FOCUSNET
TECHNOLOGY

Certified System
Quality
ISO 9001

E8 PLUS CYBER HEALTH CHECK

MANAGED I.T.

BUSINESS CLOUD

PREMIUM TECHNOLOGY

INDUSTRY SOLUTIONS

CONFIDENTIAL

[redacted]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Introduction

FocusNet Technology were contracted by [redacted] to review the Cyber posture of their current IT environment including a comparison of internal IT practices alongside the Australian Cyber Security Centres (ACSC) Essential Eight model (M1).

This audit also includes a review of their current Microsoft 365 tenancy implementation and security profile compared against various industry accepted best practice models including the Center for Internet Security's (CIS) Microsoft 365 Foundtions Benchmark.

The ACSC's Essential Eight offers a prioritised roster of practical measures that organisations can adopt to enhance the security of their computer systems and reduce the chance that the system will fall victim to a Cyber-attack.

At a high-level the audit evaluates the utilisation of services and the existing mitigating technologies within the environment. It also identifies areas that need attention to improve security across the different IT platforms.

The E8 audit involved a review of on-site services, policy, and practices as they pertain to the IT operations. The Essential Eight audit was conducted via a targeted questionnaire designed to solicit one of three possible responses from the respondent – "Yes", "No", or "Partial". The responses were then verified (if required) and submitted into a model that establishes which elements met the minimum standards required to achieve Maturity Level 1 (M1) as set out by the ACSC.

Additional input where required was solicited from your IT provider [redacted] to arrive at a position and recommendations.

The emphasis of this review is to consider the preservation of confidentiality, integrity, and availability (CIA) of information and services, and what realistic mitigations should be in place to reduce the cyber and data loss risk to the business.

What this audit is not

For the internal audit, this was an authenticated internal vulnerability assessment. We have been provided with legitimate domain credentials with no special permissions/privilege's other that of a regular user. All information presented in this report was gathered in the context of this user. The assessment was entirely passive, none of the attack vectors or identified vulnerabilities were exploited, so any statements or conclusions drawn from the findings have been made on a good faith basis.

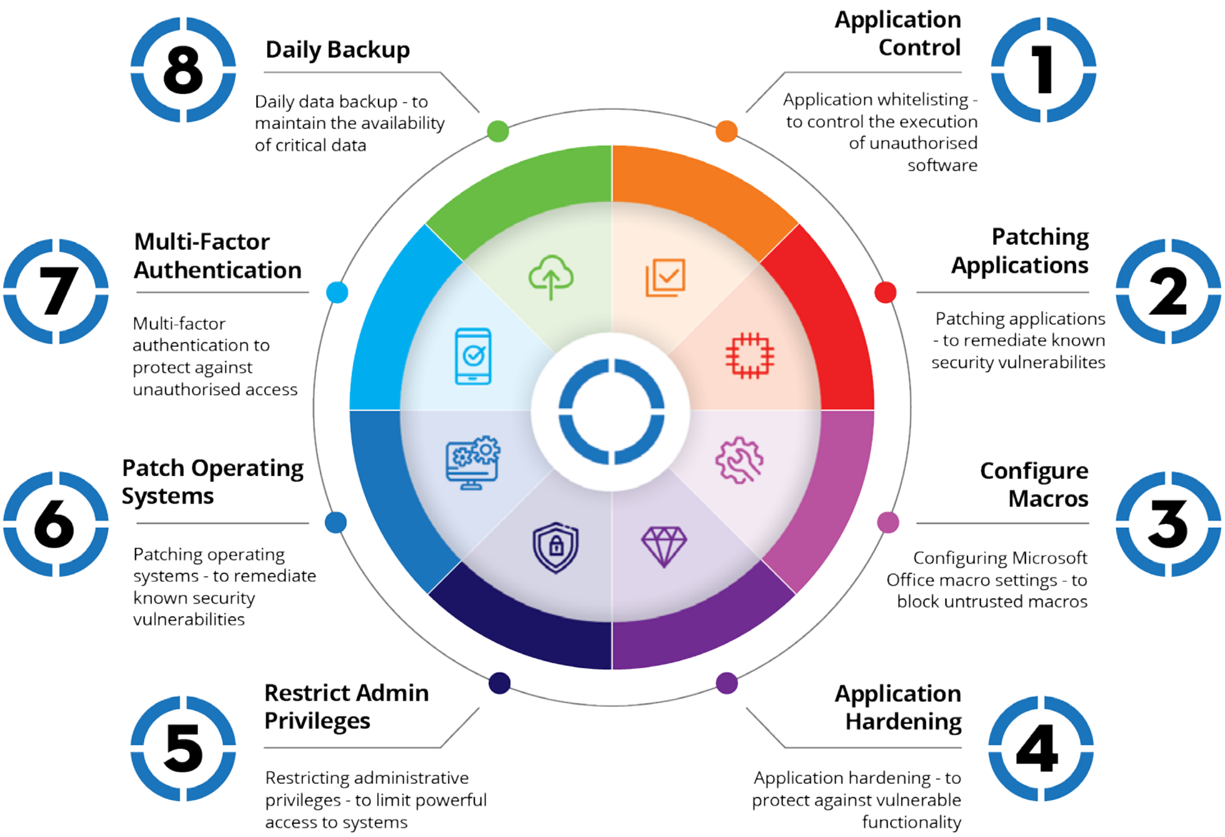
No changes to any configurations or other information (meta or otherwise) held within the domain was made.

What is the Essential Eight?

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the **Essential Eight**.

The Essential Eight has been designed to protect organisations' internet-connected information technology networks.

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement these eight essential mitigation strategies as a baseline. This baseline makes it much harder for adversaries to compromise systems.



1 **Application Control**

Application whitelisting - to control the execution of unauthorised software

2 **Patching Applications**

Patching applications - to remediate known security vulnerabilites

3 **Configure Macros**

Configuring Microsoft Office macro settings - to block untrusted macros

4 **Application Hardening**

Application hardening - to protect against vulnerable functionality

5 **Restrict Admin Privileges**

Restricting administrative privileges - to limit powerful access to systems

6 **Patch Operating Systems**

Patching operating systems - to remediate known security vulnerabilities

7 **Multi-Factor Authentication**

Multi-factor authentication to protect against unauthorised access

8 **Daily Backup**

Daily data backup - to maintain the availability of critical data

Maturity Levels

To assist organisations with their implementation of the Essential Eight, four maturity levels have been defined (Maturity Level Zero through to Maturity Level Three). With the exception of Maturity Level Zero, the maturity levels are based on mitigating increasing levels of tradecraft and targeting by cyber criminals.

Based on our knowledge and experience we believe your organisation should be looking to achieve Maturity Level One.

☠ Maturity Level Zero (M0)

This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

1 Maturity Level One (M1)

The focus of this maturity level is adversaries who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, systems. For example, adversaries opportunistically using a publicly available exploit for a security vulnerability in an internet-facing service which had not been patched, or authenticating to an internet-facing service using credentials that were stolen, reused, brute forced or guessed.

Generally, adversaries are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Adversaries will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications, for example via Microsoft Office macros. If the account compromised by a malicious actor has special privileges, they will seek to exploit it. Depending on their intent, adversaries may also destroy data (including backups).

2 3 Maturity Level Two and Three (M2, M3)

You can read the full description of Maturity Level Two and Three here.

What is the Dark Web?

The Dark Web functions as a cyber black market where stolen information is sold. Cybercriminals profit by selling previously breached data to other criminals, often without our knowledge. As their activities remain lucrative, breaches and phishing scams persist, leaving employee data and entire organisations vulnerable.

Purpose of the Dark Web Status Report

Cyber threats are becoming increasingly common and sophisticated in today's digital age. Personal information being sold on the dark web is one of the most significant risks that can expose individuals and organisations to vulnerabilities. To safeguard against this, knowing if employees have been involved in any dark web breaches is essential. By being aware of your organisation's dark web status, you can take proactive measures, such as securing compromised accounts and remaining vigilant for targeted phishing attempts to protect your organisation.

In today's digital age, cyber threats are on the rise, becoming more sophisticated. The sale of personal information on the dark web poses a significant risk, exposing individuals and organisations to exploitation. To help mitigate this risk, it's crucial to determine if employees have been part of any dark web breaches so you can take any actions deemed necessary.

