Cyber Risk Assessment

bellrockadvisory.com

Bellrock approach to Cyber Risk

Bellrock view Cyber Risk as ordinarily pervasive and integrated within an organisation culture and operations. It is not therefore a siloed IT discipline. In order to undertake an effective Cyber Risk and Maturity Assessment, Bellrock work with leading cyber risk specialists Casobe & Co to deliver an overview assessment of your organisation's information security and governance posture.

As part of the process, a number of barometers are utilised to establish the cyber risk, threat landscape, vulnerabilities and response capabilities engaged to protect and defend from a potential security incident. The approach as an overview will investigate cyber risk awareness, review the governance enforced, technical and management controls over information security and the implementation and monitoring of the information security eco system.

Our assessment and methodology will aim to benchmark your organisations against appropriate best practice and governance frameworks such as ISO/IEC27001; PCI-DSS; NIST and others. The assessment will review a number of information security areas, and each are independently assessed and subsequently evaluated to provision an overall Cyber Maturity Risk Rating.

Remote Assessment
The standard assessment is conducted remotely via a video or conference call, through open dialog against appropriate question sets. These will cover a range of security areas. The length and depth of each will vary from assessment to assessment, dependent upon client market segment and operational involvement with technology. Each customer is unique, and Bellrock acknowledge this. We believe that greater clarity can be achieved during focused discussion than completing a similar detailed activity on-line. The outcome is a tailored, unobtrusive and streamlined process, with appropriate recommendations identified for your organisation.

Getting the most from the assessment
The approach will be predominantly based on the information which is made available and discussed during the executive assessment. Please note, it is not intended that the remote assessment will identify or cover all and every information risk that may be prevalent to you. Clients wishing to gain the most benefit from the assessment will be strongly encouraged to provision all information requests through Bellrock in advance of the scheduled assessment. Information available for assessment in advance will ordinarily permit a greater opportunity to focus on key areas during the meeting to provide further and detailed insight on information available.

Why a Cyber Risk Assessment?

01 Discharge directors' duties (enquiring mind test, "we know the risk exists, what have we done to address and mitigate against it?)

02 Understand cyber resilience.

03 Ensure compliance with a company's obligations for the data it holds.

04 Ensure an adequate response in case of a security breach.

05 Identify commercial risks that arise from contractual undertakings.

06 Enable Bellrock to obtain appropriate cyber insurance.

Our approach

Approaching the assessment
There are a number of prerequisite activities that must be completed in advance of the Assessment, to ensure that logistics are arranged, and the maximum benefit can be achieved. These are outlined under Stakeholder Involvement below.

Delivering the assessment
The scope of the assessment will be aimed to align the approach to appropriate Information Security frameworks and best practice. The review will focus on physical, environment and operational security in addition to technical and procedural security controls to defend against cyber risks.

Areas of assessment
The key areas of assessment are as follows, and are tailored according to the applicability of each client and proposed areas of insurance under consideration:

- Organisation of IS, training and skills
- IS Governance
- Personnel security and education
- Physical and environmental security
- Vendor Supply Chain Management
- IT Operation Security
- Privacy and Media Relations
- Asset Management
- Identity and Access Control
- System development and maintenance
- Cyber Security and Incident Management
- Business Continuity and Resilience
- Appropriate Compliance such as PCI-DSS, SSAE 16, ISAE 3402, Privacy etc.

Cyber landscape

Rapid evolution of Cyber Risk
The cyber risk landscape is continually evolving. The number of vulnerabilities which could affect a business consistently increases year on year as threat actors actively continue to explore and exploit technologies to gain access to unsecured systems. This is why at Bellrock, we view Information Security holistically as part of our approach to assessing a business's cyber maturity risk.

Dependent upon the root cause of a claim under a Cyber Liability Policy, a cyber claim could subsequently impact a business's other insurance policies including Professional Indemnity, Directors and Officers or Public Liability leading to increased premiums or even a larger excess.

Recent high profile breaches

The increase in frequency and severity of cyber attacks as referenced below, has prompted a growing awareness of cyber risk at board level. In a recent survey, 95% of Australian CEOs identifyied cyber risk as the top threat to business growth.

2018

Facebook
87 million records. Cambridge Analyitica.

Aadhaar
1.1 billion Indian citizen data records compromised.

Under Armour
150 million MyFitnessPal customer records compromised.

2019

Capital One
100 million records compromised.

Travel Ex
Foreign Exchange Platforms.

Bio Star 2
Biometrics data breach.

2020

Cam14
10 billion records compromised.

Advanced Info Service
8.3 billion records compromised.

Microsoft
250 million records compromised.

2021

Microsoft Exchange
Server breach, 30,000 organisations compromised.

Channel Nine
Largest attack. Hundreds of companies across 17 countries compromised.

