13 June 2024

ASIAL
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
The peak body for security professionals

Attn: Chair, Inquiry into the capability of law enforcement to respond to cybercrime

Response to question on notice

ASIAL's opening statement to the public hearing on the 23rdMay 2024, provided two examples of cybersecurity professionals who had access to their client's data. Both examples resulted in a cybercrime, where the individuals were later convicted in court. These examples are why ASIAL strongly advocates mandatory criminal background checks for cybersecurity professionals who perform work for others, which is no different from physical, protective and electronic security.

Specific to the question on notice, implementation of compulsory criminal probity checks for individuals working in cybersecurity (especially those performing work for others) will enhance law enforcement capabilities in several ways. However, doing nothing will have profound negative consequences for businesses and the community throughout Australia as cyber-criminals seek to exploit vulnerabilities in our current arrangements.

The absence of mandatory probity checks for individuals working in cybersecurity roles has raised concerns about the potential risks associated with entrusting sensitive information and critical systems to individuals who have not undergone a thorough vetting process. The lack of consistent stringent screening measures has contributed to growing unease among stakeholders about the vulnerabilities that may arise from employing individuals with questionable backgrounds in positions where they have access to highly sensitive data and systems.

One of the primary arguments in favour of implementing probity checks for cybersecurity professionals is rooted in the critical nature of their roles in safeguarding digital assets and infrastructure (as noted in Shield 4: Protected critical infrastructure of the 2023-2030 Australian Cyber Security Strategy). Cybersecurity professionals are entrusted with protecting organisations, governments, and individuals from many cyber threats, including data breaches, hacking attempts, and other malicious activities. Given the pivotal role they play in maintaining the security and integrity of digital systems, it is imperative to ensure that these individuals possess the highest level of integrity and trustworthiness. Conducting probity checks can proactively mitigate the risks associated with potential insider threats and malicious intent among cybersecurity personnel.

Moreover, the evolving landscape of cyber threats and the increasing sophistication of cyber-attacks underscore the need to uphold stringent security protocols within the cybersecurity workforce. As cyber adversaries continue exploiting vulnerabilities (see page 12, 2023-2030 Australian Cyber Security Strategy) in digital systems for financial gain, espionage, or sabotage, a robust and resilient cybersecurity workforce becomes paramount. By instituting mandatory probity checks for cybersecurity professionals, organisations can enhance their security posture and minimise the likelihood of internal threats compromising their defences.

Security Industry House PO Box 1338 Crows Nest NSW 1585
P: 1300 127 425 **E:** security@asial.com.au
ABN 91 000 813 365
www.asial.com.au

From a regulatory and compliance standpoint, the absence of standardised practices for conducting probity checks on cybersecurity professionals poses challenges in ensuring adherence to industry standards and best practices. The 2020-2030 Australian Cyber Security Strategy, page 13 states “One of Australia’s core strengths is our robust legislative system. Our strong legislative and regulatory frameworks will help enforce new cyber security standards”. Regulatory frameworks across other countries have advanced, such as the European Union’s General Data Protection Regulation (GDPR) and the United States of America’s Health Insurance Portability and Accountability Act (HIPAA), which mandate stringent data protection measures and confidentiality requirements for organisations handling sensitive information. Failing to vet cybersecurity professionals through probity checks may expose organisations to regulatory non-compliance and legal repercussions in cases where there is a data breach or security incident involving personnel with undisclosed criminal histories.

Furthermore, the ethical considerations surrounding the trustworthiness and credibility of cybersecurity professionals necessitates a comprehensive evaluation of their backgrounds to ascertain their suitability for handling sensitive information and critical infrastructure. In an era where data privacy and confidentiality are paramount concerns for individuals and organisations alike, cybersecurity professionals' integrity and ethical conduct are pivotal role in fostering trust and confidence in the digital ecosystem, no different to physical, protective or electronic security.

Implementation of the requirement for probity checks as a pre-requisite for cybersecurity professionals will assist in strengthening protections to safeguard the community.