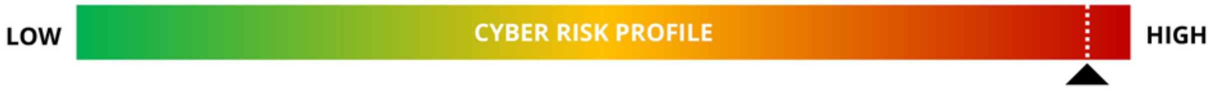
This report will make you aware of your organisation's dark web status allowing for proactive measures, including securing compromised accounts, and staying vigilant against targeted phishing attempts.

Executive Summary

We've assessed [redacted] cybersecurity posture based on industry best practices and compared them to an Australian standard, The Essential Eight Maturity Level 1. This evaluation has given us a prioritised list of risks and ways to address them. The goal is to help you tackle the most pressing issues first.

Based on the findings of this audit, we can state that there is a high degree of exposure, presenting an extreme risk to the business due mainly to misconfigurations within the domain, or deliberate policy decisions that have resulted in a weakened/compromised systems security posture. Additionally, there are process and policy items identified that increase the vulnerability of the environment.

The IT Section of the risk register seemed underdeveloped, with an over optimistic view of likelihood, mitigations in place and overall risk to the business. We feel that this section doesn't adequately reflect the true risk posed to the business and therefore requires a review and re-balancing of the risk ratings etc.



Overall, we would state that XXXX is **EXTREMELY VULNERABLE** to an attack from inside the network by a malicious actor/disgruntled employee with two (2) **CRITICAL PRIORITY** issue identified and nineteen (19) issues classified as **HIGH PRIORITY**.

2

CRITICAL PRIORITY

Any issue identified as being immediately exploitable by a suitably skilled technician leading to Domain take-over and requiring immediate action.

19

HIGH PRIORITY

Issues identified that expose attack vectors, or opportunities for malicious actors to improve their position within the network but may need additional effort or knowledge of the local environment to fully exploit.

10

MEDIUM PRIORITY

Issues identified that in themselves don't expose an immediate or obvious kill chain but could be used as part of a chained attack requiring the abuse of several issues/techniques to fully exploit the target/victim.

1

LOW PRIORITY

Suggestions for policy and administrative improvements to boost the overall cyber risk rating of the network and improve general management of the infrastructure.

[illegible]

If the staff who own these email addresses have a habit of using the same email address and password combination across multiple websites, it is strongly advised to change the password on all sites where this username/password pair was used and opt for unique passwords for each site. It is highly recommended that the owners of these accounts also change their domain password immediately.

General

As you address these concerns and move forward, it's important to consider your business goals, how much risk you're comfortable with, the skills and support available, and how proactive your IT partners are as the cybersecurity landscape shifts.

We feel that this report provides a balanced view of XXXX's' IT and Cyber security position considering the size and nature of the business. It's crucial to address the critical and high-priority issues promptly by either point mitigation, or an accelerated program of equipment replacement and a push to the cloud.

Considering the findings in this report, we would suggest sourcing recommendations and solutions from additional vendor(s) to ensure scalability, flexibility, support and most importantly that the security aspects are all fully appreciated and addressed.

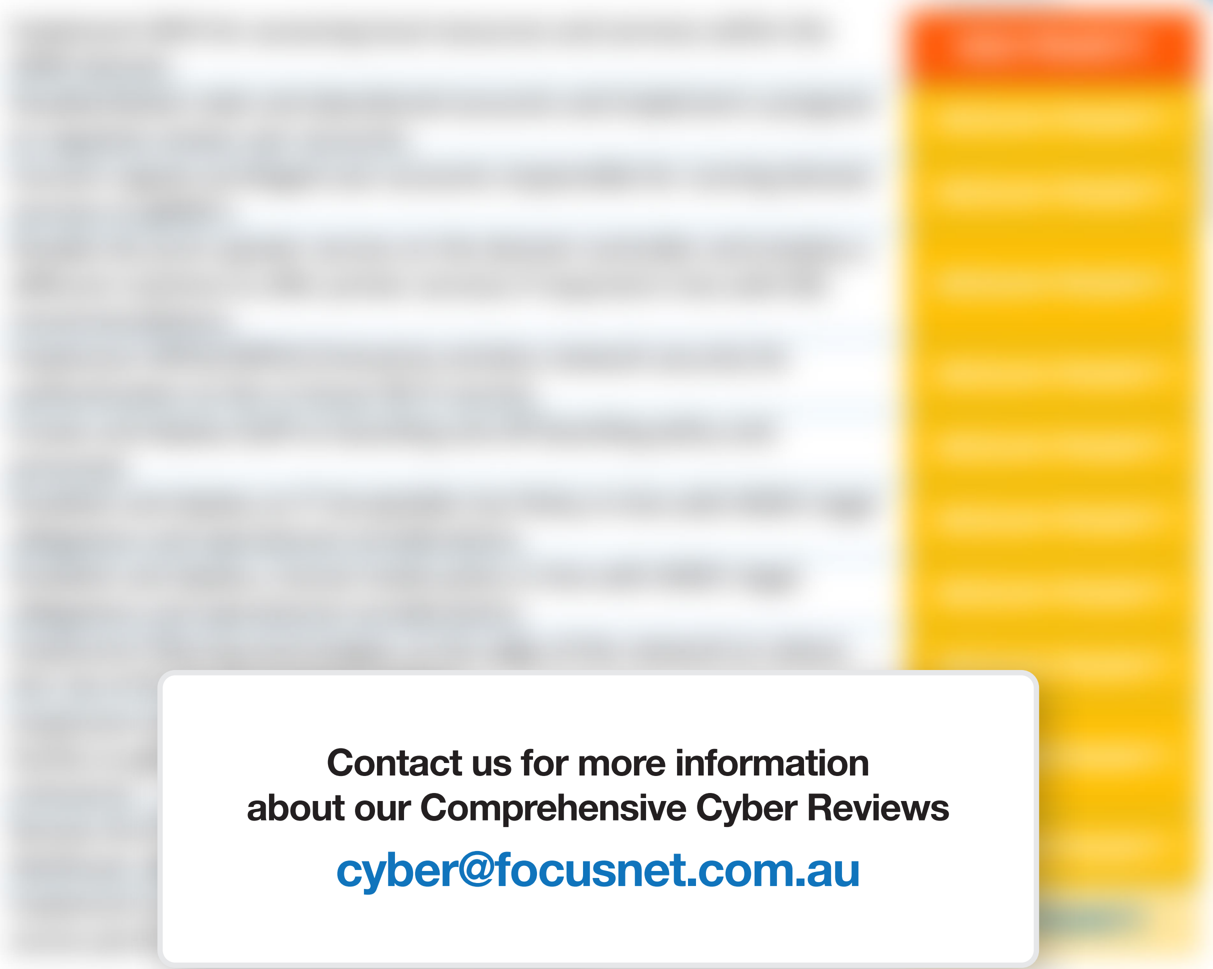
If you have any questions about this report, please don't hesitate to reach out to us at any time.

[redacted]

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

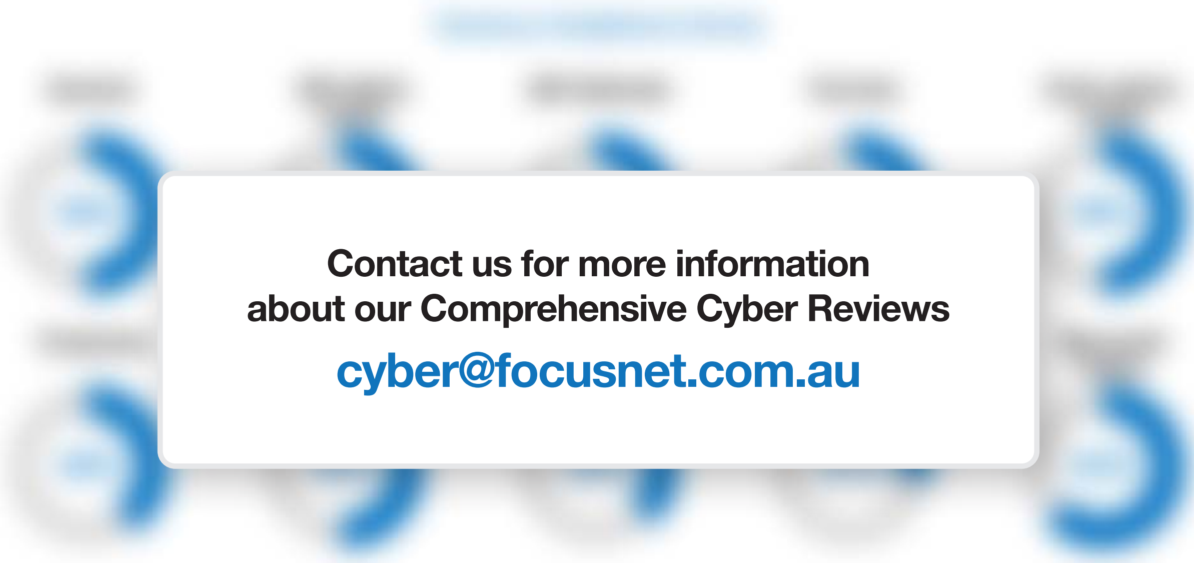


Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Overall Compliance Score

[illegible]

