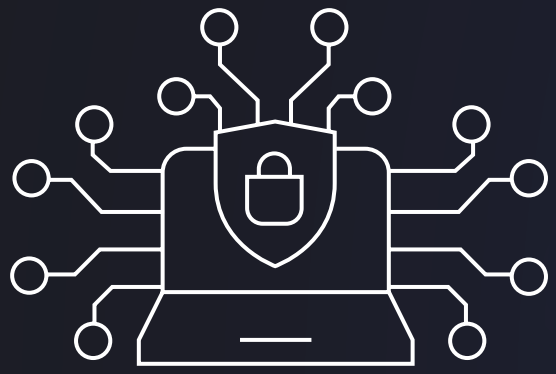
CyberMatics Playbook

Award-winning cybersecurity insights and analytics

AIG



CyberMatics is AIG's award-winning technology-driven process to help organisations verify their cyber risk postures, prioritise the implementation of cyber risk controls and make more informed investment decisions in their cyber security programmes.

CyberMatics is provided as a complimentary service to eligible AIG cyber clients. This booklet outlines: how CyberMatics works, the information and insights clients receive from its dynamic dashboard, the key benefits for businesses, and how to obtain and activate CyberMatics.

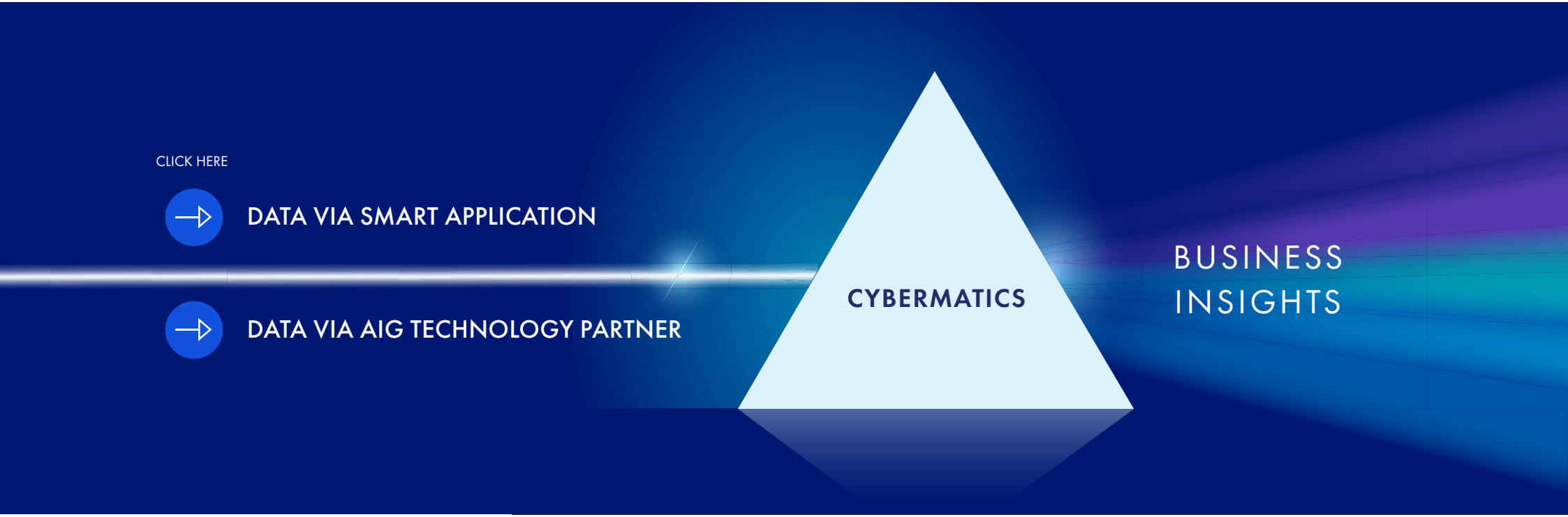
HOW CYBERMATICS WORKS
THE DYNAMIC DASHBOARD
BUSINESS BENEFITS
GETTING CYBERMATICS

GO BACK

How CyberMatics works

CyberMatics is fed by two data sources. Firstly, cyber underwriting information is provided by the business via AIG's smart application form. Secondly, cyber data is delivered and continuously updated by one of our technology partners the business chooses to work with. This information is synthesized using AIG's patented technology driven model, to generate incredible insights for the business.

