



2024

Cybersecurity Risk Assessment Report

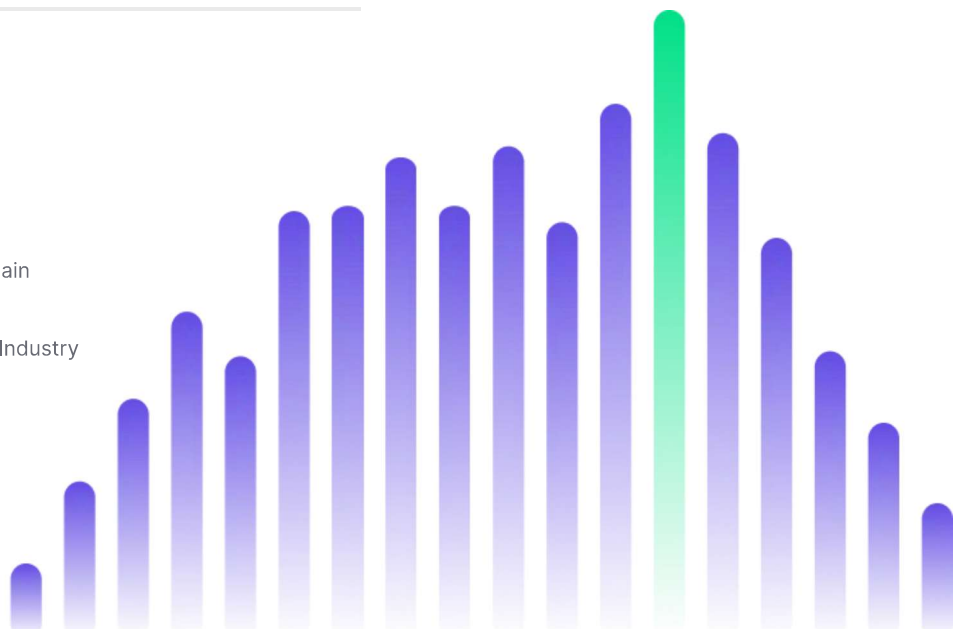
Generated For



  | Analyzed domain

 Information Technology and Services | Industry

 8 | Employees




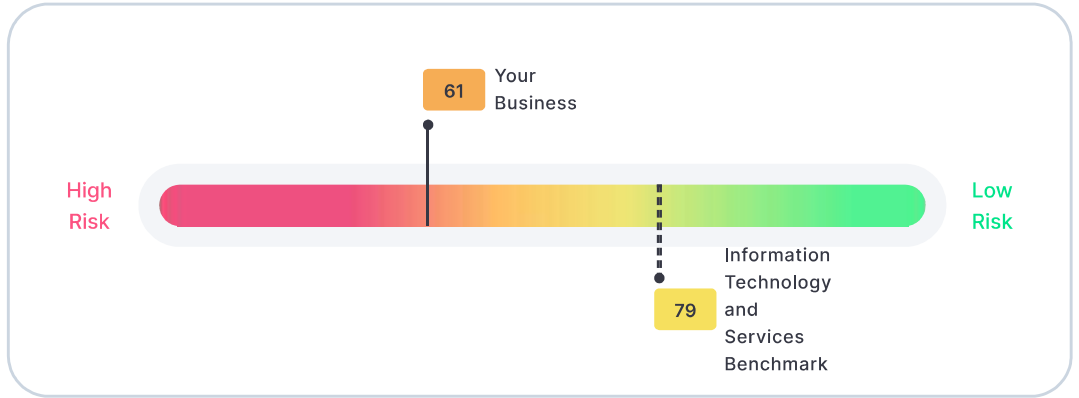
This assessment report was prepared by

White Rook Cyber

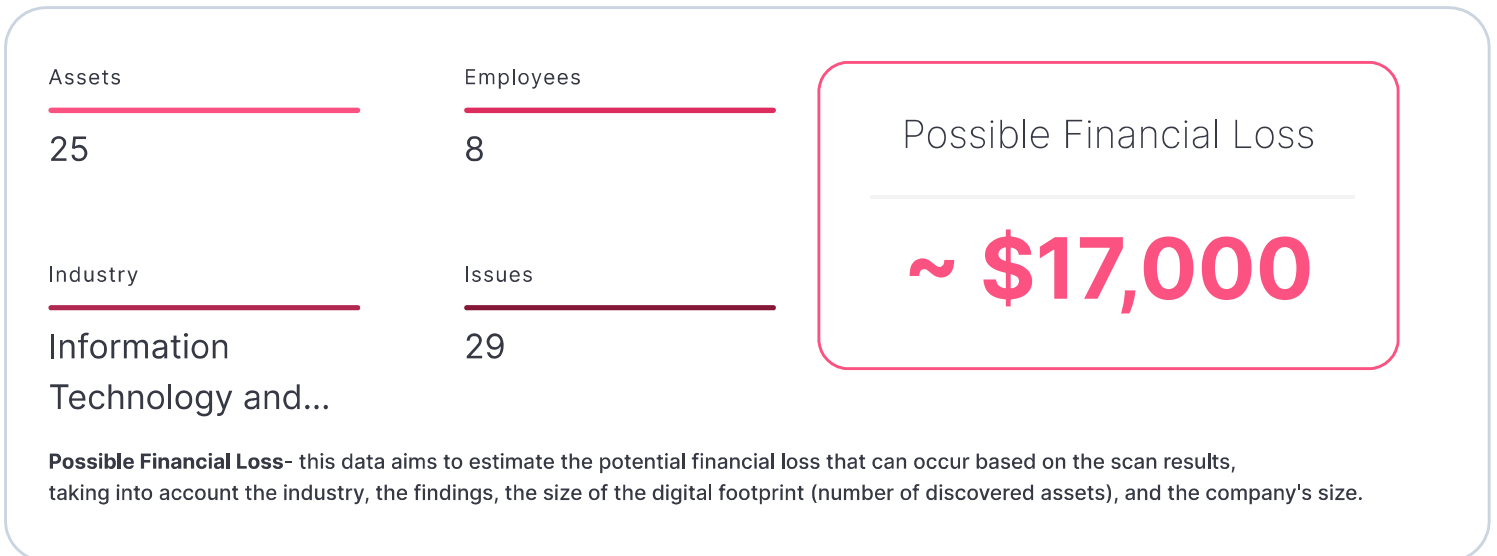
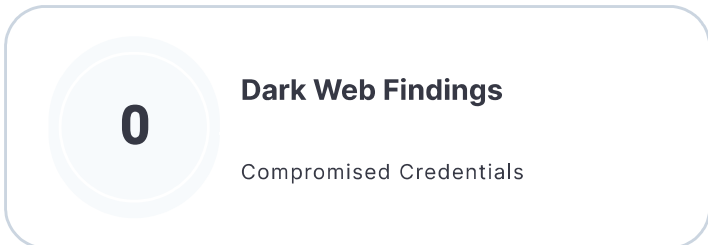
 1300 794 777

 contact@whiterookcyber.com.au






 whiterookcyber.com.au








Risk Status Legend: High | Medium | Low | Secured



Top Assets With Potential Risk (5 / 25)

Asset	Asset Type	Geolocation	Findings
[REDACTED]	Domain	 Australia	4
ftp-[REDACTED]	Domain	 Australia	4
portal-[REDACTED]	Domain	 Australia	3
www-[REDACTED]	Domain	 Australia	2
[REDACTED]	Domain	 Australia	2

External surface scan - Top Vulnerabilities (5 / 29)

Vulnerability	Risk	Findings
 Technologies with critical severity vulnerabilities	Critical	10
 TLS (SSL) supports deprecated protocols	High	2
 SSH vulnerable algorithms	Medium	10
 TLS (SSL) with cipher suites configuration	Medium	4
 TLS (SSL) hostname certificate invalid	Medium	2

Impact: Vulnerable Assets

Publicly exposed vulnerable assets can be exploited by hackers to launch attacks against your company.

Dark Web Scan



There are over 10 Billion stolen credentials (username & pwd) on the dark web.

