avertro
The cyber-why company

AVERTRO CYBERHQ

Cyber Management Decision System

Data Sheet

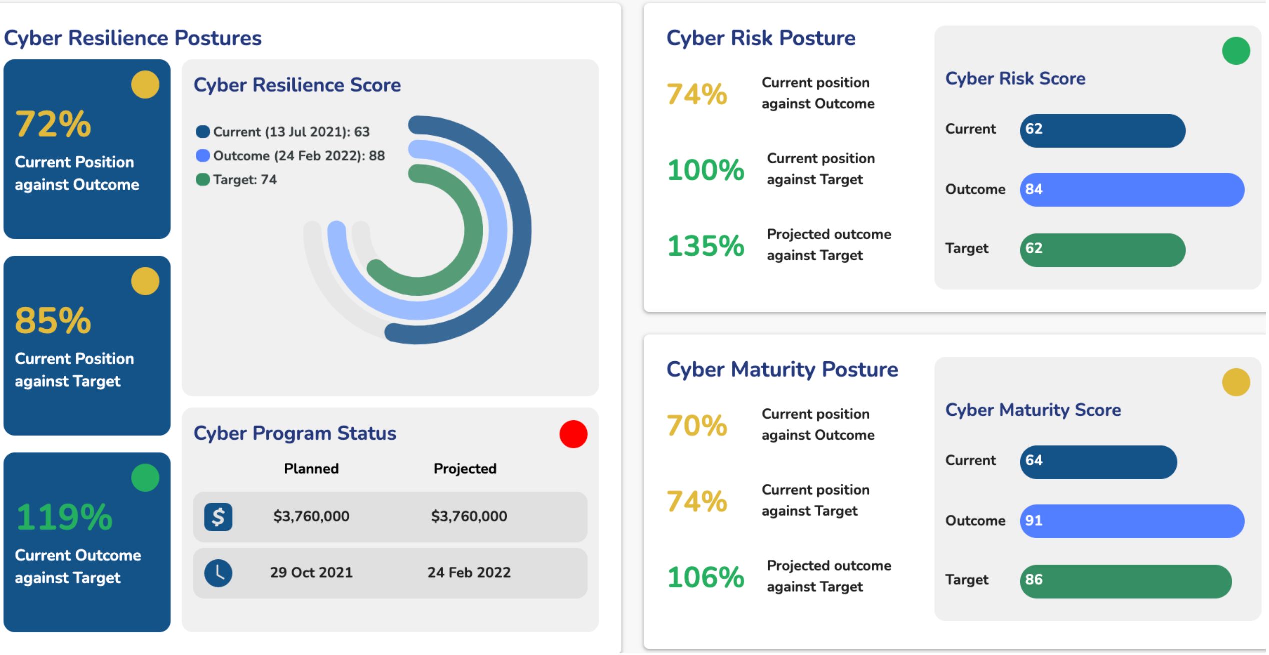
avertro.com

Problem

One of the key challenges facing leaders is the disconnect between the cyber team and everyone else, particularly with the executive layer. Organisations continue to struggle with aligning the tracks. The promise of Governance, Risk and Compliance (GRC) technology was to address this. The reality is that teams still need spreadsheets and consultants. We can do better than the GRC and spreadsheet status quo. Elevating our game requires focusing on the business representation of cyber and building that permanent bridge to translate and normalise cybersecurity for everyone else.

Solution

Avertro CyberHQ® is your Cybersecurity Headquarters (HQ). Elevate your game with a Cyber Management Decision System (MDS) that helps you manage the business of cyber using defensible insights to determine what is essential.



Cyber Resilience Postures

72% Current Position against Outcome

85% Current Position against Target

119% Current Outcome against Target

Cyber Resilience Score

● Current (13 Jul 2021): 63
● Outcome (24 Feb 2022): 88
● Target: 74

Cyber Program Status

	Planned	Projected
$	$3,760,000	$3,760,000
🕒	29 Oct 2021	24 Feb 2022

Cyber Risk Posture

74%	Current position against Outcome
100%	Current position against Target
135%	Projected outcome against Target

Cyber Risk Score

Current	62
Outcome	84
Target	62

Cyber Maturity Posture

70%	Current position against Outcome
74%	Current position against Target
106%	Projected outcome against Target

