October 2024 | Volume 34 | Number 2

Australasian BioTechnology

The journal of AusBiotech
AUSTRALIA'S BIOTECHNOLOGY ORGANISATION

Australia's golden opportunity for mRNA technology

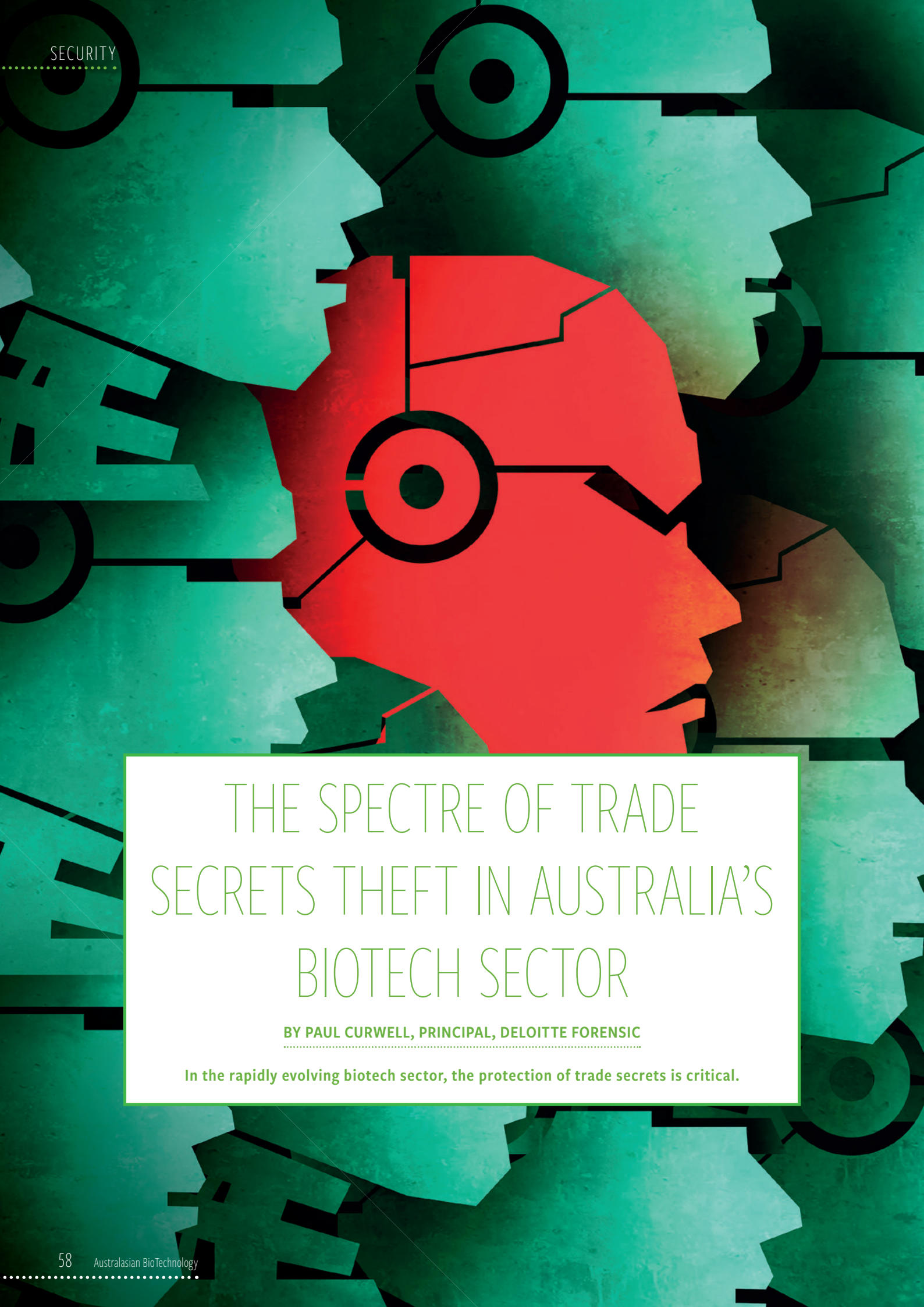
The global renaissance of radiopharmaceuticals

Building and retaining Australian ventures

Australia's biggest week in medtech: showcasing Australia's capabilities

AND MORE...

PRINT POST APPROVED 10101022288



THE SPECTRE OF TRADE SECRETS THEFT IN AUSTRALIA'S BIOTECH SECTOR

BY PAUL CURWELL, PRINCIPAL, DELOITTE FORENSIC

In the rapidly evolving biotech sector, the protection of trade secrets is critical.

Paul Curwell

THROUGHOUT MY CAREER, I've witnessed several instances of trade secrets theft, each highlighting the vulnerability of even the most sophisticated organisations. First, a competitor lured away key researchers from an Australian biotech. This 'talent grabbing' allowed the competitor to rapidly commercialise using nearly patent-ready research. Second, an Australian biotech company partnered offshore to scale its business, only to discover that the partner had a history of research fraud and IP theft. Lastly, a principal researcher secretly established an offshore company to commercialise their employer's research, creating a conflict of interest, and a breach of their employment and grant conditions.