AIG's Patented Model

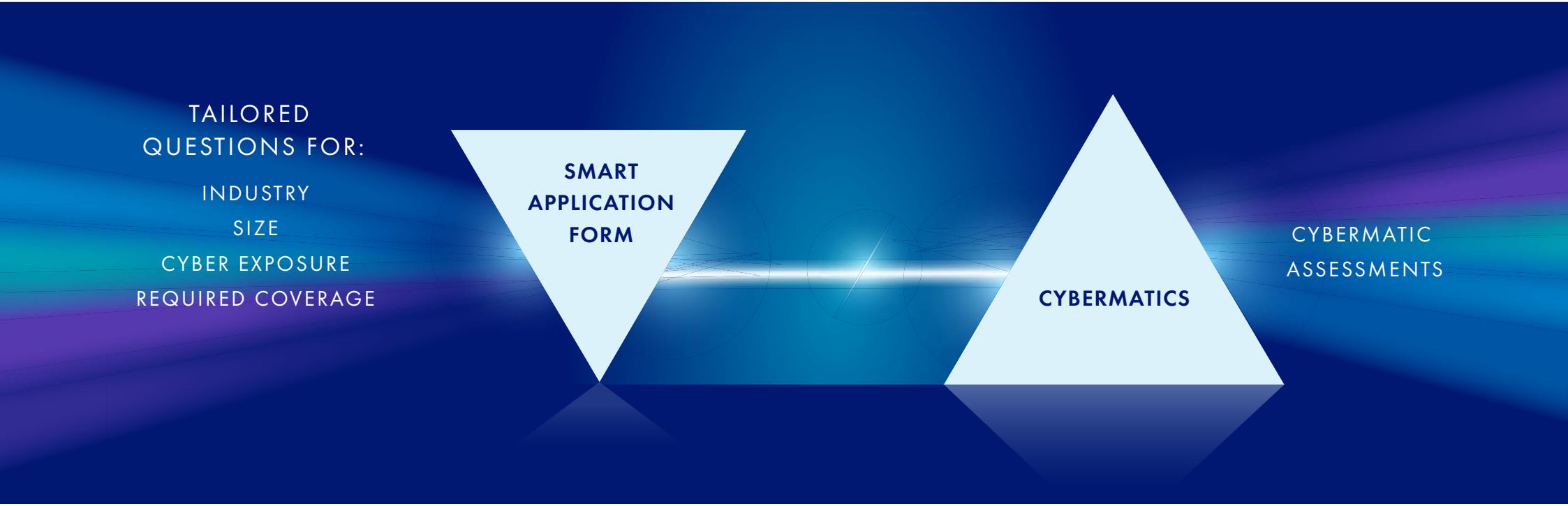


GO BACK

Data via AIG smart application

AIG's dynamic and interactive smart application form allows businesses to respond to tailored questions relevant to their industry, size, cyber exposure and required cyber coverage. The question set adapts itself as it is completed and the business's answers, fed into CyberMatics enables a range of assessments including the likelihood of malicious or accidental cyber actions, the potential impacts on the business and the effectiveness of the business's cyber loss measures.

Executive Summary Report



GO BACK

Data via AIG technology partner

CyberMatics is also supplied with secure data from one of our technology partners working with the business. The selected partner provides regular, verified data responses to our underwriting application questions. Partners will never contradict any of the clients' responses (see "no downside") and data is aggregated before delivery to AIG so we do not receive any of the client's raw data. In this way the client's cyber maturity profile is updated weekly with risk scores, benchmarking, recommendations, and more. Clients can view this continuously updated information on the Dynamic Dashboard.