Cyber Maturity Score

Current	64
Outcome	91
Target	86

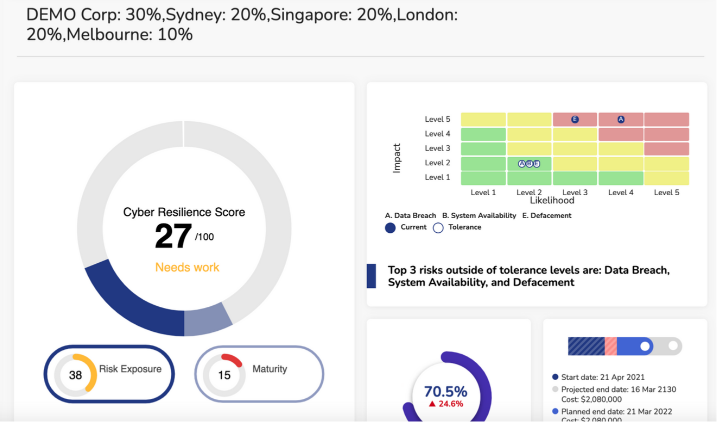
Outcomes

- **Elevate your reporting with** defensible, standardised executive and board reports for cybersecurity using data points from any historical point in time.
- **Continuously assess your cyber risk and maturity posture the way you choose,** and let the platform harmonise and translate between all the regulatory compliance frameworks required for reporting.
- **Get rid of all your spreadsheets** by using the platform as your cyber management information system, a.k.a. your ISMS.
- **Manage and model the business of cyber and right-size spend** by aligning costs with outcomes that make sense to all stakeholders.
- **Forecast, visualise, and report on** future outcomes and timelines.
- **Streamline and automate** the way continuous cyber risk management and assessments are done.
- **Manage issues** (e.g. penetration test findings, audit findings, vulnerability scans) and have these inform business-level cyber risks at all times.
- **Manage third party supply chain** and project cyber risks.
- **Meet** regulatory compliance requirements.

Segmentation

A common challenge for most organisations is that different locations, business units, logical groups (e.g. IT vs OT), or subsidiaries need to be treated differently when it comes to cybersecurity. For example, the cyber resilience of head office may need to be higher than a remote outpost. Other solutions on the market do not provide enough precision and fine-grained control to account for these differences.

CyberHQ® supports the ability to segment an organisation into its sub-units and manage each separately. The platform can take this further, giving you the power and flexibility to consolidate, compare and aggregate your cyber resilience data and reports through segmented lenses as well as a pan-organisational view.



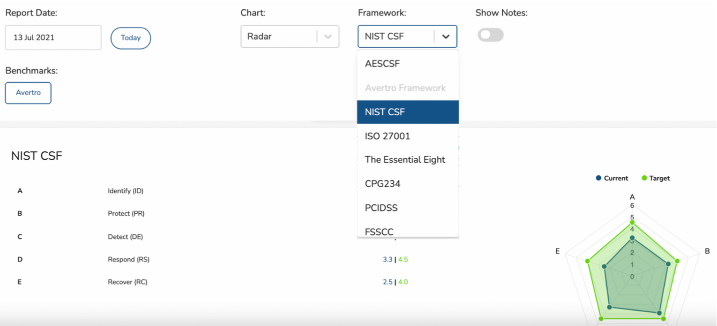
DEMO Corp: 30%,Sydney: 20%,Singapore: 20%,London: 20%,Melbourne: 10%

Top 3 risks outside of tolerance levels are: Data Breach, System Availability, and Defacement

- Start date: 21 Apr 2021
- Projected end date: 16 Mar 2130 Cost: $2,080,000
- Planned end date: 21 Mar 2022 Cost: $2,080,000

Standards Harmonisation

Often, organisations are required to report against a different framework or would like to compare how they fare against a different standard. CyberHQ® has the ability to perform automatic translations between different frameworks as needed.



