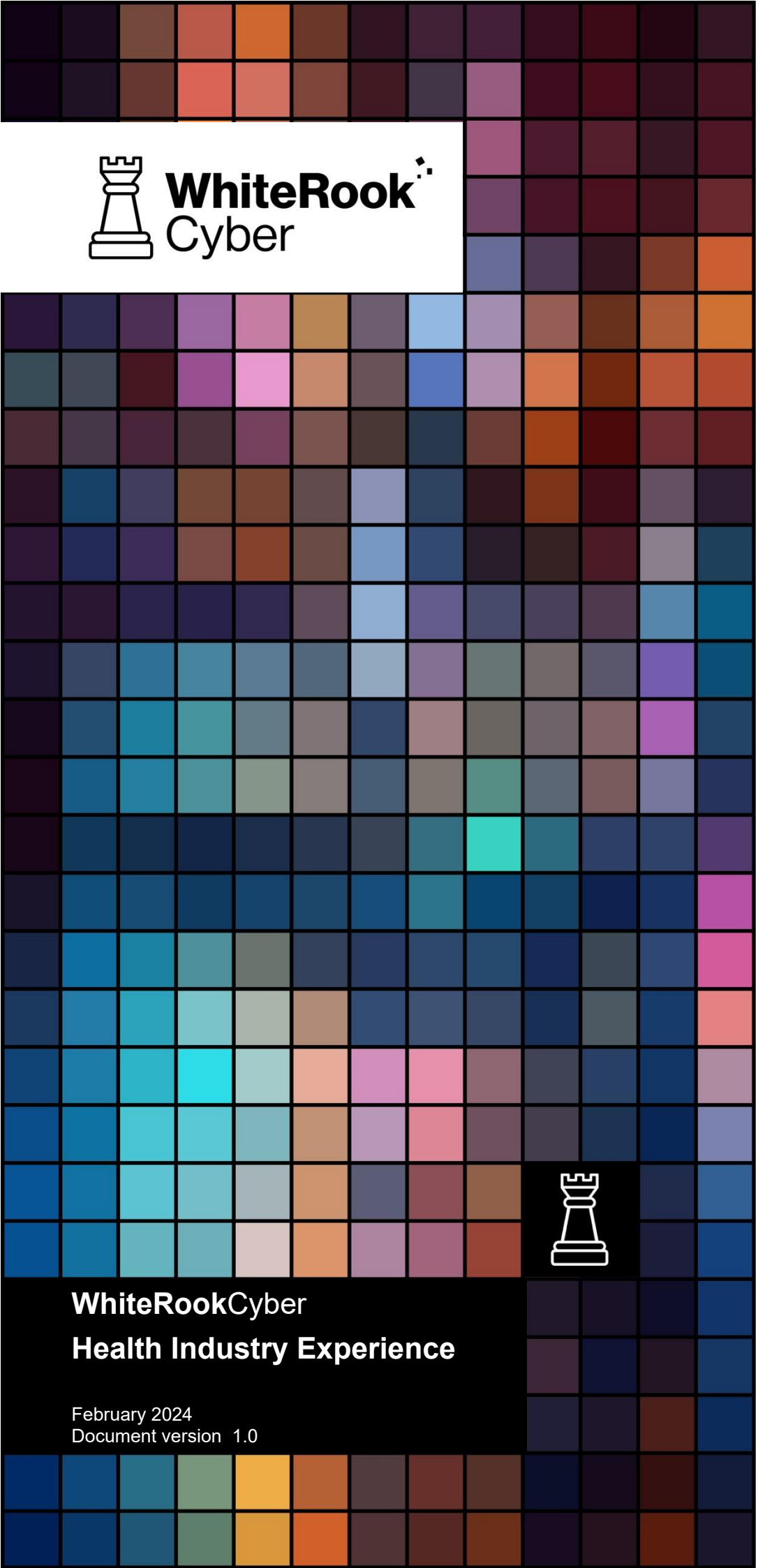


WhiteRook Cyber

WhiteRookCyber
Health Industry Experience

February 2024
Document version 1.0

WhiteRookCyber Health Care Experience

High-level summaries of WhiteRookCyber engagements and experience within the Health care sector.