Cyber Tech Partners

No Downside

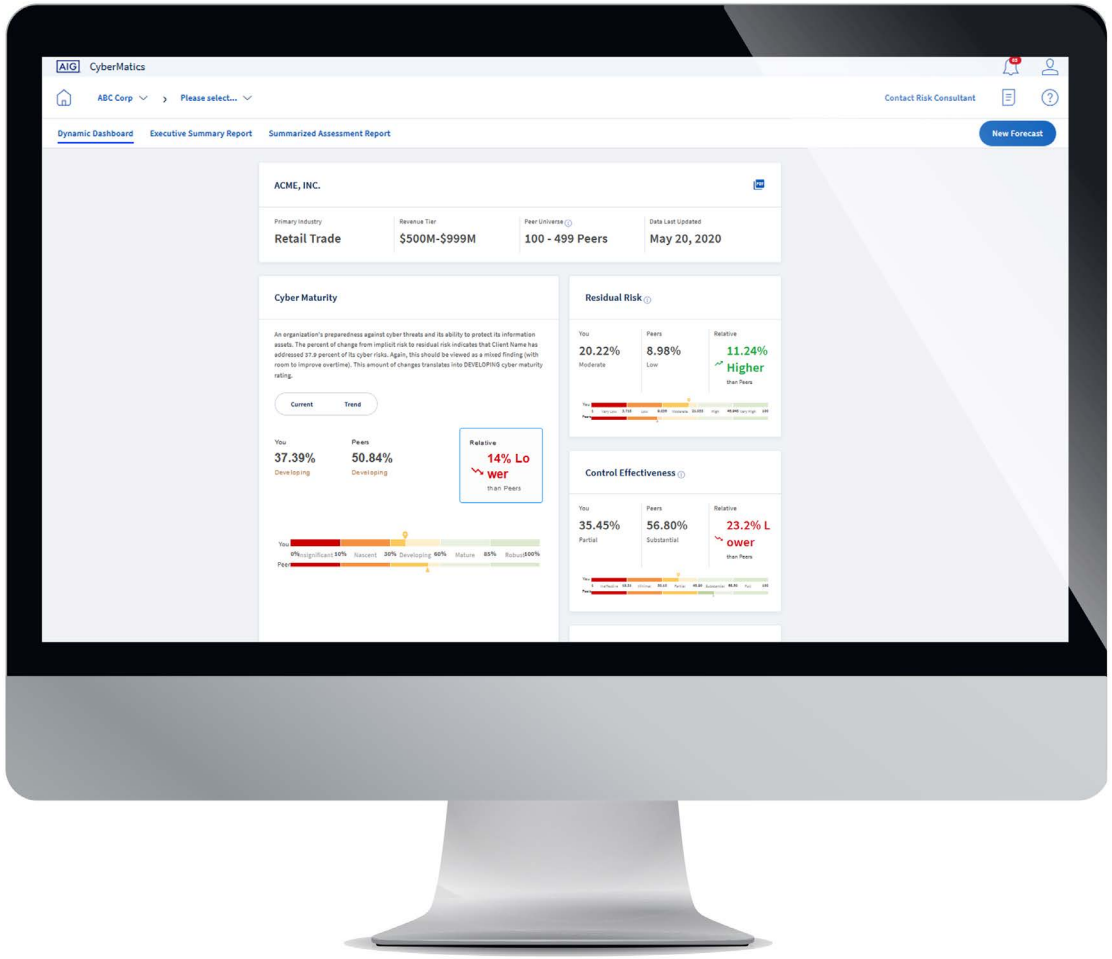
GO BACK

The Dynamic Dashboard

Every CyberMatics client has its own Dynamic Dashboard. This provides comprehensive, updated information about multiple aspects of the business's cyber posture that combine to deliver a holistic view of its overall cyber risk position.