The Dark Web is a part of the internet that is intentionally hidden and inaccessible through standard search engines, often associated with illicit activities, anonymous communication, and the exchange of illegal goods and services.

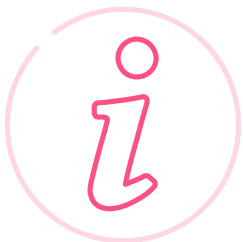
Potential Impact: Compromised Credentials

Business email compromise can result in email spoofing and the hacking of your company's accounts.

External Risk Posture

Your complete risk posture offers an extensive overview of your organization's cyber exposure, covering assets, data vulnerabilities, and technologies that could be exploited, as identified by our External Surface Scan.

Categories - Secured / At Risk	Findings / # of Assets Impacted
At Risk Technologies	10 / 10 Assets
At Risk Application Security	10 / 10 Assets
At Risk TLS	9 / 4 Assets
Secured Exposed Services	0 / 0 Assets
Secured Cloud	0 / 0 Assets
Secured DNS	0 / 0 Assets
Secured Domain Attacks	0 / 0 Assets
Secured Mail Server	0 / 0 Assets
Secured Web Server	0 / 0 Assets
Secured Asset Reputation	0 / 0 Assets
Secured Endpoint	0 / 0 Assets
Secured Social Posture	0 / 0 Assets
Secured Responsiveness	0 / 0 Assets
Secured Security Team	0 / 0 Assets
Secured Employee Attack Surface	0 / 0 Assets



Financial loss due to cyber incidents in Information Technology and Services

In the Information Technology (IT) and Services sector, the storage of valuable intellectual property has led to an average cost of a data breach reaching a staggering \$7.91 million.