Cyber Security Services: Advisory

ISO27001 Gap Assessment and Implementation for a Large Technology Provider

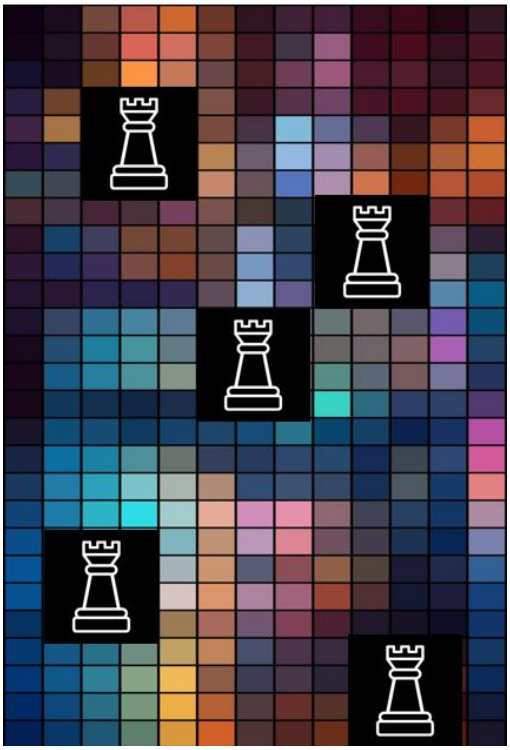
WhiteRookCyber conducted an ISO27001 Gap Assessment and Implementation on a large technology solutions provider in Queensland, Australia. As part of its IT Security & Risk planning, the technology provider decided to focus on its Cyber Security Strategy, including the development of its ISMS against an industry-recognised framework – ISO27001.

This engagement involved helping the technology provider prepare for ISO27001 certification with the objective of using this to demonstrate to current and future clients that the business follows best practice in the delivery of key services, such as its managed service suite of offerings.

As a result of the above, **WhiteRook**Cyber was engaged to perform an ISO27001 Gap Assessment and assist with the associated implementation activities, based on outputs from the initial assessment.

By completing the ISO27001 Gap Assessment, the technology provider was provided with:

- The identification of gaps in the current implementation of the ISMS
- Details of where the client performed strongly against the ISO27001 requirements
- The remediation recommendations mapped to the findings to support the client and provide inputs into the subsequent implementation phase
- A detailed current state assessment of their ISMS



Thanks to the services of **WhiteRook**Cyber, the technology provider was able to:

- Quantify the current state of its ISMS
- Define an implementation plan consistent with the findings and business priorities
- Leverage the **WhiteRook**Cyber consultant's expertise during the implementation phase, facilitating an expedited implementation phase

Cyber Security Services: Advisory

Essential Eight Audit for a Regional Healthcare Network

WhiteRookCyber conducted an Essential Eight Audit on a regional healthcare network (The Network) in Queensland, Australia, serving over 50,000 patients across multiple hospitals and clinics. The network faced growing concerns about its cybersecurity posture, particularly surrounding patient data protection and compliance with the Australian Privacy Act 1988.

Challenges with legacy IT infrastructure, siloed operations, and limited cybersecurity expertise left The Network vulnerable to modern cyber threats, compounded by an increase in ransomware attacks on healthcare organisations, highlighting the need for proactive measures.

The Network partnered with **WhiteRook**Cyber to conduct a tailored Essential Eight audit, focusing on:

- Application Hardening: Assessing and hardening critical healthcare applications (EMR, billing systems) against common vulnerabilities.
- Patch Management: Implementing robust patch management processes to address software vulnerabilities promptly.
- Multi-Factor Authentication (MFA): Enabling MFA for all access points to patient data, including remote staff and administrative accounts.
- Application Whitelisting: Implementing application whitelisting to restrict the execution of unauthorised software on devices.
- Endpoint Protection: Deploying advanced endpoint protection solutions to detect and prevent malware infections.
- Data Backup and Recovery: Ensuring regular backups of patient data and testing recovery procedures for efficient incident response.
- User Awareness Training: Educating staff on cyber hygiene best practices and phishing attack recognition.
- Incident Response Planning: Developing a comprehensive incident response plan to contain and mitigate data breaches effectively.

Thanks to the services of **WhiteRook**Cyber, The Network was able to:

- Reduce its vulnerability footprint as the audit identified required remediation activities for critical vulnerabilities in applications and systems, significantly reducing the attack surface.
- Improved compliance against the Australian Privacy Act by meeting key data security mandates.
- Enhanced user security through the use of MFA to strengthen access control and prevent unauthorised access attempts.
- Increased staff awareness through training programs, which equipped staff to identify and report suspicious activity, bolstering the organisation’s overall security posture.

Cyber Security Services: Offensive

Offensive Penetration Test on Health Client Infrastructure

WhiteRookCyber conducted internal penetration testing against the client's infrastructure across multiple sites. The testing focused on finding and exploiting vulnerabilities in the data centres and associated sites, including physical penetration testing. The client required assurances that the internal systems and sites in scope were robust and secure against malicious cyber attackers due to the sensitive nature of the networks and data, which included PII and health data.

As a result, the client required **WhiteRook**Cyber to conduct the internal penetration testing activities above to ensure the internal network is secure and resilient and ensure the system is compliant with the relevant standards applicable.

