Casobe & Co

Information Security: Governance: Assurance

prepare for the unknown

stay in control in an age of evolving cyber threats

Intelligence Led Insurance

Intelligence Led Underwriting - Cyber

All too often, there can be a disparity between what a client proposes to require insurance for and the level of cover an underwriter is willing to accept. As a consequence, a misunderstanding of the risk can result in no cover or inappropriate cover and risk allocation, coupled with excessive premiums. Utilising an intelligence led approach for underwriting and risk assessment, we ensure that technological and Cyber risk can be identified, managed, mitigated and insured.

Cyber Resilience and Risk Assessment

Manny organisations will accept that Cyber threats pose a constant and evolving risk to commercial activities. Such risks need to be identified, quantified and mitigated as part of the strategic roadmap and integrated into operational procedures. The threat vector for Cyber risks is pervasive across the entire organisation, and is not solely an IT focused technology matter.

Organisations require a vigilance approach to Cyber risk, through organisational development and change an integrated and strategic approach, permits executives the opportunity to make well informed security decisions.

Source: The 2016 Global State of Information Security Survey

Risk and Realities or Media Hysteria ?

A Cyber threat can have significant impact on an organisation, its operations and invariably compromise a corporate brand, resulting in financial loss for an organisation and potential liability for its executives and officers. There are many documented cases within the media, the number for which is increasing daily. The associated effect is an increase on claims under respective policies and a requirement to investigate, remediate and recover from the event, where possible.

Accompanying the commercial risk activities, across Asia Pacific, US, Africa and EU, there is dramatic increase targeted use to organisations in the use of;

- State sponsored activities
- Serious and organised crime
- Interest motivated groups
- Cyber terrorism

Objective: Identify and quantify Cyber risk, to provide better security posture intelligence on which underwriters and clients, can base quantitative risk decisions and tailor insurance appropriately.

Cyber Risk Assessment

- **Co #** - 610 303 896
- **ABN** - 86 610 303 896

Po Box 2688
Clarkson, WA
6030, Australia

E- info@casobe.com

www.casobe.com

Casobe & Co

Information Security: Governance: Assurance

prepare for the unknown

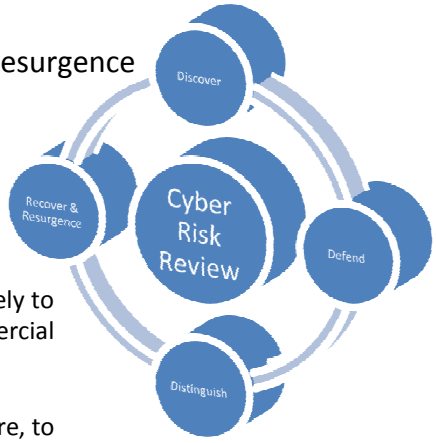
stay in control in an age of evolving cyber threats

Our Approach to Risk

Intelligence Led Underwriting - Cyber

A continual and pragmatic risk based approach is required, to identify, mitigate and manage Cyber risks. Risk can emanate from people, process and technology and Cyber should not be siloed just as a technical risk and solution. Our approach to Cyber Risk Assessment Framework, covers four key integrated and iterative areas. These are.

Discover, **D**efend, **D**istinguish, **R**ecovery and Resurgence



Cyber Resilience and Risk Assessment

All organisations are unique as too challenges that they face. A uniform one size fits all is not likely to have effective application in an environment of evolving business market activities, commercial obligations and cyber threats.

To stay ahead and prepared, many organisations must continually review their Cyber risk exposure, to identify, manage and mitigate risks.

The Casobe Approach

Understanding technical risk and commercial practice, we can engage with executive management, underwriters or their agents, to provide a clear and concise risk assessment of an organisational commercial and technical security posture. Our approach will focus an organisation to consider:

- What are the categories and class of data that we hold ?
- What technology and process integrate with this data ?
- Whom has access and how is this regulated ?
- Are there any governance and regulatory controls applicable to reduce risk ?

Working with clients on the Cyber Risk Review, we can base our assessment on our Cyber Resilience Model and relevant security frameworks and guidance such as:

- ASD Mitigation Strategies
- ASIC Report 429 – Cyber Resilience Health Check
- NIST – Framework for improving Critical infrastructure Cyber security
- APRA PPG 234 – Management of Security Risk in Information and Information Technology

Cyber Risk Assessment

- **Co #** - 610 303 896
- **ABN** - 86 610 303 896

Po Box 2688
Clarkson, WA
6030, Australia

E- info@casobe.com

www.casobe.com

Casobe & Co

Information Security: Governance: Assurance

prepare for the unknown

stay in control in an age of evolving cyber threats

Cyber Risk Model

Cyber Resilience Model

Our comprehensive approach is based on relevant government and regulatory requirements, undertaken by appropriate practitioners.

