CONSULT . DELIVER . SUPPORT

Enhancing Business
Through **Technology**

CALIBRE ONE
calibreone.com.au
1300 4 CALIBRE (1300 422 542)

Calibre One
Monitor, Detect & Advise Cybersecurity Service

CONSULT . DELIVER . SUPPORT

Some sobering 2020 Cyber Security Statistics

67 DAYS
the average time before a company becomes aware they have been compromised.

90%
of malware comes via email

39 SECONDS
how often a cyber-attack occurs

24%
of data breaches are caused by human error

The world we live and work in is more digital and online than ever. We protect our buildings, our physical equipment, and our staff yet few people and companies consider their online presence and data security with the same degree of attention. This is especially concerning as it is now a far more likely event and is also more probable to cause serious harm to your business, finances, and reputation. Many companies think that because they have an existing Managed Services Provider undertaking their IT support that they have this covered and while it's true to say that some have a better handle on it than others, the provision of Managed SECURITY services is NOT a general maintenance function.

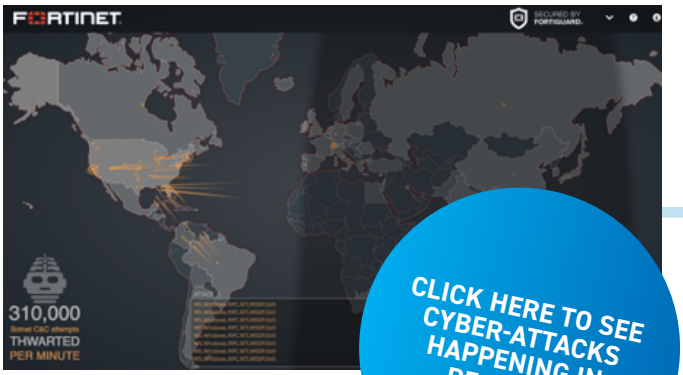
The above statistics are common in every country in the world – it is not limited to large companies and other countries - thousands of Australian businesses and individuals have been compromised costing millions of dollars. This is a matter that needs to be seriously considered by all Boards, Managers and Executives as a significant RISK to your business.

The Australian Federal Government has recognised the magnitude of this risk to the financial security of our country and in February 2018 introduced the Notifiable Data Breach legislation.

(See: https://www.oaic.gov.au/privacy/notifiable-data-breaches/).

To help you comply and mitigate this risk, Calibre One has partnered with a series of Security vendors to deliver a Monitor, Detect and Advice Cybersecurity service to improve your security posture, and make it less likely you'll be a victim of these attacks. This coupled with effective business Cyber insurance will help avoid the financial impact, potential fines, and certain loss of reputation to your business in the event of an incident.

A common misconception is that your Maintenance Service Provider does all this. This is simply not true or realistic - and while many providers perform a great deal of the more basic security functions they are simply not skilled, equipped or in the right mindset to address the real time nature of security defence. It is a very specialised activity and why Calibre One has an entirely separate Security Services Team. Managed Security Services is unfortunately a whole new requirement that has evolved out of the changing threat landscape.



CLICK HERE TO SEE CYBER-ATTACKS HAPPENING IN REAL-TIME

C1 CALIBRE ONE

Essential Components of our Program

The Calibre One Monitor, Detect & Advise Program Consists of the following Key Elements:

1 Onboarding and Shaping Up

2 Monitor, Detect & Advise

Additional option

Ongoing Reviews, Audits and Risk Assessments

1 - Onboarding and Shaping Up

Office 365 is a very secure platform with many tools to assist with securing and monitoring the environment and while the Out of the box default setup is good, to be truly secure it needs to be configured and optimised for your needs. This is not a function of normal ICT maintenance and most IT maintenance companies will lack the expertise to configure many of the variables, the tools necessary to monitor the conditions and the manpower to act on such alerts in a timely manner. This is the role of our security specialist team.

Our onboarding and Shaping Up process is designed to bring your Office365 tenancy to a higher level of security. To do this we use the built in Microsoft Office 365 Scorecard System to generate an overall security score for your tenancy. This will provide a score reflecting the points from a maximum possible - for example 74% (pretty good) or 11% (really bad). Our onboarding process is designed to bring your Tenancy to a MINIMUM 75% of the potential score for your specific environment - in the above example the 74% would be acceptable while the lower figure is not. This figure is an evolving score and changes over time as Microsoft introduce new features and threats change. (Future Monitoring of this score and adaptation of the environment is one of the variables our security services monitors).

The one-off charge for Onboarding and Shaping Up varies as a result of this core with the lower the score, the more work required to get the tenancy to this level.

Please NOTE: *We consider this to be an ESSENTIAL component - Calibre One will not provide security services to any tenancy not meeting minimum acceptable Microsoft score values.*

2 – Monitor, Detect & Advise

Our suite of tools provides essential monitoring and alerting - warning us to suspicious or malicious activities within your environment. Some are designed to detect ongoing and persistent external threats; others are designed to mitigate and react in the event your tenancy is compromised. This provides essential coverage and then speedy reaction should anything happen.

How do we Monitor and Detect?