This is underpinned by a wealth of detail around the organisation's cyber risk landscape including, but not limited to:

- CYBER MATURITY
- CONTROL EFFECTIVENESS
- SCENARIOS AND PRACTICES
- BUSINESS IMPACTS
- FORECASTING



GO BACK

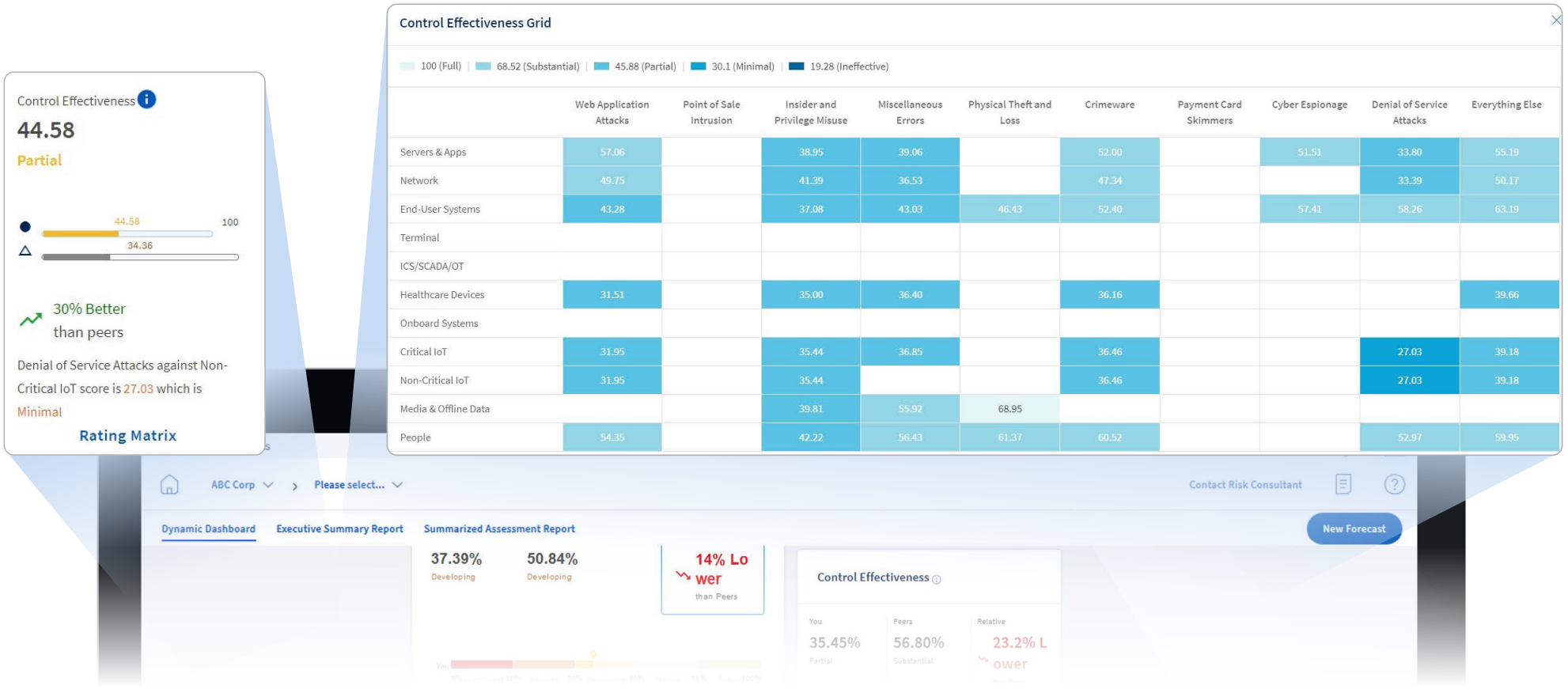
Cyber Maturity

The Cyber Maturity chart displays the organisation's preparedness against cyber threats and its ability to protect its data. (A higher maturity rate implies greater success managing new and unexpected cyber threats). It can be analysed at the most currently available point in time, or as the example below shows, over preceding periods to help reveal performance trends. In both cases the data is benchmarked against the organisation's peer group in terms of industry sector, revenue, and geography.