Discover	Asset Management	Corporate Environment	Governance	Risk Assessment	Risk Strategy	
Defend	Access Management	Training	Data Security	Info Sec Procedures	Maintenance	Proactive Technology
Distinguish	Detection Mechanisms	Security Monitoring	Security Incidents	Analytical Reporting		
Recovery	Planning	Communications	Evaluation	Remedial Measures	Review and Improvement	

Resilience and Risk Scale

Our assessment of Cyber resilience is quantified on the following scale.

Resilience Scale	1 – No Resilience	2 – Limited Resilience	3 – Risk Informed	4 - Repeatable	5 – Adaptive High

Risk High — Risk Medium — Risk Low

Cyber Risk Assessment

Po Box 2688
Clarkson, WA
6030, Australia

E- info@casobe.com

www.casobe.com

- **Co #** - 610 303 896
- **ABN - 86 610 303 896**

Casobe & Co

Information Security: Governance: Assurance

prepare for the unknown

stay in control in an age of evolving cyber threats

Cyber Risk Intelligence

Relevant Reporting

Our reporting is clear, concise and precise to assist executives and stakeholders make informed decisions.

Whilst our evolutionary and comprehensive approach to Cyber Resilience is holistic and leading edge, it also needs to be quantified and presented in visible and digestible sections. If any media does not communicate its meaning effectively, then any Cyber Resilience Plan has a high degree of failure, before it can be adopted.

Strategic Reporting – Dashboard

An executive and stakeholder report, with acute salient points, such as:

- How resilient is our organisation across all the cyber domains ?
- What are our strengths and vulnerabilities ?
- How do we refine or Cyber Strategy based on the outcomes ?
- What are the independent recommendations ?
- What would a strategic roadmap look like in the short to medium term addressing the key issues raised ?

Detailed & Technical Cyber Risk Reporting

We can provide the substantive detailed technical risk data that supports our strategic analysis. This enables the operational element of the organisation to focus and streamline activities, process and controls (as appropriate) to mitigate risk on the basis of comprehensive documented findings.

LLOYD'S
LLOYD'S OF LONDON

Additional Reporting

Our Cyber Resilience Reporting can complement and integrate with other documentation. It is possible for some concurrent activity, to review and focus on updating such material. For example:

- Enterprise Framework
- Crisis and Incident Management Protocols
- Information Security Policy, Guidelines and Control Sets

Cyber Risk Assessment

Po Box 2688
Clarkson, WA
6030, Australia

E- info@casobe.com

www.casobe.com

- **Co #** - 610 303 896
- **ABN - 86 610 303 896**

Casobe & Co

Information Security: Governance: Assurance

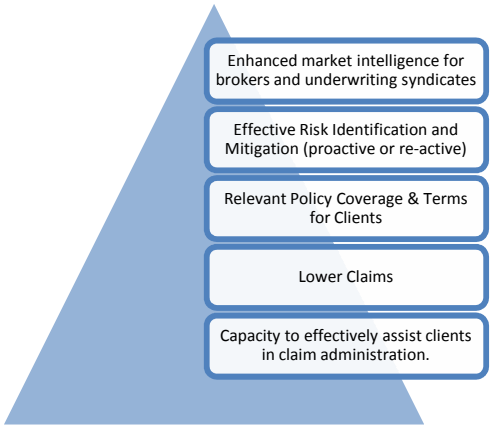
Intelligence Led Underwriting

- The time to act is now – don't wait until you are attacked and there is a potential claim
- We are ready to help you shape your security posture and mitigate Cyber Risk for the future
- You need a guide with experience of known and unknown threats
- Take your next steps with us.

Our Benefits

Casobe is bespoke with it clientele solutions. Our Principles have pioneered techniques which are at the forefront of our industry, and practiced globally. We understand risk, its application to technology and relevant measures of support to mitigate these. In delivering our services, we understand our clients requirements and continually review the service delivery to effect best practices and market changes. From engaging our services to reduce cyber risk on critical infrastructure in hostile environments, to assisting with IT Strategy and development for a government executive agency, our partnered and collaborated approach will aim to ensure support from all project stakeholders.

Insurers Value



Our Principles have been undertaking risk assessment work for underwriting syndicates and brokers for over two decades. At Casobe, we can provide an overview of salient risks and key mitigation provisions which can be tailored into policy coverage. In short, you know what is insured, the relevant risk exposure and in the event that insurable event transpire, that stakeholders have adequate capacity and professional vendor support to assist your clients mitigate the event.

Supporting and intelligence led risk assessment, permits more accurate and competitive insurance quotation and appreciation of risk and cover, for underwriter, broker and the end client.

Po Box 2688
Clarkson, WA
6030, Australia

E- info@casobe.com

www.casobe.com

Think of Reducing Cyber Risk.
Always **Think Casobe.**

Co # - 610 303 896

ABN - 86 610 303 896

V1a 2016