Kaseya
Ransomware attack. Hundreds of companies across 17 countries compromised.

Uniting Care
Ransomware attack, systems compromised.

2022

Woolworths MyDeal
2.2M customer records brached.

Optus
9.8M customer records breached. Ongoing class action.

Medibank
9.7M customer records breached.

Twitter
5M user accounts breached.

Toyota
Malicious cyber attack resulting in temporary shut down of 14 vehicle assembly plants in Japan.

2023

MOVEit
Software hack impacting 600 organisations worldwide, leading to over 600 separate breaches.

Australian Defence Force
2.5M documents downloaded.

Latitude Fiance
14 million customers affected. 98 million incurred costs.

2024

TicketMaster
560 million customers affected.

Qantas
Privacy breach exposing customer's travel information.

MediSecure
Data breach impacting personal and health information.

Fujitsu
Malware attack resulting in the theft of customer information.

Documentation checklist

What information do we need?
In order to ensure efficient analysis of your information security environment, access to the following information is beneficial in ensuring that all parties achieve the most from the assessment process.

Governance, legislation, security controls and best practice respective to information security will vary across industries, organisations and geographical operational boundaries. In this Executive Assessment, the approach will not be finite regarding documentation required.

However, we would respectfully ask for the following or similar derivatives which you may have available and appropriate to your organisation:

	Key Document	Context	Provisioned
1.	Previous Cyber Security Assessments or Audits	Provision of previous review and findings may allow you to demonstrate how identified cyber security risk has been managed or mitigated.	
2.	Business Continuity Plans (BCP)	Provision of an appropriate documented operational BCP to identify the scope of the plan and allocation of responsibilities. Any Business Impact Assessment document would be beneficial.	
3.	Crisis Management Plan (CMP)	Provision of an appropriate documented operational BCP to identify the scope of the plan and allocation of responsibilities and mediaresponse plans.	
4.	IT Disaster Recovery Plan (IT DRP)	IT DRP which details key procedural steps in recovery of IT Services as outlined in CMP/BCP	
5.	Information Security Policies	Overview and copies of the respective Information Security Policies, including but not limited to Acceptable Use Policies, Information Security Policy and Data Privacy	
6.	Privacy Impact Assessment (PIA)	A PIA governing the enterprise wide use of technology and management of personal and confidential data.	
7.	IT Operational Security Procedures	Overview of the IT Operational Security Procedures.	
8.	IT Infrastructure Topology Diagrams	High level schematic or network architecture and systems interaction diagrams. This should also include the security architecture engaged.	
9.	Staff Vetting Policies	Overview and copies of HR procedures for Staff Vetting.	
10.	Vendor Management Policies and Governance	Policies and procedures for ensuring vendors information security practices are commensurate with your own organisational requirements and legal and risk management is undertaken.	
11.	Software Development Lifecycle Policies and Procedures	Security objectives relating to the development and deployment and use of internal and external developed code.	
12.	Cyber Insurance Policy Schedules	Schedule specifying scope of cover currently in place and requested.	
13.	(Master Service Agreement and Service Level Agreement) Critical IT Vendors	Contractual documents from Application Providers Managed Service Providers (Service Desk, Web Hosting, Critical Business Applications development and support etc) That govern the use and service provisions.	

Assessment process

Conference call

How long does it take?

Ordinarily the conference call and assessment should be scheduled for around 1.5 - 2 hours. The time and content can be ordinarily adjusted dependent upon the dialog stakeholder preferences and information provisioned in advanced. The main focus is to make available key individuals whom have operational knowledge of data security, in particular with reference to the discipline areas as outlined on the previous page.

Whom should attend?

As an indication, the following stakeholder positions or equivalents should be considered;

Client;

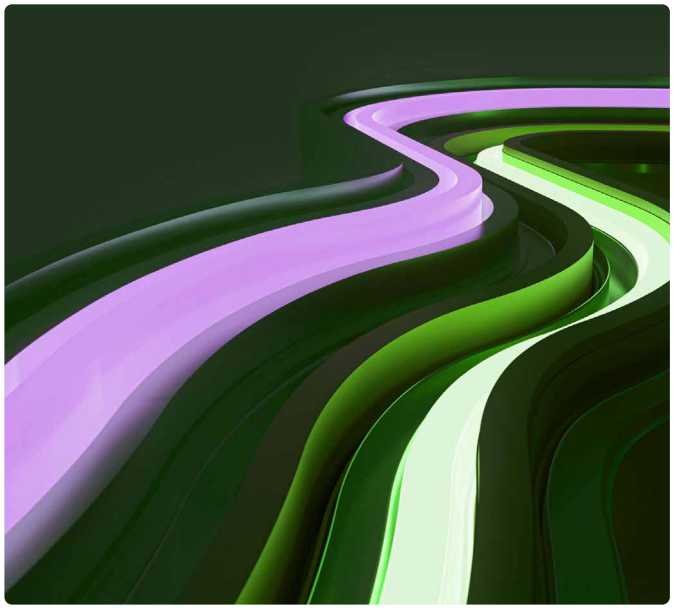
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Risk Officer (CRO)
- Technical Services Director
- Group Risk and Continuity Manager
- IT Manager
- Head of Compliance

Advisor;

- Client Manager (not essential)

Casobe & Co

- Security and Governance Assessors.