The potential ramifications of overlooking the importance of probity checks for cybersecurity professionals extend beyond organisational security concerns to encompass broader societal implications. In instances where cybersecurity professionals with undisclosed criminal backgrounds are entrusted with safeguarding critical infrastructure such as power grids, financial systems, or healthcare networks, the repercussions of their actions could have far-reaching consequences for public safety and Australia’s national security. The interconnected nature of digital systems underscores the need for a comprehensive approach to vetting individuals in cybersecurity roles to prevent malicious actors from exploiting vulnerabilities for nefarious purposes.

Moreover, the risks associated with employing cybersecurity professionals without conducting thorough probity checks will tarnish the reputation and credibility of organisations in the event of a security incident or data breach attributable to insider threats. Public trust and confidence in the ability of organisations to protect sensitive information and uphold cybersecurity standards are contingent upon the diligence and rigour with which personnel are screened and vetted for their roles. By prioritising implementation of probity checks for cybersecurity professionals will result in greater transparency, accountability and more thorough due diligence in mitigating risks associated with insider threats and malicious activities within their workforce.

With increasing convergence of physical and digital security threats, the imperative to fortify cybersecurity defences through comprehensive probity vetting processes for personnel is a pressing priority. The interconnected nature of cyber-physical systems, Internet of Things (IoT) devices, and critical infrastructure underscores the need for a holistic approach to cybersecurity that encompasses technological safeguards and robust personnel security measures. Probity checks serve as a core foundational component of a multi-layered security strategy aimed at mitigating risks associated with insider threats, social engineering attacks, and other forms of malicious behaviour that could compromise organisational security and resilience.

Furthermore, the prevalence of insider threats in cybersecurity incidents highlights the vulnerabilities that can arise from overlooking the significance of vetting personnel through probity checks. Insider threats, whether perpetrated out of malice, negligence, or coercion, pose a significant risk to organisations' cybersecurity posture and can result in substantial financial losses, reputational damage, and legal liabilities. By proactively screening cybersecurity professionals for any red flags in their criminal histories, organisations will be able to pre-emptively identify individuals who may pose a threat to their security infrastructure and take appropriate measures to mitigate the risks associated with insider attacks.

Implementing probity checks as a pre-requisite requirement for cybersecurity professionals aligns with industry best practice and standards for ensuring the integrity and trustworthiness of personnel entrusted with safeguarding digital assets and information. As cyber threats evolve in complexity and scale, the need for a vigilant and resilient cybersecurity workforce equipped with the necessary skills, expertise, and ethical standards has never been more critical. Incorporating probity checks as a pre-requisite for cyber security professionals will enhance organisations risk management strategies and bolster their defences against internal threats that may compromise their cybersecurity resilience.

Moreover, the ethical considerations surrounding protecting sensitive information and preserving individuals' privacy rights underscore the importance of conducting probity checks in a transparent, fair, and non-discriminatory manner. Organisations must adhere to legal and ethical guidelines governing probity checks in the hiring process to ensure compliance with anti-discrimination laws, data protection regulations, and privacy rights. By establishing clear policies and procedures for conducting probity checks on cybersecurity professionals, organisations can uphold the principles of fairness, equity, and accountability in their recruitment practices while safeguarding the interests of both employees and stakeholders.

In conclusion, the issue of whether cybersecurity professionals should undergo probity checks is a complex and multifaceted matter that warrants careful consideration and deliberation. However, the critical role that cybersecurity professionals perform in safeguarding digital assets, protecting sensitive information, and defending against cyber threats necessitates a comprehensive approach to vetting individuals for their suitability and trustworthiness in these roles.

By implementing mandatory probity checks as a pre-requisite for cybersecurity professionals, organisations will be able to enhance their security posture, mitigate the risks of insider threats, and demonstrate their commitment to upholding ethical standards and regulatory compliance in an increasingly interconnected and digital world. And, as a whole the community will be better protected.