[illegible]

[illegible]

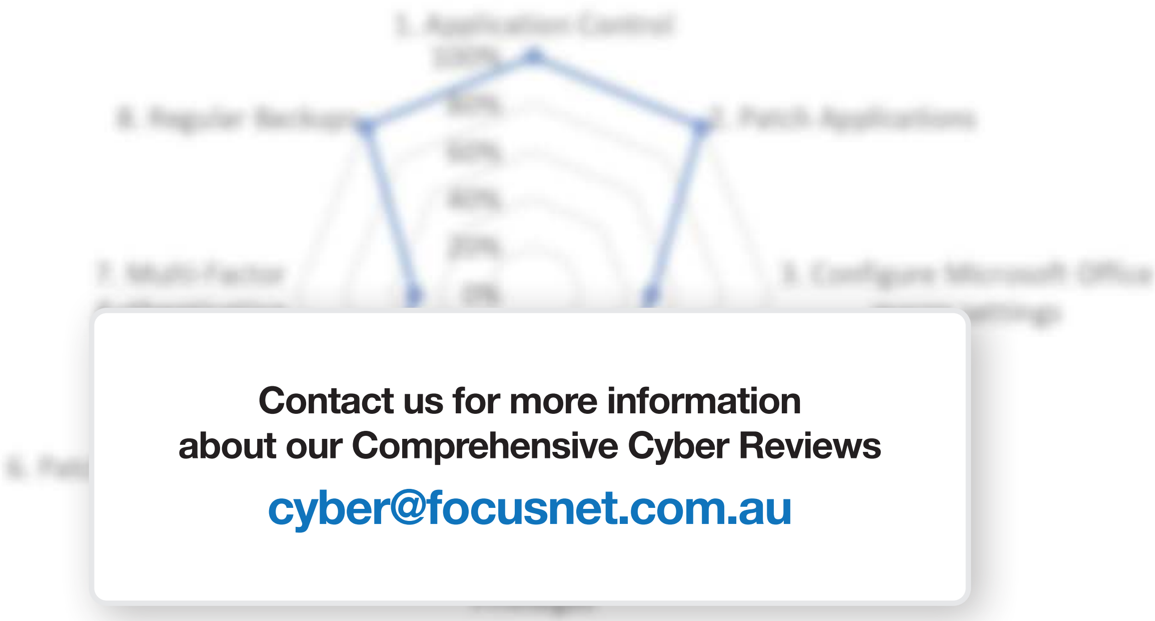
Contact us for more information about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]

[illegible]



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Mitigation Strategy	[illegible]
1. Application Control	[illegible]
2. Patch Applications	[illegible]
3. Configure Microsoft Office macro settings	[illegible]
4. User Application Hardening	[illegible]
5. Restrict Administrative Privileges	[illegible]
6. Patch Operating Systems	[illegible]
7. Multi-Factor Authentication	[illegible]
8. Regular Backups	[illegible]

Contact us for more information about our Comprehensive Cyber Reviews

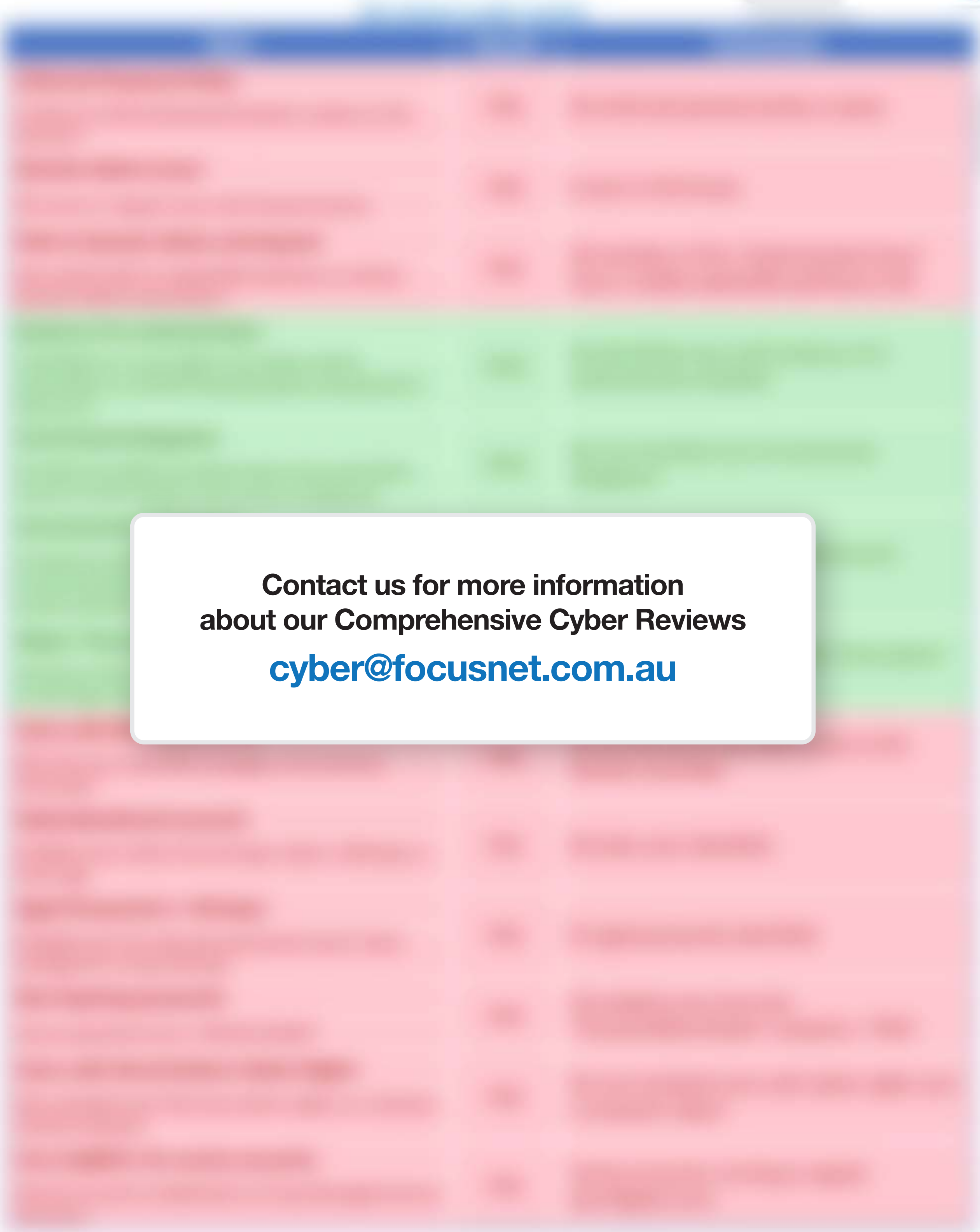
cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]

[illegible]