Structure of the call

The conference call will aim to follow a standard format but may be varied slightly in line with advance information provision or any time constraints. It is important that advance quality information is provided succinctly a minimum of 72 hours prior to the call.

Casobe & Co will ordinarily co-ordinate the discussions between all parties, asking relevant questions. Nonetheless, our experience would suggest that all parties engage in open dialog, to ensure the optimum information exchange can be achieved, in the time allocated assessing the key areas under discussion.

Introduction: 5 mins

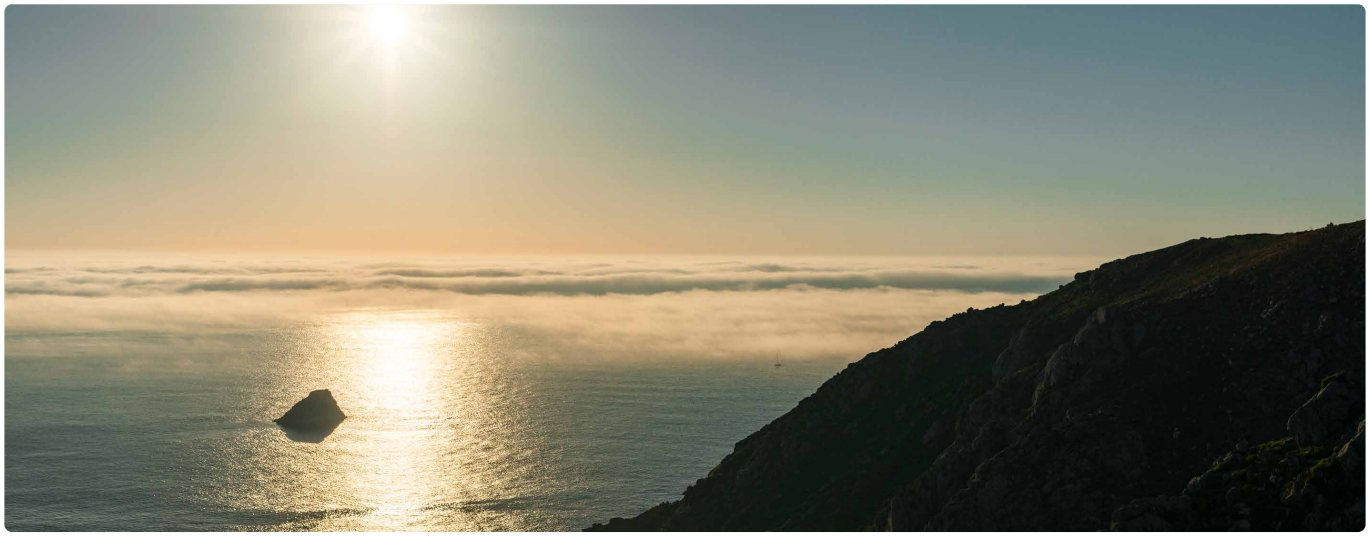
- Advisor makes introductions.
- Casobe & Co confirm format, attendees and agenda.

Assessment: Up to 2 hours

- Casobe & Co will lead with question and answers dialog on security matters outlined in Delivering the Assessment.
- Timing is ordinarily kept to 90 mins in the maximum, and should be comfortably completed in this time frame. Answers should be clear, concise and precise and supportedby evidence where appropriate.
- Open dialog between all participants

Conclusion: 5 mins

- Summary and opportunity for stakeholders to understand and seek clarifications on the content or process on-going.



Reporting
An Executive Cyber Security Assessment will ordinarily be produced within 14 days of receipt of all completed information and conference call. The information, provisioned jargon free and in plain English, will ordinarily contain:

- Summary of the conference call and information provision
- Executive Risk assessment and overview of key objectives
- Summary determination of information security risk and overall cyber maturity
- Summary of improvement areas to reduce risk and enhance cyber maturity capability

The report will be delivered as an encrypted document through Bellrock.

Dealing with confidentiality
Casobe & Co, specialise in information security, governance, assurance and risk. We have a specialist team of engineers, lawyers and risk professionals, who's experience is second to none. You can rest assured, that information which is shared with us during the course of the engagement is controlled and managed securely using a range of technical and best practice solutions.