By completing the internal penetration test, the client received:

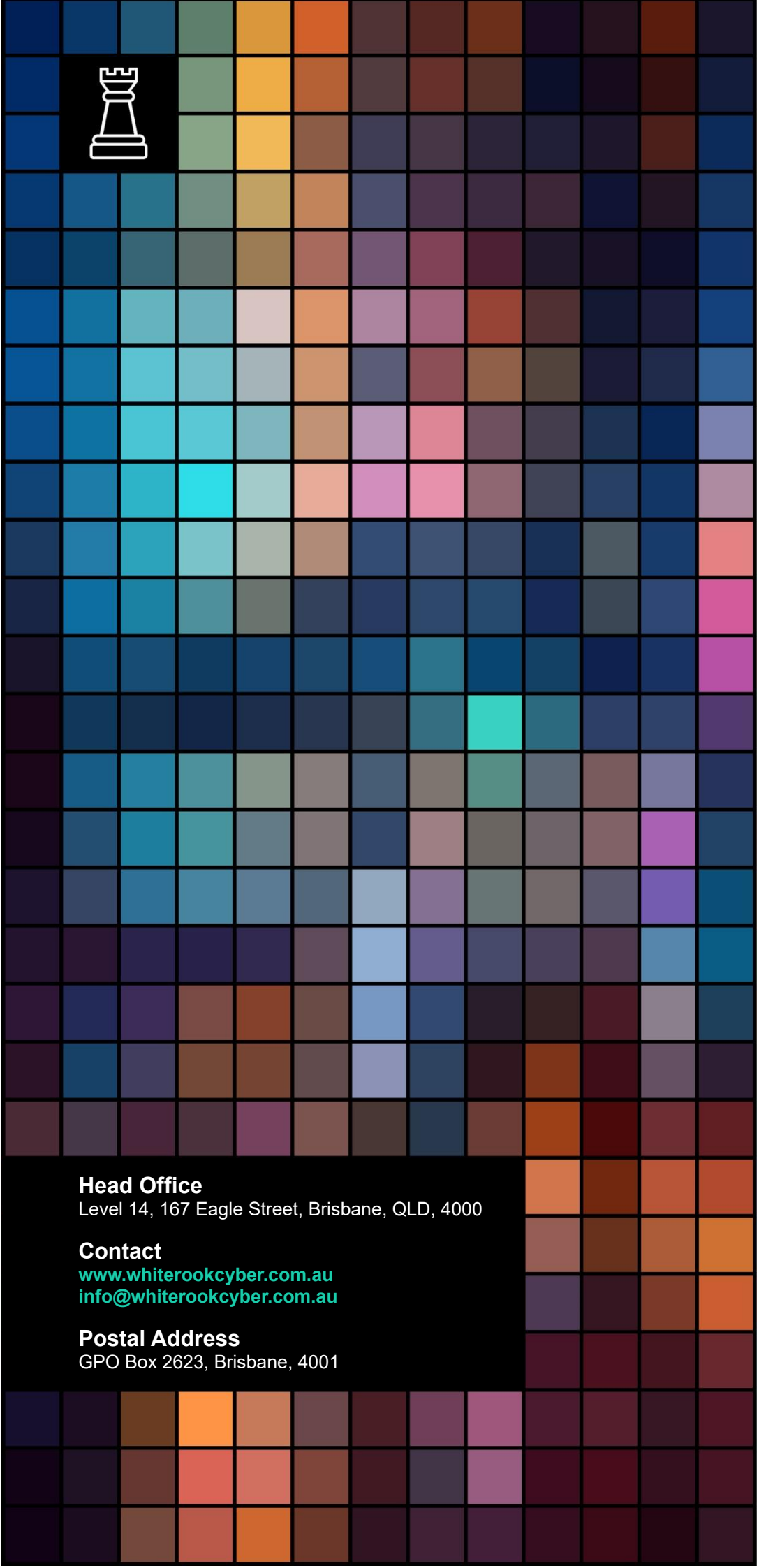
- An identified list of vulnerabilities and how they were exploited by the consultant
- Detailed attack walkthrough chronicling how the consultant successfully identified and exploited the vulnerabilities
- Detailed list of remediation recommendations to support the uplift of the cyber security of the systems
- Risk matrix linking technical risks to business risks, facilitating management buy-in

Due to the services of **WhiteRook**Cyber, the client was able to:

- Quickly rectify the technical findings of the penetration test before the system's scheduled go-live date
- Go-live with the confidence that the systems were adequately protected and hardened
- Remain compliant with internal policies

For more information, please contact us at:

info@whiterookcyber.com.au
or visit **www.whiterookcyber.com.au**



Head Office
Level 14, 167 Eagle Street, Brisbane, QLD, 4000

Contact
www.whiterookcyber.com.au
info@whiterookcyber.com.au

Postal Address
GPO Box 2623, Brisbane, 4001