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

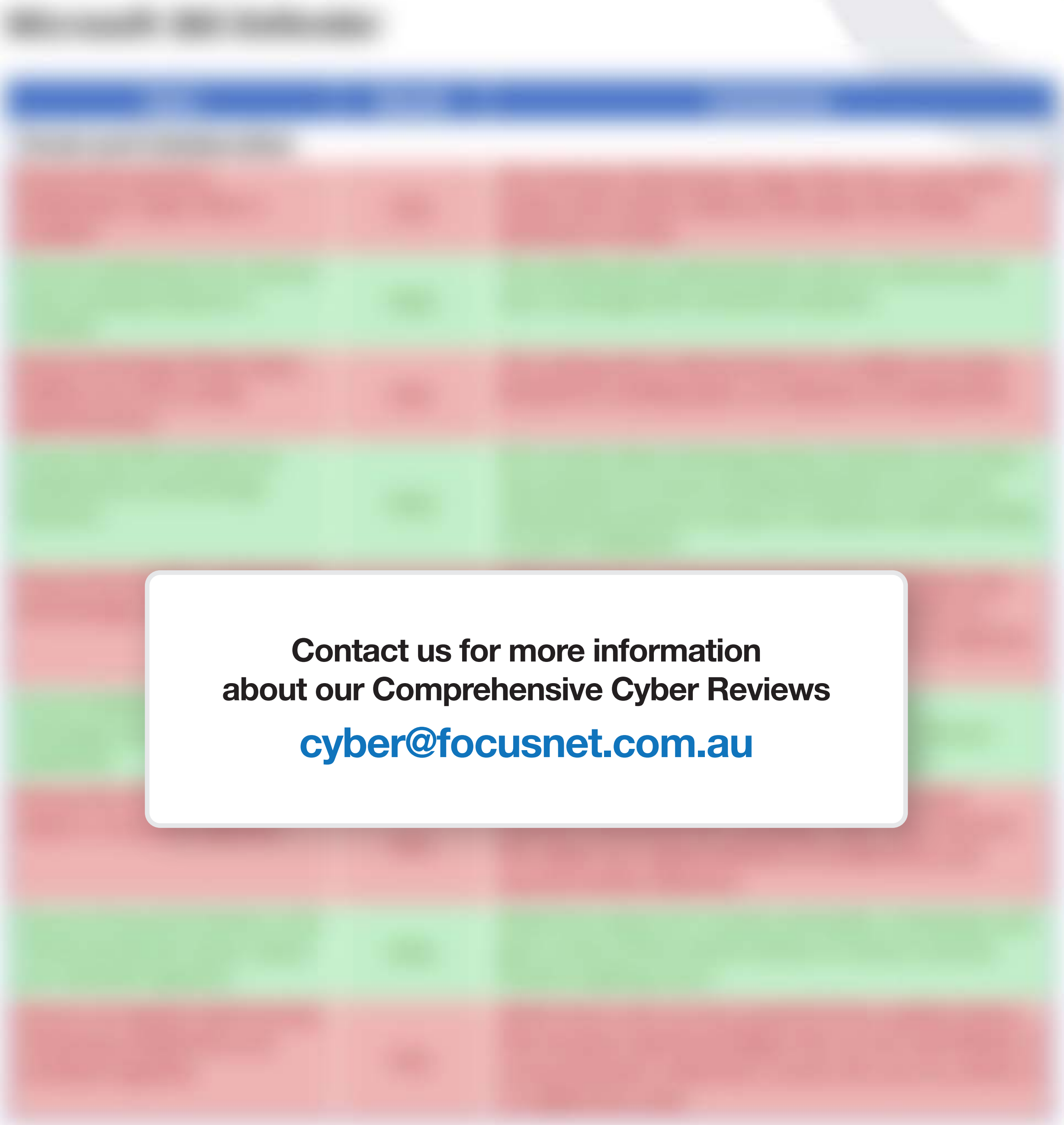
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

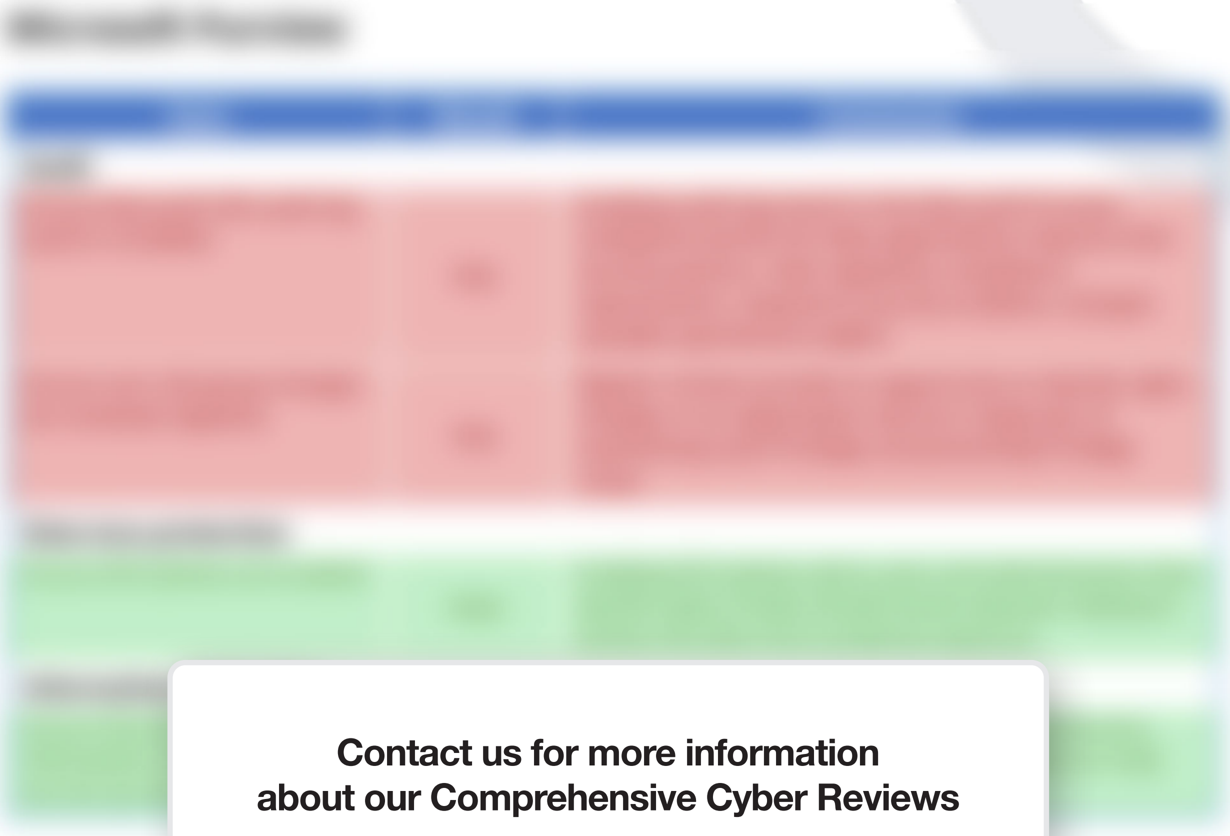
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



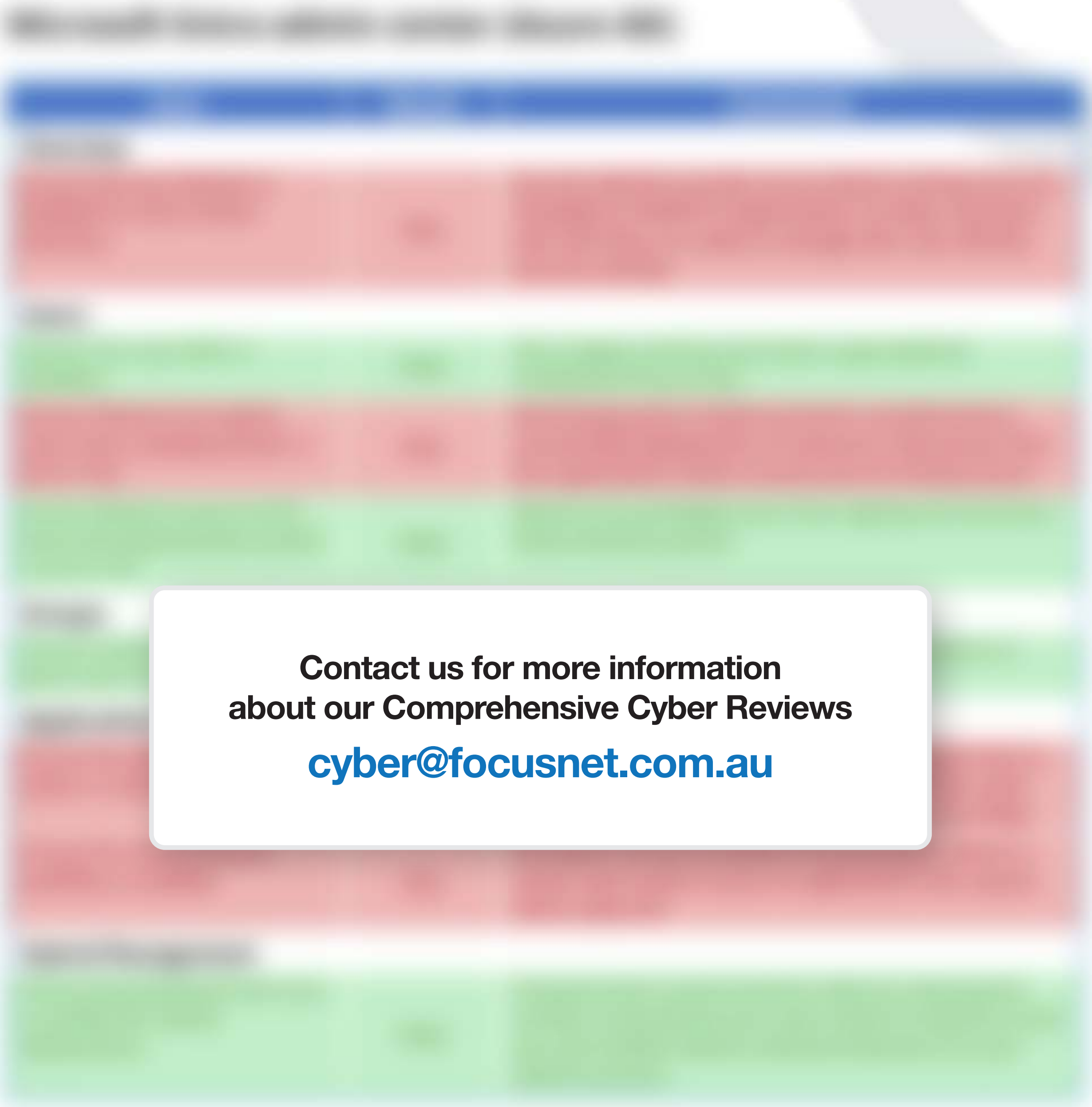
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