Report Date: 13 Jul 2021 Today

Chart: Radar

Framework: NIST CSF

Show Notes:

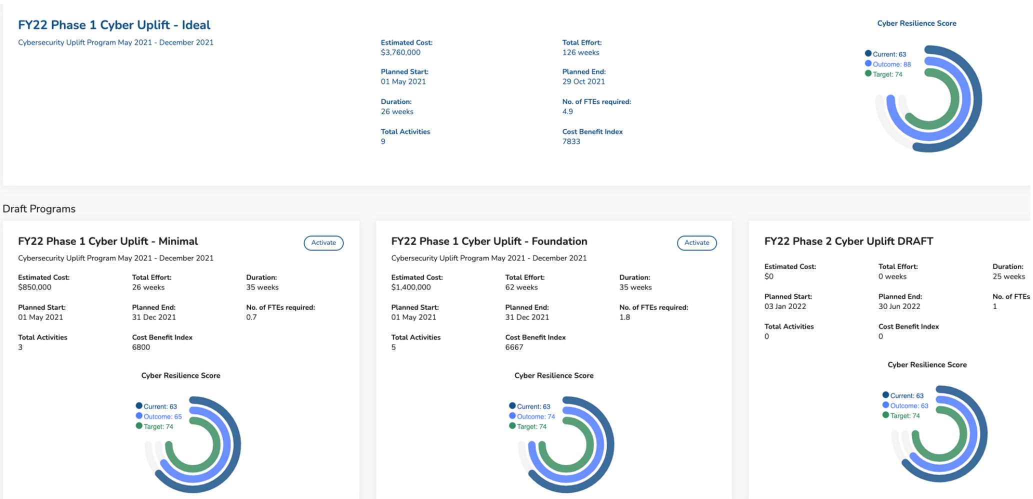
Benchmarks: Avertro

NIST CSF

A	Identify (ID)	
B	Protect (PR)	
C	Detect (DE)	
D	Respond (RS)	3.3 | 4.5
E	Recover (RC)	2.5 | 4.0

Business Case Modelling and Justification of Cyber Spend

Most organisations struggle to right-size their strategy in terms of finding the optimal spend for the desired outcome. Cyber risk is a complex and dynamic construct. Managing a moving target makes it extremely difficult to maintain an optimised cyber strategy at all times. The continuous visibility and business-lens required to address this in an agile manner is something very few organisations have achieved. With CyberHQ®, this becomes easy.



FY22 Phase 1 Cyber Uplift - Ideal

Cybersecurity Uplift Program May 2021 - December 2021

Estimated Cost: $3,760,000
Total Effort: 126 weeks
Planned Start: 01 May 2021
Planned End: 29 Oct 2021
Duration: 26 weeks
No. of FTEs required: 4.9
Total Activities 9
Cost Benefit Index 7833

Cyber Resilience Score
- Current: 63
- Outcome: 88
- Target: 74

Draft Programs

FY22 Phase 1 Cyber Uplift - Minimal Activate

Cybersecurity Uplift Program May 2021 - December 2021

Estimated Cost: $850,000
Total Effort: 26 weeks
Duration: 35 weeks
Planned Start: 01 May 2021
Planned End: 31 Dec 2021
No. of FTEs required: 0.7
Total Activities 3
Cost Benefit Index 6800

Cyber Resilience Score
- Current: 63
- Outcome: 65
- Target: 74

FY22 Phase 1 Cyber Uplift - Foundation Activate

Cybersecurity Uplift Program May 2021 - December 2021

Estimated Cost: $1,400,000
Total Effort: 62 weeks
Duration: 35 weeks
Planned Start: 01 May 2021
Planned End: 31 Dec 2021
No. of FTEs required: 1.8
Total Activities 5
Cost Benefit Index 6667

