenges of negating those threats. In short, there are three levels of threat sharing:

1. Yes, you want to share
2. You don't want to share too much, because you don't want to let your adversaries know what's happening, and
3. With whom should you be doing the sharing — police or intelligence agencies?

The challenge with the third level is because these enforcement agencies work to a different bureaucratic rhythm, they need to be sure that it's a problem before they act. And by that time, it's often too late.

Consumers and practitioners are demanding a trusted environment to share relevant information at the regulatory level. This will ensure the safeguarding and encouragement of threat sharing.

"Risk management is fundamental to everything that we do. How do you get to what your risks have to be relative to your control position? Having that threat-informed view, you can be more proactive, understand the threat's relevance, figure out what your position looks like (i.e. your residual risk position) and that's what you base your counter decisions on."

— David Sandell, Chief Executive Officer and Managing Director at CI-ISAC

Conclusion

Critical infrastructure and cyber responsiveness are the tools to build cyber resilience and leverage cyber governance.

Imagine the impact of centralisation on value creation.

Leveraging the network effects of shared critical infrastructure in a safe environment is paramount. Just as cyber threats are not sector specific, there is an industry-wide consensus to use the network experience of mature players to help lesser-resourced or informed small-to-medium enterprises – particularly those downstream providers that don't consider themselves to be affected by the new legislation.

Recognising the key attributes of the hacker profile are crucial when anticipating cyber-attacks and executing strategies to thwart them before the damage is done.

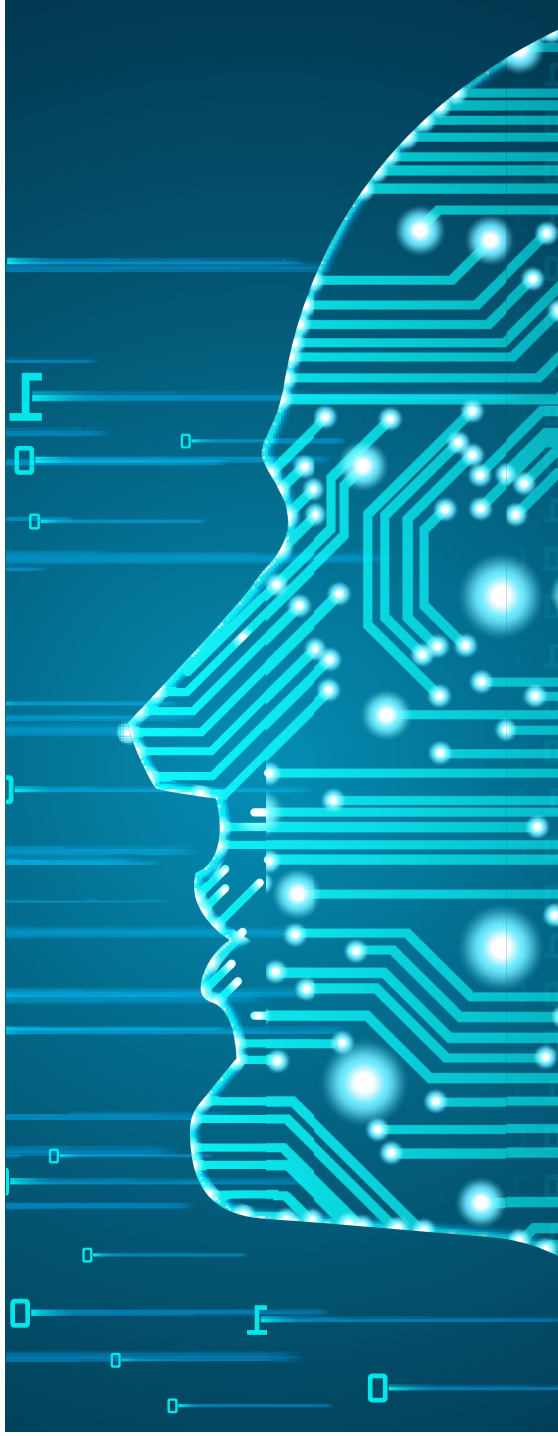
Hackers are becoming more plentiful, uniform and professional. From the consumer-level hacker to the non-paid services hacker to vendor hackers (who commoditise demand in skills due to consumer hackers), the hacking community represents an increasingly vicious cycle.

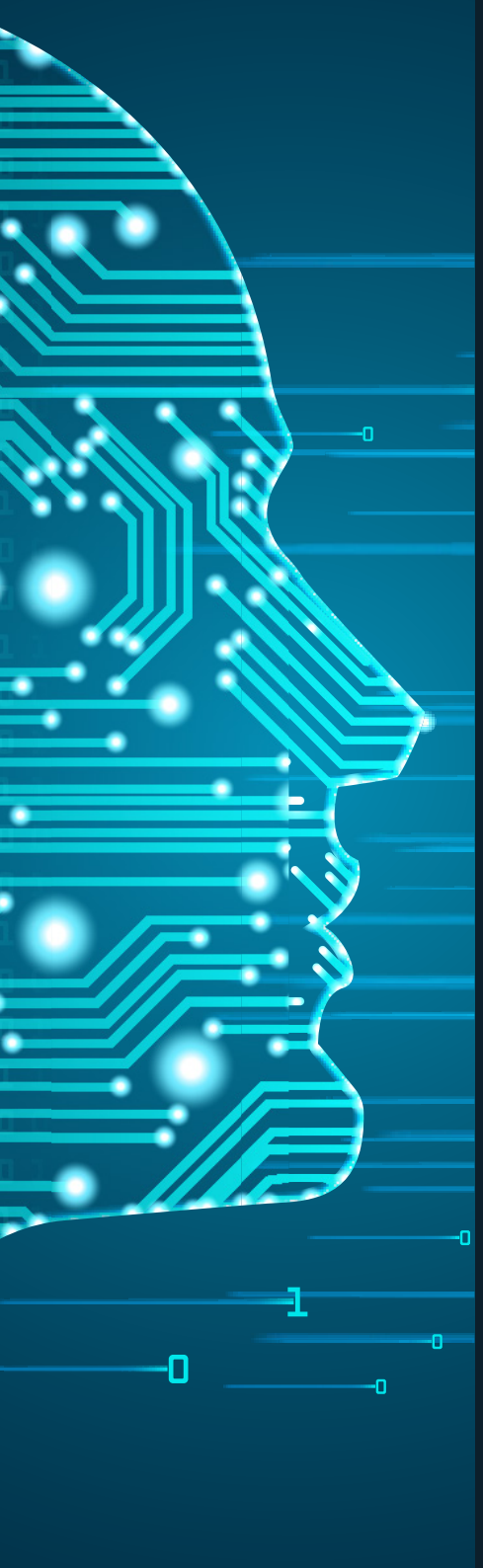
Identifying the types of threat sharing helps to overcome the challenges of negating those threats. The three critical threat-sharing types are:

1. Agreeing to threat sharing
2. Reticence to share for fear of divulging too much sensitive information to your adversaries
3. Querying which enforcement agencies to share the threats with due to the inadequacy or insufficiency of their response methods or capabilities.

Questions remain about whether the legislation and compliance that organisations must follow to meet their objectives of cyber resilience are working, given that cyber criminals don't have the same restraints, so their options are wide open.

Therefore, the major takeaway of the group discussion calls for a middle ground between government and the private sector, to effectively regulate cyber compliance and mitigate the risk of threats.





For further information, please contact:

Corrie McLeod
Publisher
+61 419 526 848
corrie@innovationaus.com

Infosys®

InnovationAus.com
PUBLIC POLICY AND BUSINESS INNOVATION