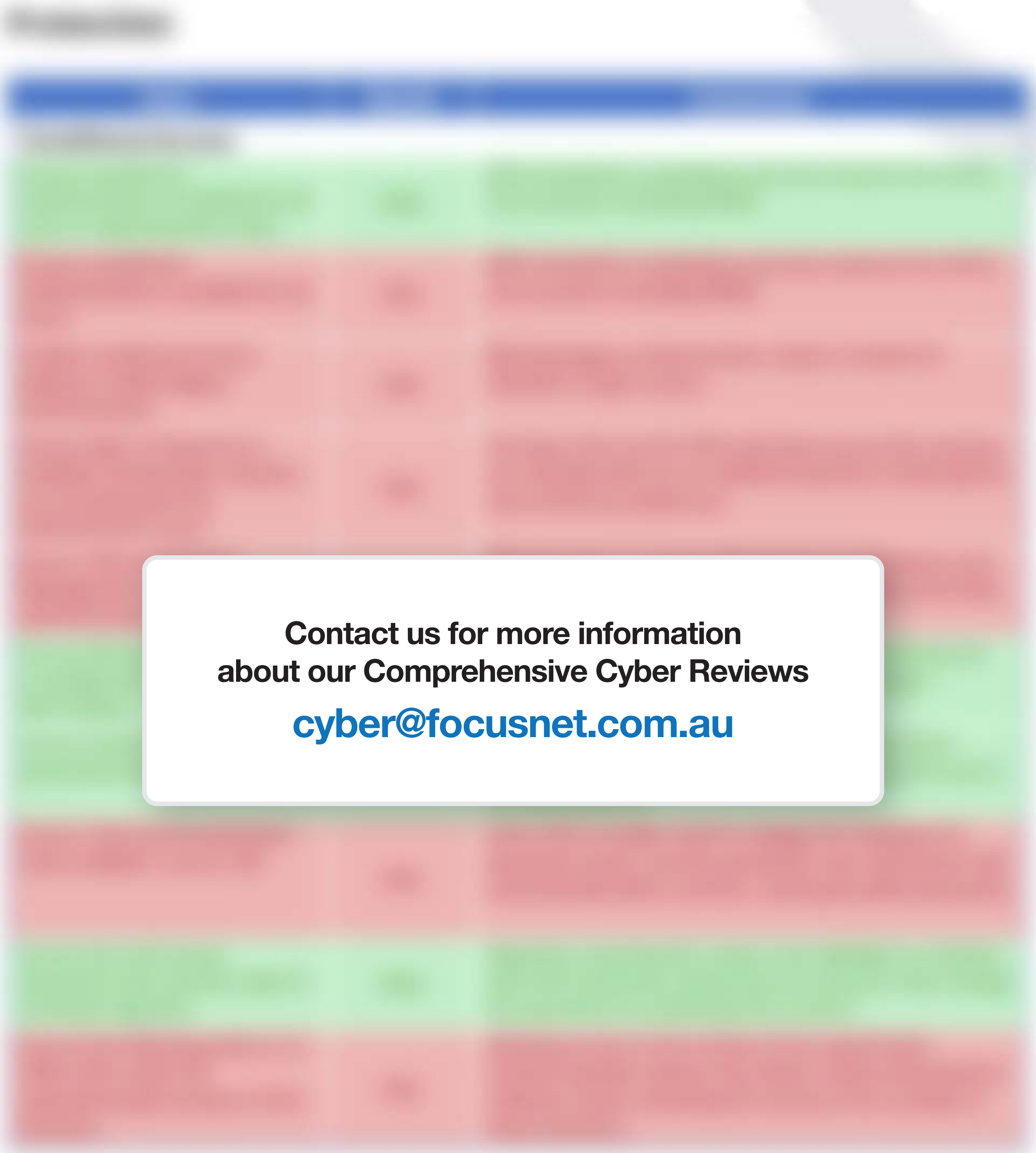
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



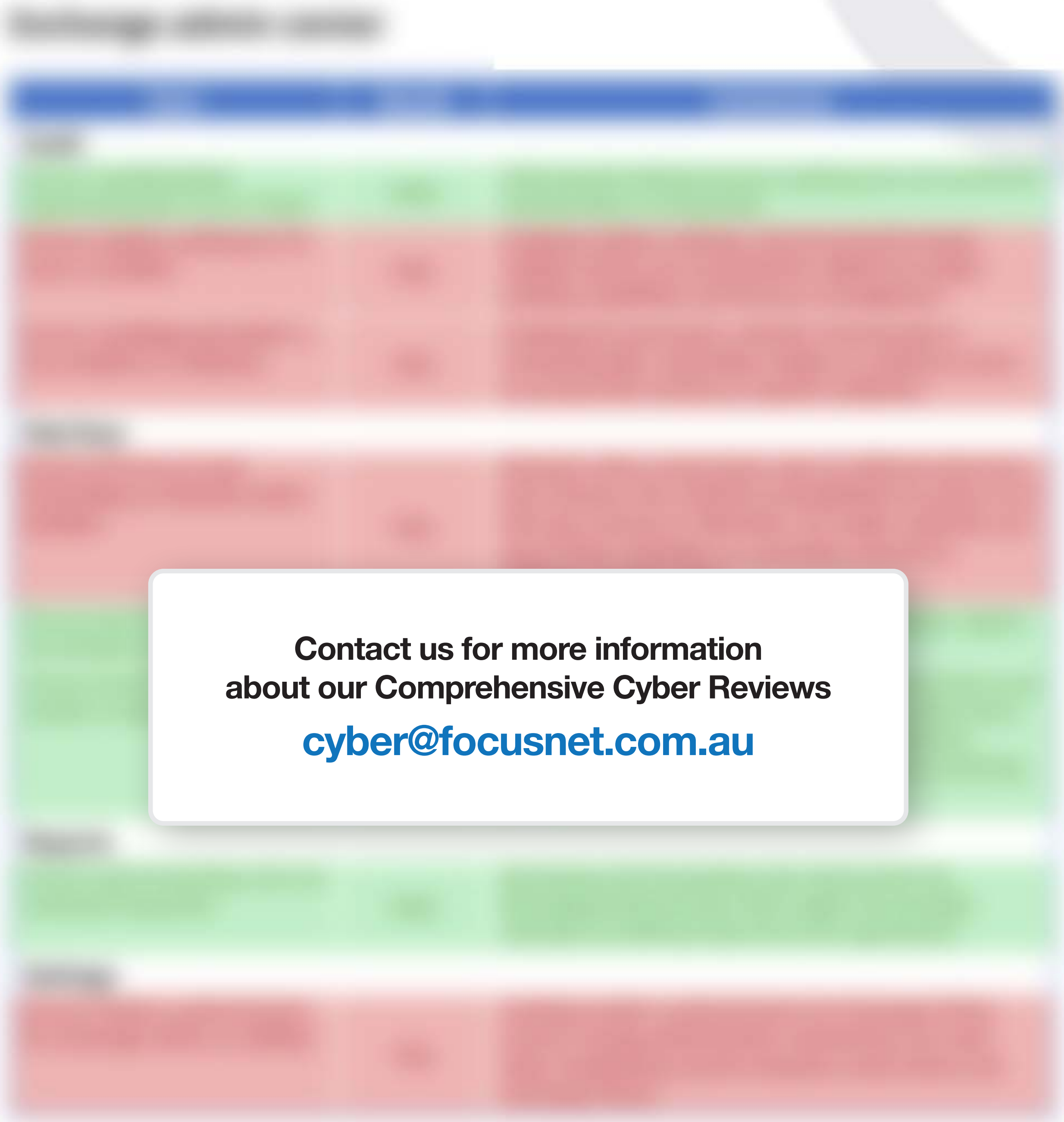
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