Cyber Resilience Score
- Current: 63
- Outcome: 74
- Target: 74

FY22 Phase 2 Cyber Uplift DRAFT

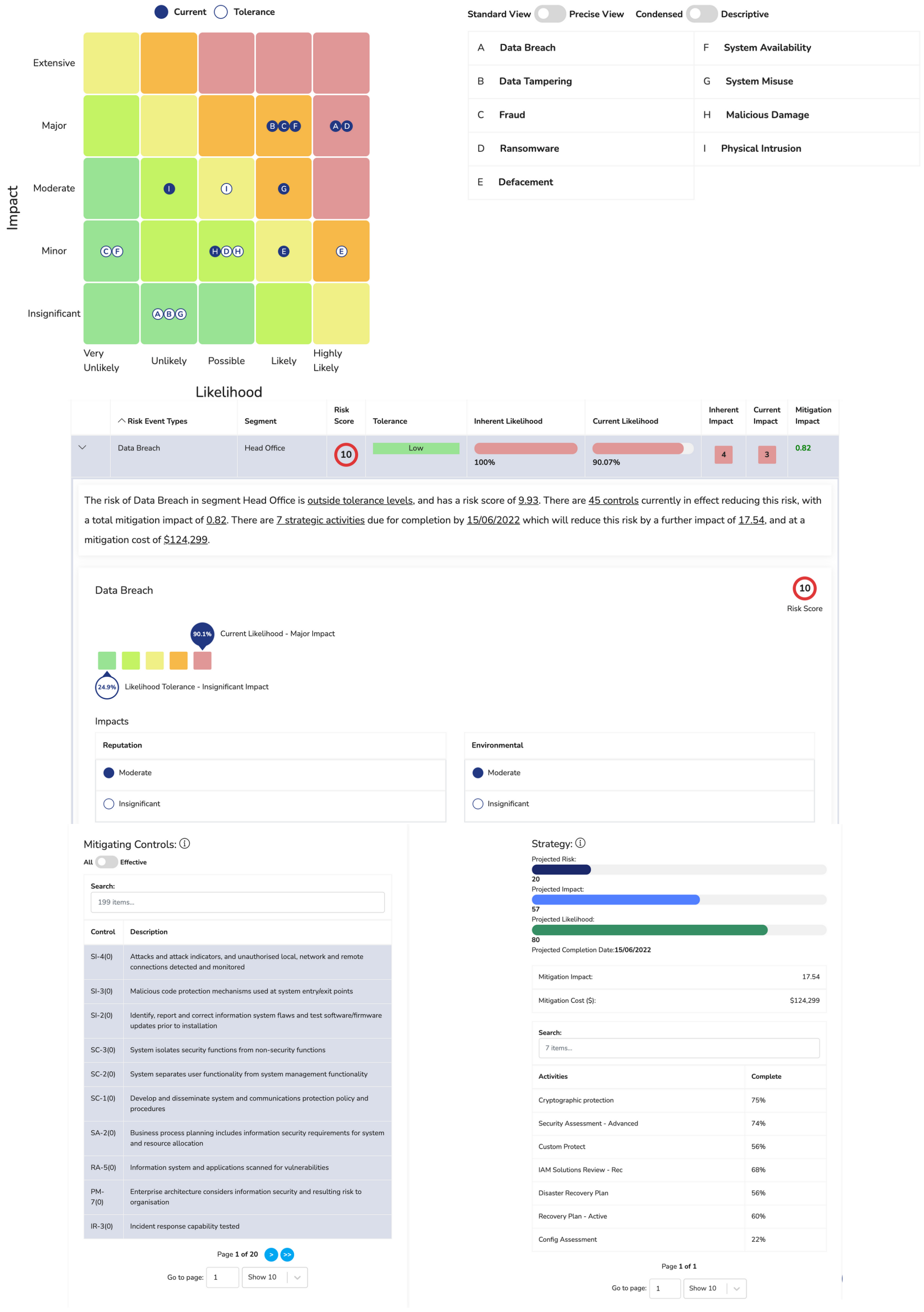
Estimated Cost: $0
Total Effort: 0 weeks
Duration: 25 weeks
Planned Start: 03 Jan 2022
Planned End: 30 Jun 2022
No. of FTEs 1
Total Activities 0
Cost Benefit Index 0

Cyber Resilience Score
- Current: 63
- Outcome: 63
- Target: 74

Cyber Risk Management

Cybersecurity is ultimately about managing risk. CyberHQ® fast-tracks an organisation’s ability to identify, track and manage its cyber risks for executives at the business level, and cybersecurity teams at the technical level.

The platform provides a set of pre-configured, industry-curated business-level cyber risks and key risk indicators. CyberHQ® can also manage already identified cyber risks while offering further customisations to align with an organisation's enterprise risk framework.