The compounding factor here is the stringent regulatory obligations that IT companies must abide, including GDPR or FISMA, where regulations could lead to fines up to €20 million or 4% of the company's annual turnover. The impactful example of Uber's \$148 million settlement underlines the dire financial consequences of non-compliance.

IP Address	An IP address is a distinct numerical label, unique to a device, server or website, serving as a specific online location. It's vital for all online activities, and should be protected as a valuable 'digital asset'.
Cyber Posture Rating	Based on the results of a non-intrusive external surface attack scan and dark web monitoring, a cyber posture rating is calculated from 0-100 which represents the level of risk allocated to a company's external digital footprint.
Security Findings	Security findings refer to identified vulnerabilities or weaknesses discovered during the risk assessment, highlighting security issues that organizations need to address. The findings in this report cover; Network & IT, Application, Human, and Compromised Credentials.
Dark Web	The Dark Web is a hidden part of the internet, commonly used by cybercriminals for illegal activities. A dark web scan identifies leaked credentials indicating the potential for unauthorized access of personal data, eventually leading to the risk of security breaches.
External Surface	The external surface refers to an organization's digital footprint that is visible and accessible to the public. This includes company websites, email systems, servers, protocols and other exposed services.
Assets	For the purposes of this report, a digital asset refers to company owned domains, subdomains, servers, and IP addresses. These assets often carry a lot of value, as they form a part of an organization's digital identity and operations which should be protected against cyberthreats.
Domain	A domain is a unique identifier that represents the web address or URL which is crucial for people to find and interact with a website. Domains are essential digital assets because of the traffic they attract, requiring protection to prevent misuse or unauthorized changes.
Web Server	A web server is a system that stores, processes, and delivers web pages to users. These servers require regular maintenance and if not updated can open up publicly accessible vulnerabilities.
TLS/SSL	TLS and SSL are protocols designed to provide secure communication by encrypting data between a browser and a website. It's crucial to ensure up-to-date versions of TLS or SSL to avoid vulnerabilities in the system.
Web Certificate	A web certificate authenticates a website's identity and enables an encrypted connection. When it is outdated, site traffic may be compromised.



Phishing

Hackers use phishing to trick people into giving away sensitive information, such as passwords, by posing as a trustworthy entity or person. Holistic protection against phishing combines email security, browsing, endpoint protection, perimeter posture, and awareness culture in one native solution.



Ransomware

This malware encrypts a victim's files or data and demands payment in exchange for the decryption key, causing damage to businesses. A managed anti-virus solution should detect and isolate infected systems in parallel with monitoring of vulnerable servers, email attachments, and abnormal activity.



Data Loss

Unauthorized loss of sensitive information, can have severe consequences, including financial losses, reputational damage, and legal implications. Data loss protection includes data in the cloud and secures several vectors of attack while exposing the risks of negligent and intentional data exfiltration.



User Risk

Users are the first line of defense against a cyber attack but are often also the weakest link, so in addition to ongoing security training, employees should be protected through monitoring for leaked credentials, spear-phishing prevention, as well as cloud and device posture analysis.

Common Threats FAQ

How can I identify a phishing email?

Looking for suspicious senders or sloppy formatting are quick indicators you can catch with your eye. But hackers are getting more sophisticated, and it is recommended by regulation and industry best practices to utilize email security with other detection tools.

How can I protect my computer or network from ransomware attacks?

To defend against ransomware, keep software updated, use reputable antivirus software, be cautious with email attachments/links, regularly back up important files offline/cloud, enable automatic backups/versioning, and educate about phishing and safe browsing. Bottom line employees need to be actively involved in security, and systems need to be in place to quickly detect and prevent ransomware attacks.

How to prevent data loss?

In a world where we are focused on collaboration, the same tools that allow us to be productive open up vectors of attack for external exposure of confidential data. It's about being diligent regarding cloud posture and sharing best practices to avoid accidental data leakage.

How to prevent user risk in cybersecurity?

To prevent user risk in cybersecurity, implement comprehensive user awareness and training programs to educate employees about common cyber threats, phishing attacks, and safe online practices as well as having the right tools in place to automate user access policies and mitigate common vectors of risk.



This assessment report was prepared by

White Rook Cyber

 1300 794 777

 contact@whiterookcyber.com.au

 whiterookcyber.com.au

Generated For



 .com.au | Analyzed domain

 Information Technology and Services | Industry

 8 | Employees

Secure Your Business Today

Powerful Cybersecurity in Action