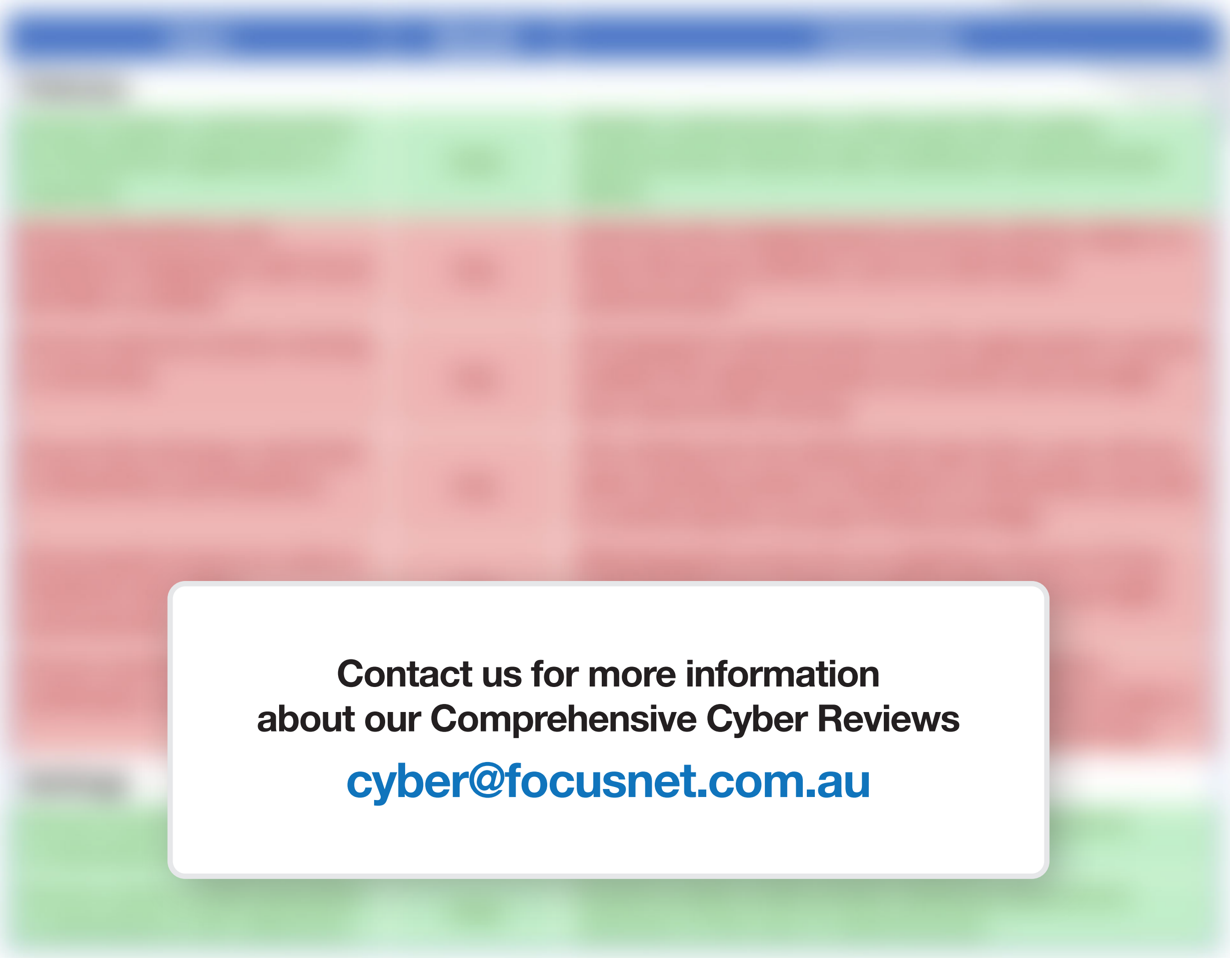
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



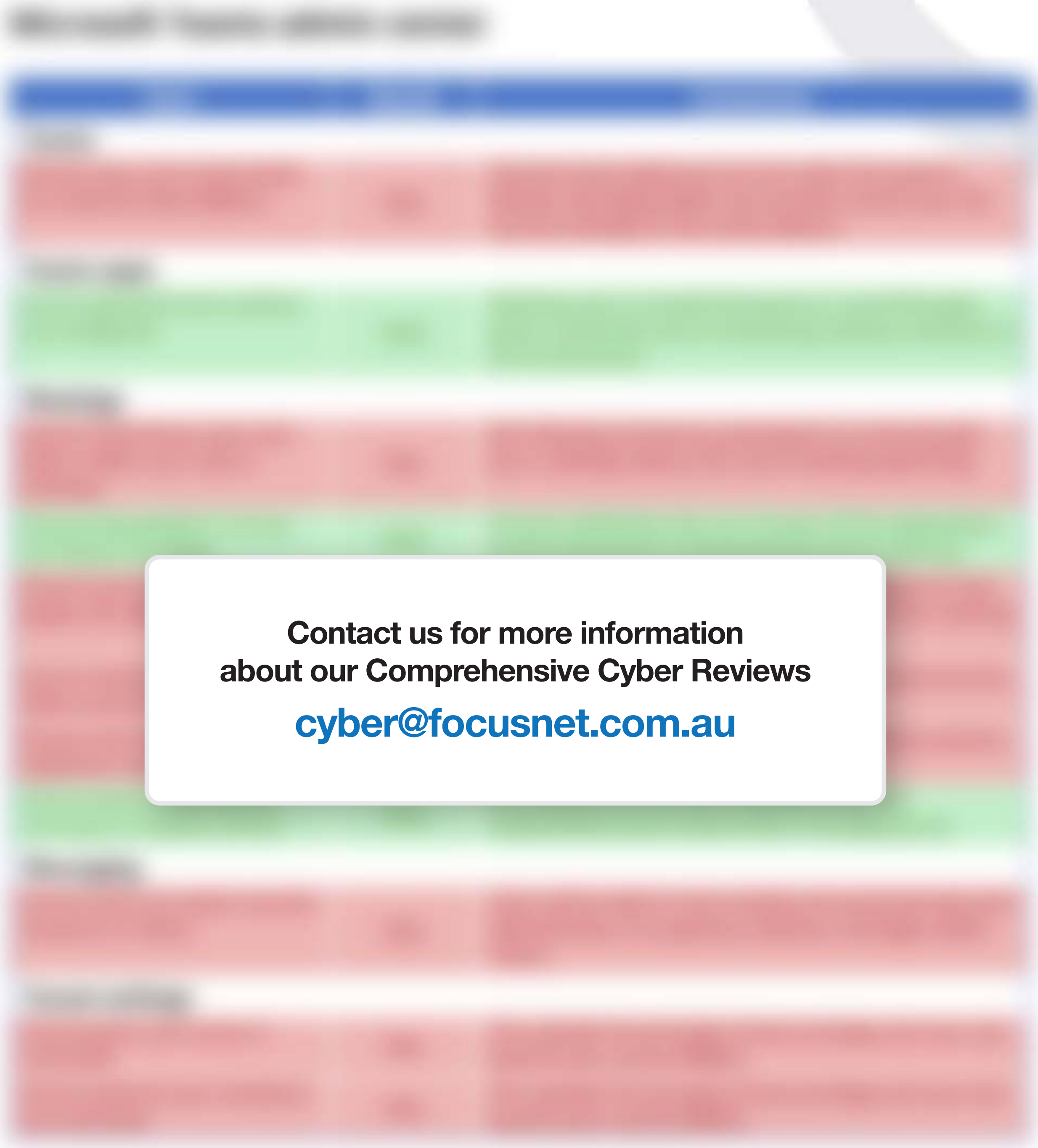
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