Standard View ○ Precise View Condensed ○ Descriptive

A	Data Breach	F	System Availability
B	Data Tampering	G	System Misuse
C	Fraud	H	Malicious Damage
D	Ransomware	I	Physical Intrusion
E	Defacement		

	Risk Event Types	Segment	Risk Score	Tolerance	Inherent Likelihood	Current Likelihood	Inherent Impact	Current Impact	Mitigation Impact
	Data Breach	Head Office	10	Low	100%	90.07%	4	3	0.82

The risk of Data Breach in segment Head Office is outside tolerance levels, and has a risk score of 9.93. There are 45 controls currently in effect reducing this risk, with a total mitigation impact of 0.82. There are 7 strategic activities due for completion by 15/06/2022 which will reduce this risk by a further impact of 17.54, and at a mitigation cost of $124,299.

Data Breach

10
Risk Score

90.1% Current Likelihood - Major Impact

24.9% Likelihood Tolerance - Insignificant Impact

Impacts

Reputation	Environmental
● Moderate	● Moderate
○ Insignificant	○ Insignificant

Mitigating Controls: ⓘ

All ○ Effective

Search:
199 items...

Control	Description
SI-4(0)	Attacks and attack indicators, and unauthorised local, network and remote connections detected and monitored
SI-3(0)	Malicious code protection mechanisms used at system entry/exit points
SI-2(0)	Identify, report and correct information system flaws and test software/firmware updates prior to installation
SC-3(0)	System isolates security functions from non-security functions
SC-2(0)	System separates user functionality from system management functionality
SC-1(0)	Develop and disseminate system and communications protection policy and procedures
SA-2(0)	Business process planning includes information security requirements for system and resource allocation
RA-5(0)	Information system and applications scanned for vulnerabilities
PM-7(0)	Enterprise architecture considers information security and resulting risk to organisation
IR-3(0)	Incident response capability tested

Page **1 of 20** > >>

Go to page: 1 Show 10

Strategy: ⓘ

Projected Risk:
20
Projected Impact:
57
Projected Likelihood:
80
Projected Completion Date:**15/06/2022**

Mitigation Impact:	17.54
Mitigation Cost ($):	$124,299

Search:
7 items...

Activities	Complete
Cryptographic protection	75%
Security Assessment - Advanced	74%
Custom Protect	56%
IAM Solutions Review - Rec	68%
Disaster Recovery Plan	56%
Recovery Plan - Active	60%
Config Assessment	22%

Page **1 of 1**

Go to page: 1 Show 10

What Makes CyberHQ® Unique?

Our research and development efforts, access to industry experts, and extensive experience has meant our platform is built on the right ontology, taxonomy, language, data relationships, data models, and algorithms.

Avertro CyberHQ® leads the industry. We have the most comprehensive, defensible, visual platform on the market. Best of all, our customers can be sure that they are doing cyber right simply by using the platform.

Where Does the Data Come From?

Avertro CyberHQ® has pre-built integrations with many systems, including AWS, Azure, ServiceNow, Jira, and common security operational tools. While we constantly add to our list of integrations, there is scope to build custom connectors to and from the platform through our API should the need arise.

In addition, we are the system of record for a large number of data points required for the ongoing management of cybersecurity. We help streamline and automate the workflows and ongoing monitoring, collection, and attestation of this information to reduce the significant burden of work normally required.

Use Cases

- Cybersecurity Executive and Board Reporting.
- Historical and Predictive Point-in-Time Reporting via the "Time Machine".
- Cybersecurity Business Case Justification.
- Cybersecurity Cost Benefit Modelling and Analysis,
- Third Party Supply Chain Cyber Risk Management.
- Cybersecurity Service Catalogue Management.
- Cybersecurity Issues Management and Technical Risk Register.
- Cybersecurity Strategy Management.
- Cybersecurity Project Management.
- Cybersecurity Asset Management.
- Regulatory Compliance Reporting.
- Continuous Controls Monitoring.
- Cyber Risk Assessments.
- Cyber Maturity Assessments.
- Cybersecurity Governance, Risk and Compliance Management.

Email us today at info@avertro.com for a demonstration of how Avertro CyberHQ® can help you be the hero in your own cyber story.

avertro
The cyber-why company

The Avertro platform is the Cyber Management Decision System (MDS) helping leaders manage, measure and report on cybersecurity performance, empowering them to make the right cybersecurity decisions for the organisation, improve cyber resilience and level up their cyber game.

For more information, visit https://avertro.com