Cyber-crime is rising.

The last two years alone have seen significant increase in reports of cyber criminal activity and majority of this activity is financially motivated.

Cyber criminals don't discriminate by sector, location or by size. They target organisations around the world based on what they do and what kind of information they hold.

Organisations that process or store Personally Identifiable Information (PII) and other sensitive information, are prime targets.

Cyber criminals often specifically target smaller organisations because they know it's unlikely they have invested in the necessary security controls /training to protect their systems and their information.

It's easier to steal from smaller organisations.

What's more, 90% of cyber security incidents are caused by human error - do you or your staff know how to identify sophisticated scams? How do you account for your privileged user activity?
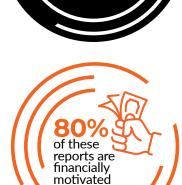
Organisations leave themselves exposed and at a risk of a massive data breach of information when a business owner:

▶ doesn't understand the right security requirements for their organisation

▶ doesn't understand their risk posture or acceptable risk level

▶ doesn't understand how susceptible their organisation is to cyber crime

So what can be done?...

200% increase in cyber crime reports

80% of these reports are financially motivated

90% of cyber incidents are caused by human error

WATCHFULNESS | GUARDIANSHIP | SECURITY

CYBER CERBERUS

The threats are real and numerous!

CRACKS

DATA VIRUS

THEFT

SOCIAL MEDIA ATTACKS

MALICIOUS SOFTWARE

VIRUS

CYBERWARFARE

SOFTWARE FAILURE

NETWORK SNIFFING

YOUR DATA SAFETY

SPYWARE

HUMAN ERROR

SOFTWARE ERROR

STOLEN INFORMATION

TROJAN

CYBER ATTACKS

HACKING

PASSWORD CRACKING

FRAUD

CYBERCRIMINALS

TROJAN

ADWARE

SYSTEM PENETRATION

CYBERSTALKING

Cyber Cerberus is committed to protecting large and small organisations in today's continually evolving cyber landscape.

70% of organisations fear their cyber security risk is increasing.

To combat this, Cyber Cerberus conducts security audits to identify everything that your organisation isn't prepared for or doesn't know about cyber security.

We identify weaknesses in your IT environments, assess them and provide a remediation roadmap. We do this through:

1. Thorough stakeholder engagement (including your managed service provider/s)

2. Comprehensive audit and assessment

3. Cyber maturity and organisational risk assessments

4. Remediation plans and roadmap development

5. Identifying solutions/opportunities to enhance the maturity of your IT/Digital environment.

At Cyber Cerberus, we align our audit methodology with several information security standards, depending on the complexity and legislative requirements of the business.

We offer the following services:

▸ Security Audit and Assessment
▸ Privacy Impact Assessments
▸ Disaster Recovery Assessment
▸ Open-Source Intelligence Assessments
▸ Penetration Testing / Vulnerability Assessments
▸ Security / Solution Architecture Reviews
▸ Network Device & Infrastructure System Reviews
▸ Threat & Risk Assessments

Cyber Cerberus specialises in helping organisations to realise and manage their cyber security risks to develop a strong, established and mature cyber security posture.

Contact us to discuss how we can help reduce your organisation's susceptibility to cyber-crime.

Email: hello@cybercerberus.com
Phone: 0404 092 538

Visit **www.cybercerberus.com** for more information.

WATCHFULNESS | GUARDIANSHIP | SECURITY

CYBER CERBERUS