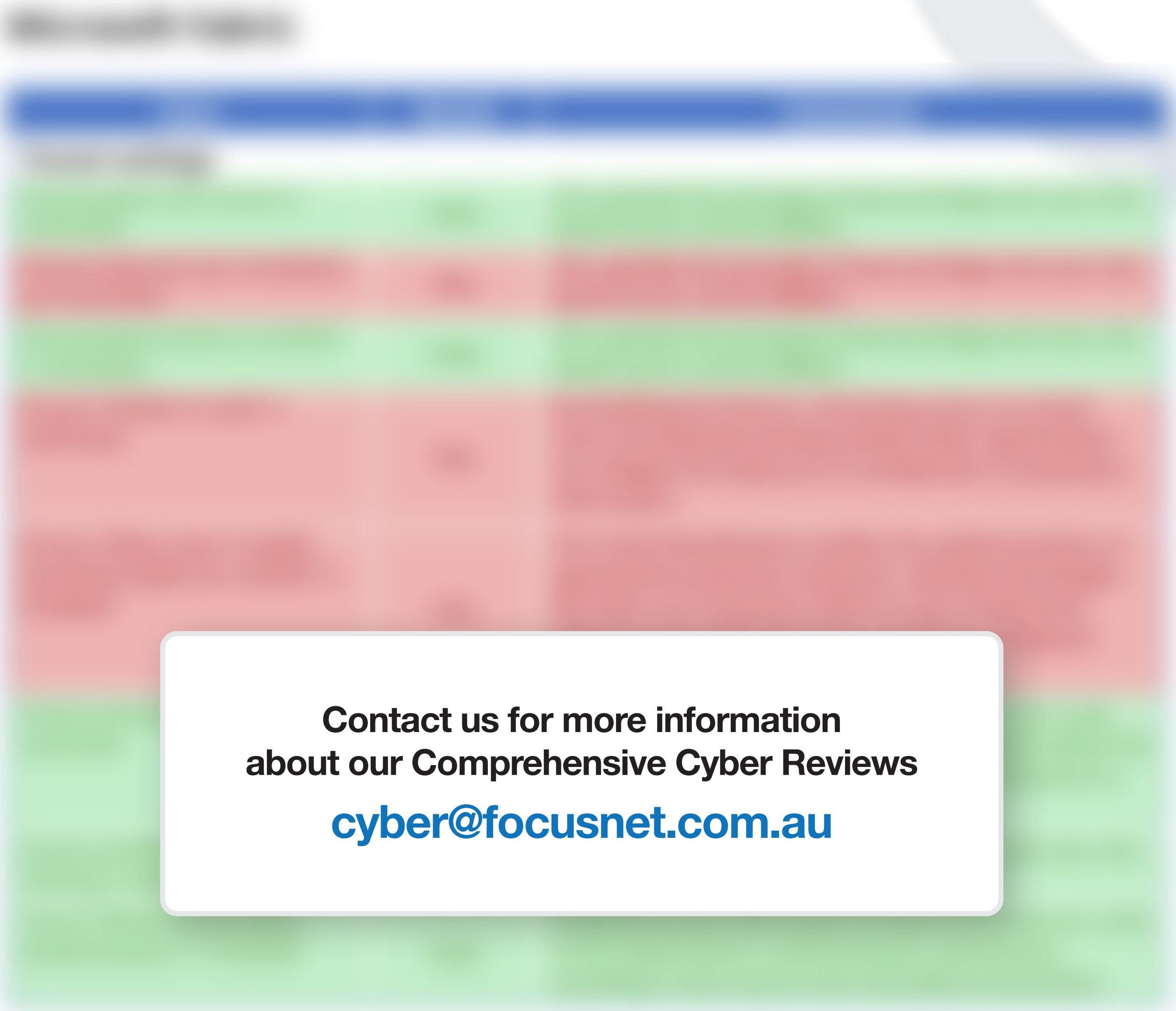
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