These examples underscore the significant and ongoing risk of trade secrets theft in Australia's life sciences sector; however, these challenges are not insurmountable. By adopting a few targeted strategies, companies can protect their innovations. This article delves into the threats facing trade secrets in Australia's biotech sector, and outlines five practical steps to safeguard your organisation's valuable intellectual property.

Traditional approaches to protecting trade secrets are no longer enough

Trade secrets encompass any confidential information that gives a business a competitive edge, such as proprietary formulas, methods or processes. While laws vary across jurisdictions, Australia relies on common law, unlike the dedicated legislation in the United States, United Kingdom and European Union. In 2018, Australia criminalised the theft of trade secrets on behalf of foreign governments or their agents.

Historically, Australian companies have relied heavily on legal protections like employment contracts, IP assignments and confidentiality agreements to manage IP risks. Unfortunately, these measures alone rarely discourage determined actors. The sophistication and persistence of perpetrators is increasing, prompting the Australian Research Council[1], National Health and Medical Research Council and National Science Foundation[2] to implement Research Security programs to safeguard research and development.

In 2023, the Australian Security Intelligence Organisation launched its Protect Your Research campaign[3] to raise awareness of threats across the scientific community. While cyberthreats, scams, ransomware and data breaches

have increased security awareness, biotech companies face additional challenges from trusted insiders and foreign interference.

Threats to trade secrets are varied, sophisticated and persistent

There is a long list of actors seeking to steal trade secrets. Cyber attacks are most common, but they are not the only threat. Accidental data spills, intentional leaks by employees or suppliers (insider threats), and ill-considered disclosures at trade shows and conferences are common, as is theft involving licensing and foreign direct investment, and by business partners.

International travel and remote work introduce vulnerabilities, with insecure wi-fi and low security awareness posing significant risk. It is not uncommon to hear about documents or samples disappearing during lab tours for prospective collaborators. Once a trade secret is compromised, it is lost forever. A thriving dark web black market brokers stolen trade secrets between current or former employees, competitive intelligence practitioners, criminals and nation-states. So, what can you do about it?

Five simple actions to protect your trade secrets

1. Identify your trade secrets

The first step in safeguarding trade secrets is identifying them. Review your organisation and catalogue data satisfying the trade secret definition. Draft patents should be treated as trade secrets until granted. Understand where records are stored, who has access, how they are marked, accounted for and destroyed, and whether data has been shared with third parties.

2. Identify your risks

Once you've identified your trade secrets, assess their security risks. This includes evaluating cybersecurity risks[4] to your IT networks and devices, but it is equally important to consider risks from people and suppliers. Can IT, contract manufacturer, research, or clinical trial service providers access your trade secrets? How are these secrets protected both contractually and in practice? Do your suppliers prioritise protecting your trade secrets as much as you do?

Don't overlook tangible forms of trade secrets, such as prototypes, samples and paper documents. Once you've identified the risks, compile a Risk Register and develop treatment plans to mitigate them, remembering you need to control any disclosure.

3. Build a strong security culture

People are often the weakest link in security, but they can also be the strongest line of defence. A strong security culture ensures that everyone in your organisation, including suppliers, understands what your trade secrets are, why they need to be protected, and the measures to safeguard them. Leadership must set the tone, and there must be an ongoing awareness program for all staff and suppliers. Induction of new hires is essential. An engaged workforce with a strong security culture is invaluable, while complacency and ignorance are leading contributors to insider risk.

4. Develop a Technology Protection Plan

A Technology Protection Plan (TPP) protects your intellectual 'crown jewels'. The TPP should focus on protecting your trade secrets, outlining roles and responsibilities, onboarding and offboarding procedures, and establishing controls for cyber, data, workforce, facilities, suppliers, and products. If you don't have a plan, start small and prioritise actions with the greatest impact. Don't leave your TPP on the shelf to show investors – implement it by actively managing your risk.

5. Actively manage your risks

It is not enough to simply complete these four actions and review them annually. You need to actively manage these risks as your business grows and adapts to the daily needs of the workforce, customers, and suppliers. This involves appointing someone with ongoing responsibility for trade secret protection, leading responses when incidents occur and providing practical recommendations for managing exposure.

Conclusion

Australia's biotech sector cannot thrive without addressing the threat of trade secrets theft. Implementing effective systems, processes, and workforce practices is essential to protect your innovations, attract investors, and safely scale your business.

Now that you are aware of the spectre of trade secrets theft, what steps will you take to protect your organisation? Share this article with your peers and leadership to raise awareness, and start a conversation about what you can do to safeguard your valuable intellectual property.

Paul Curwell is a Principal in the Deloitte Forensic consulting practice and a lecturer at the Australian Graduate School of Policing and Security, at Charles Sturt University. He holds qualifications in biotechnology, biotech management, fraud and security.

End notes

1 https://new.nsf.gov/research-security

2 www.arc.gov.au/funding-research/research-security

3 www.asio.gov.au/protect-your-research

4 www.cyber.gov.au/resources-business-and-government/essential-cyber-security/protecting-your-business-and-employees.