The services which are provisioned to you, are subject to a strict duty of confidentiality between Casobe & Co and Bellrock. We will only use the data for its intended purpose, and do not directly or indirectly use, exploit, sell or otherwise disseminate information obtained (unless legally required to do so), without written consent. In the event that you have a preference for a direct Non Disclosure agreement between Casobe and yourselves, we have a standard form agreement which we will propose for execution.

Please note, thatordinarily conference calls (audio, video or collaboration notes etc) are not recorded. If there is a specific request from a participating party, then express consent from all attendees, must be agreed in advance.

+

Stakeholder involvement

Suggested stakeholder involvement and responsibilities:

Client
- Provision information to ensure an overall process timeline of no more than three to four weeks and make key personnel available for assessment.

Bellrock
- Co-ordinate preferred time for assessment between stakeholders
- Provision preferred communication details for conference call
- Provision all information from client one week in advance of conference call (where possible)
- Ensure outstanding Q&A between parties are facilitated.

Casobe & Co
- Understand stakeholder preferences and suggested scope
- Administer assessment
- Generate and provision a Cyber Risk Maturity Report
- Assist as required in the broking and underwriting process.

About Casobe & Co

Casobe & Co expertise
The Casobe & Co team have over 20 years of designing, building and managing secure systems. Our unique approach to intelligence led insurance, allows us an unparalleled ability to identify key commercial and cyber issues early, in order to review effective options for mitigating and managing risk globally.

Not only do our engineers understand Cyber and Risk, but our key practitioners as qualified lawyers, understand insurance terms, governance and commercial impact that security breaches can have. In short, working with Bellrock, we can quantify Cyber Risk.

Our Insurance work:
Pre-Policy-Risk Assessment
As an indication, the following stakeholder positions or equivalents should be considered;

- Security Assessments
- Ethical Penetration Testing
- Infrastructure and Application Security Assessments
- Vendor and Supply Chain Security Analysis
- Specialist Security Investigations and Threat Intelligence
- Technical and Security Service Level Agreements Assessment
- Risk quantification for Cyber Risk Exposure
- Board Education on Cyber Risk and Exposure
- Governance and Compliance Review
- Client Insurance Requirements for Cyber Risk

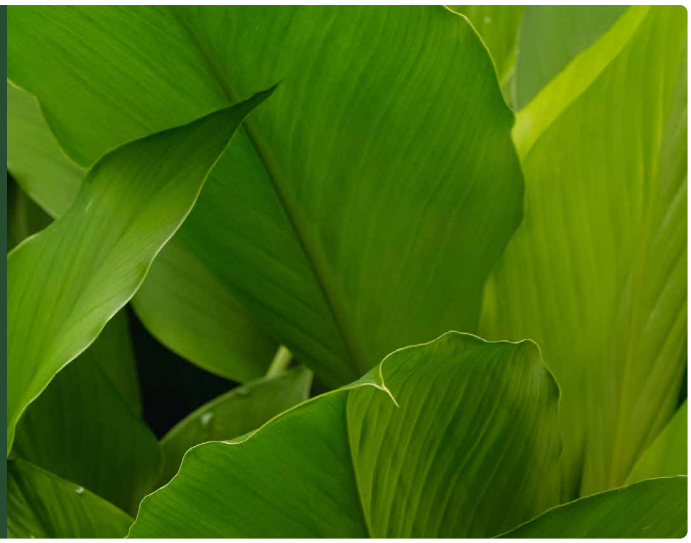
Claims Assistance and Incident Management

- Single Point of Contact for Cyber Incident Coordination
- Emergency Triage and Response
- Executive Assessment of Policy Coverage and Liabilities against breach
- Scope Forensic Investigation on root causation in line with Policy Terms
- Undertake Forensic, root causation and remediation plan
- Assess enterprise wide data breach and client impact.
- Co-ordinate Client Crisis Management Response, relevant stakeholders, on Media, PR Release, First and Third Party Legal matters.
- Provision of Expert Witness as may be required

Other corporate downloads, service deliveries documents and capability statements etc. are available at www.casobe.com

Jonathan McCoy
Managing Director

A leading security practitioner and lawyer, Jonathan has over two decades of delivering technical and commercial solutions globally.



Bellrock

Here to help

Your Bellrock Service Team is here to assist you
Acknowledged as industry thought leaders, Bellrock's Team of Advisors are well known and respected across the industry. Our passion for delivering superior risk advisory and advocacy services to our clients is a cornerstone of our offering. We believe this is reflected in the outcomes we achieve for our clients.

View our full team of Risk Advisors including contact details here.

Bellrock Advisory Pty Ltd
ABN 78 611 143 410 AFSL 520 281

Head Office
Level 25, 171 Sussex St Sydney NSW 2000
Ph +61 2 9188 2460
contact@bellrockadvisory.com