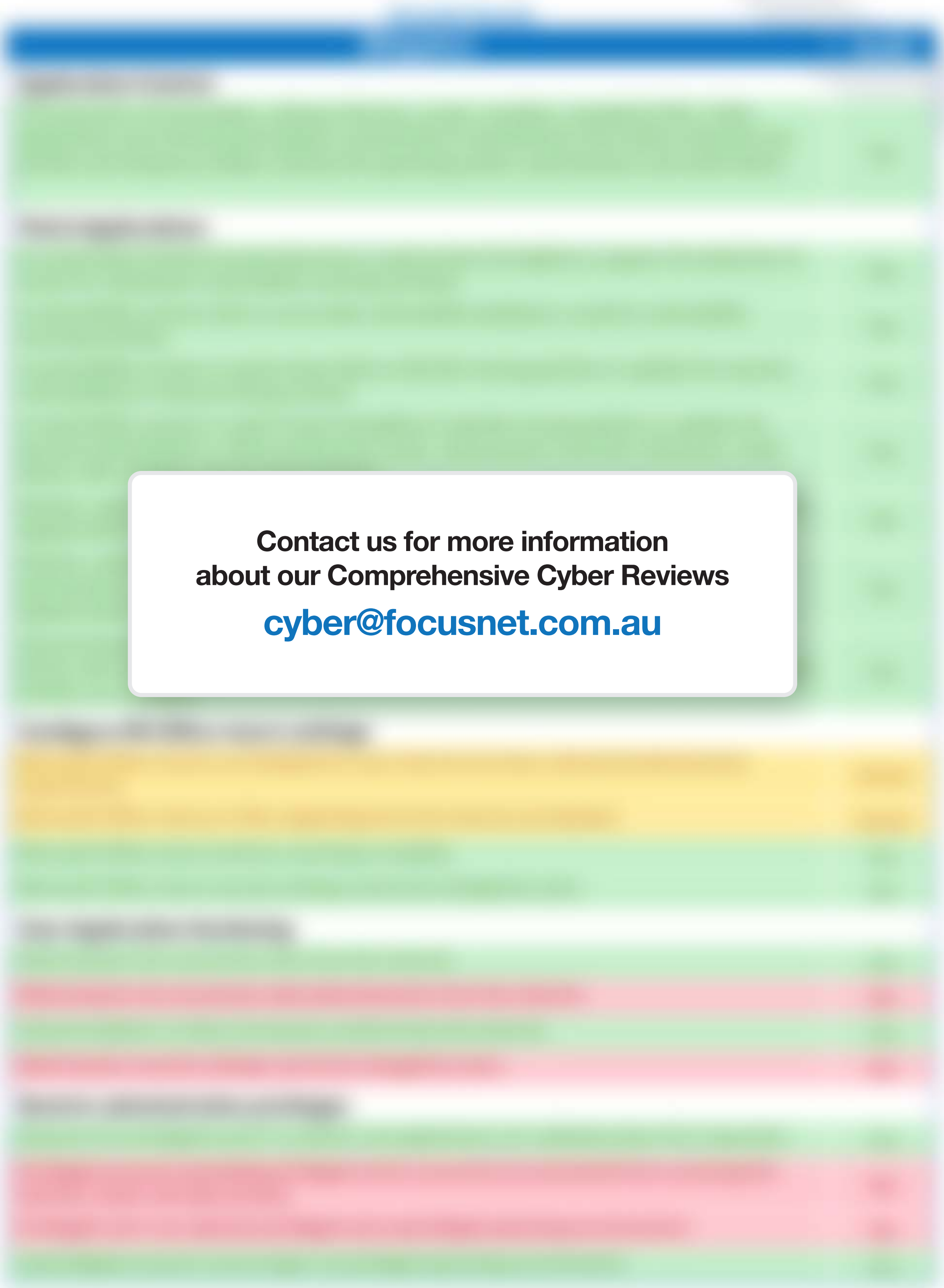


Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

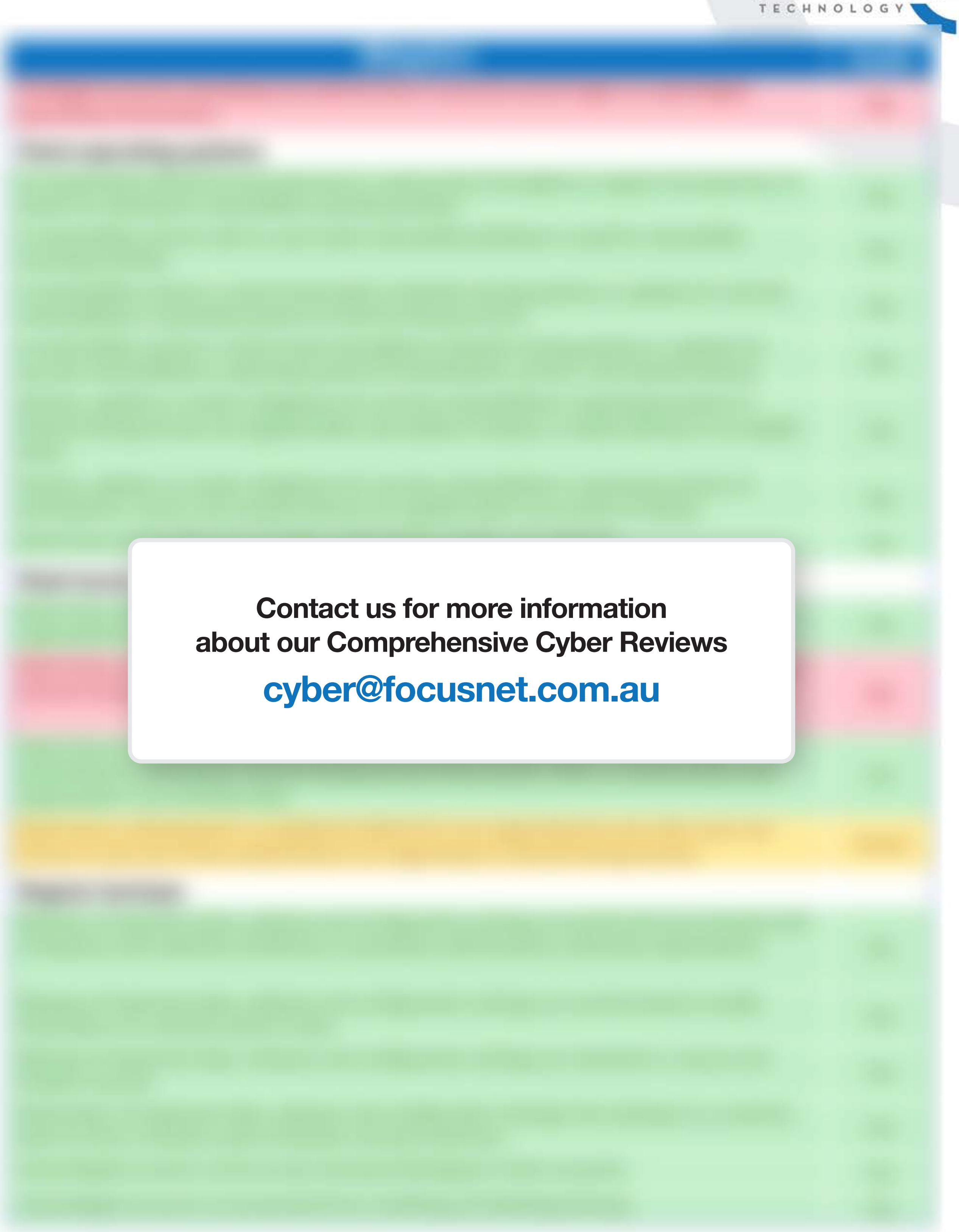
Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au



Contact us for more information
about our Comprehensive Cyber Reviews

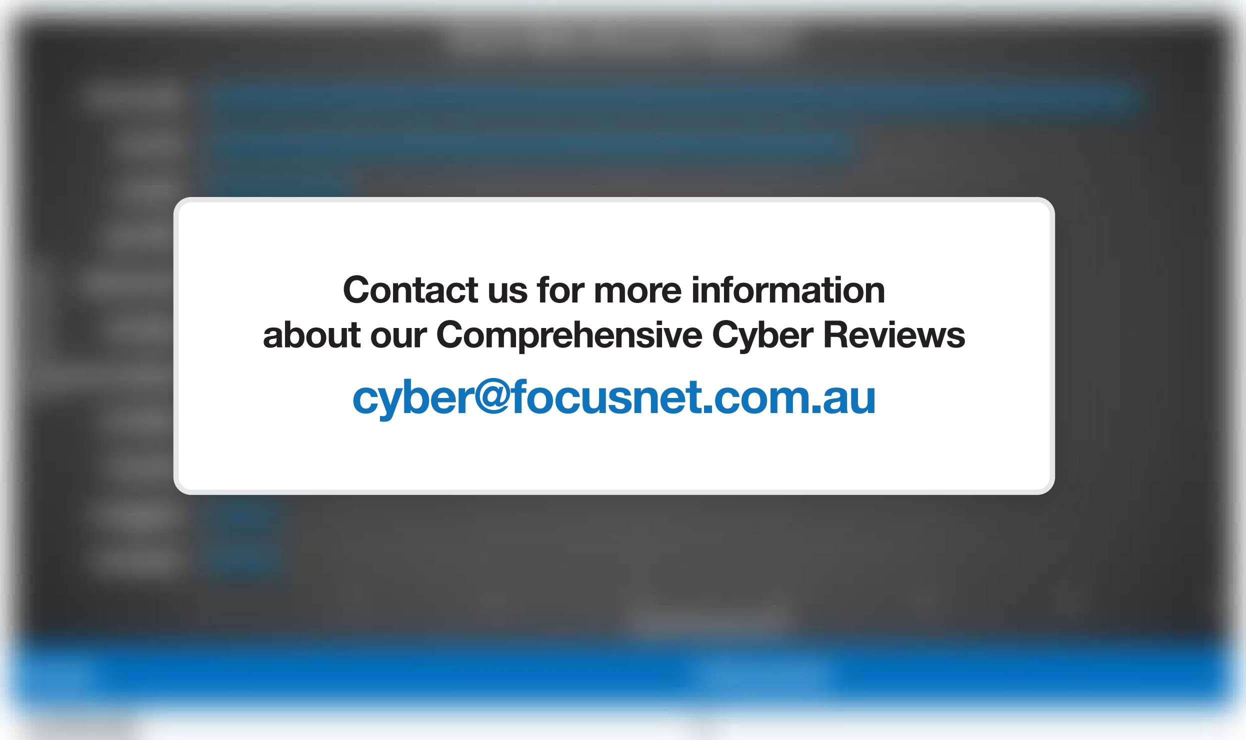
cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]



Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

What's the actual impact?

Breached Passwords

[illegible]

Organisation Exposure

11

[illegible]

33

[illegible]

[illegible]

[illegible]

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

[illegible]

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Contact us for more information
about our Comprehensive Cyber Reviews

cyber@focusnet.com.au

Disclaimer

This report (including any enclosures and attachments) has been prepared for the exclusive use and benefit of the addressee(s) and solely for the purpose for which it is provided based on information provided by the addressee(s). We do not accept any liability if this report is used for an alternative purpose from which it is intended, nor to any third party in respect of this report.

It has been compiled from incomplete information, which is the information that was available to us at the time of audit and reflects a point in time position of the items detailed. It does not guarantee the security of the IT assets, not does it guarantee that information cannot be pilfered from the services audited.

It is strongly advised to consult with your insurance professional to assess the appropriateness and advantages of obtaining a Cyber Policy.

Who is FocusNet?

Statistics tells us that, in Australia, 60% of Small/Medium businesses that experience a significant Cyber incident do not survive and ultimately go out of business within 12 months of the incident.

FocusNet are data security experts and provide a cohesive range of data and cyber services to the SME space that are informative, effective and affordable for everyone. Our team prides itself on the ability to strike the balance between robust security and powerful performance. With a consultative approach to your business, our friendly consultants are well equipped to listen, identify issues, and set out a comprehensive roadmap of recommendations to fulfil your unique requirements.

Below are some of the key business services available in FocusNet's Cyber suite:

E8 Cyber Health Checks

Comprehensive Cyber review of your business based on the ACSC Essential Eight maturity model and NIST standards. Includes detailed findings and recommended mitigations.

Cyber Advisory & Risk Mitigation

Expert Cyber advisory is a critical support service for every modern-day business - Cyber incident prevention, cyber risk management, cyber incident response.

Penetration Testing

Internal stress testing of your IT environment to expose any cyber risks and recommend strategies to be implemented to reinforce your cyber posture.

Staff Security Awareness Training

A training platform designed to reduce staff's risky online behaviour via Phishing simulations, training content, cyber policy management and effective reporting.

If you would like to know more about these services, feel free to contact:

[redacted]