An effective program of monitoring and detection is essential to provide basic levels of security. The Calibre One Cybersecurity program monitors and detects customers for the below security threats and attacks:

Alert Type	Description of potential attack
Suspicious Logins	This detection identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as Botnet C&C, and may indicate compromised account.
Impossible Travel	This detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials. This detection uses a machine learning algorithm that ignores obvious "false positives" contributing to the impossible travel condition, such as VPNs and locations regularly used by other users in the organisation.
Activity From Infrequent Country	This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or never visited by the user or by any user in the organisation. Detecting anomalous locations necessitates an initial learning period of 7 days, during which it does not alert on any new locations.
Brute Force Attacks	Generates an alert when an excessive volume of login attempts to an account is detected.
Suspicious Email Volume detected	Generates an alert when someone in your organisation has sent more mail than is allowed by the outbound spam policy. This is usually an indication the user is sending too many emails, or that the account may be compromised. This policy has a Medium severity setting. If you get an alert generated by this alert policy, it's a good idea to check whether the user account is compromised.
User restricted from sending email	Generates an alert when someone in your organization is restricted from sending outbound mail. This typically results when an account is compromised, and the user is listed on the Restricted Users page in the Security & Compliance Center. (To access this page, go to Threat management > Review > Restricted Users). This policy has a High severity setting. For more information about restricted users, see Removing a user, domain, or IP address from a block list after sending spam email.
Creation of Forwarding Rules	Generates an alert when someone in your organisation creates an inbox rule for their mailbox that forwards or redirects messages to another email account. This policy only tracks inbox rules that are created using Outlook on the web (formerly known as Outlook Web App) or Exchange Online PowerShell.
Creation of Suspicious Email Rules	Generates an alert when someone in your organisation creates an inbox rule for their mailbox that performs an action deemed as suspicious.

CONSULT . DELIVER . SUPPORT

Calibre One provides complete visibility across your environment, delivering real-time continuous threat monitoring 24x7. Our monitoring platform houses over 20 purpose-built detection and monitoring apps that aims to protect our customers with enterprise grade Security Operation Centre capabilities.

How do we advise customers?

All issues detected will be raised in the Calibre One ticket recording system as an Incident Ticket. On becoming aware of the incident, Calibre One will:

- Triage the ticket to determine its nature, validity and severity.
- Issues determined to be of an Immediate threat in nature will result in the NOC engineer responsible taking action to:
  - Immediately restrict further access to the account.
  - Liaise with the effected user to determine if the threat was in fact real and the circumstances surrounding the incident.
  - Reenable the account or take further action to secure and freeze it as required.
  - Document all actions.
  - Report the incident via the predetermined reporting chain.
- Lodge a ticket with your Managed Services provider (MSP) to undertake any further action.

All actions required to triage and respond to an immediate threat is included in the cost. Follow up and/or subsequent investigation work is subject to additional costs to be determined at the time.

3 - Ongoing Reviews, Audits and Risk Assessments

Essential to any program is ongoing Monitoring and Assessment of the program itself. The risk constantly changes and so you need to regularly review your policies, practices and procedures against the evolving risks. Our Essentials package provides a suggested bi-annual scheduled Risk Assessment reviews and Audits to ensure you remain compliant.

Pricing

There are three elements to the program pricing:

- uplifting and securing of the Office 365 tenancy, configuration of monitoring agents and equipment
- the ongoing per user cost of monitoring
- the initially suggested compliance reviews and inspections to ensure ongoing compliance.

The Shaping Up charge varies depending on current state as determined by the Microsoft Security Score card and complexity of your environment. The Shaping Up costs are tiered for tenancies with scores less than 75%, 50% or %25 of the possible score. That is; the better your initial score, the less is required to get the environment up to shape and the lower the Shaping up charge will be.

Shaping up	Ongoing	Reviews
• Once off fee	• $9.50 Per User (Monthly) • $10.00 Per Device (Monthly) • $8.24 per user (Microsoft 365 P1 License Monthly)	• Once off fee per Review

Pricing quoted is exclusive of GST, minimum 12 month term applies.

CONSULT . DELIVER . SUPPORT

Calibre One Contact Points

For over the phone support
1300 422 542

For support via email
mss@calibreone.com.au

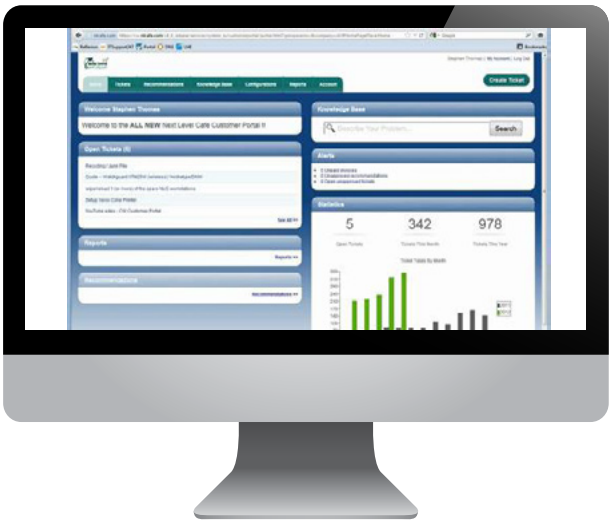
For Sales, your Account Manager or our Finance and Admin Team call:
1300 4 Calibre (1300 422 542)

Or email

Sales	**sales@calibreone.com.au**
Finance/Accounts	**accounts@calibreone.com.au**
Account Manager	**myaccountmanager@calibreone.com.au**

Online Access

Create, view and report on your tickets through our online portal, access given on request.



C1 CALIBRE ONE