GO BACK

Control Effectiveness

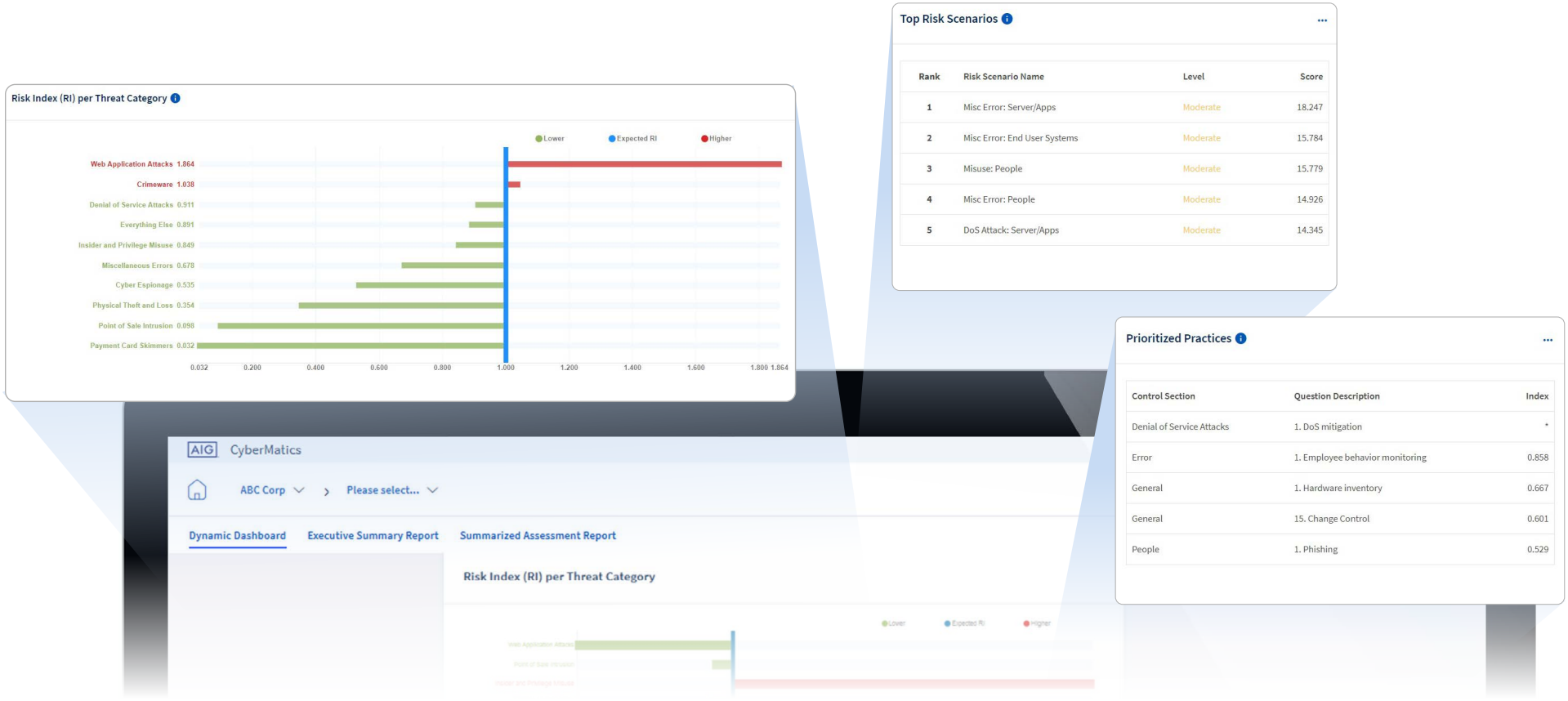
This provides an aggregated score of the effectiveness of the client's cyber risk controls (depending on their suitability for the business's cyber exposures and on the effectiveness of their implementation). The score is benchmarked against similar organisations. For detailed analysis, users can toggle to the underlying rating matrix detailing the relative effectiveness within each control category.



GO BACK

Scenarios and Practices

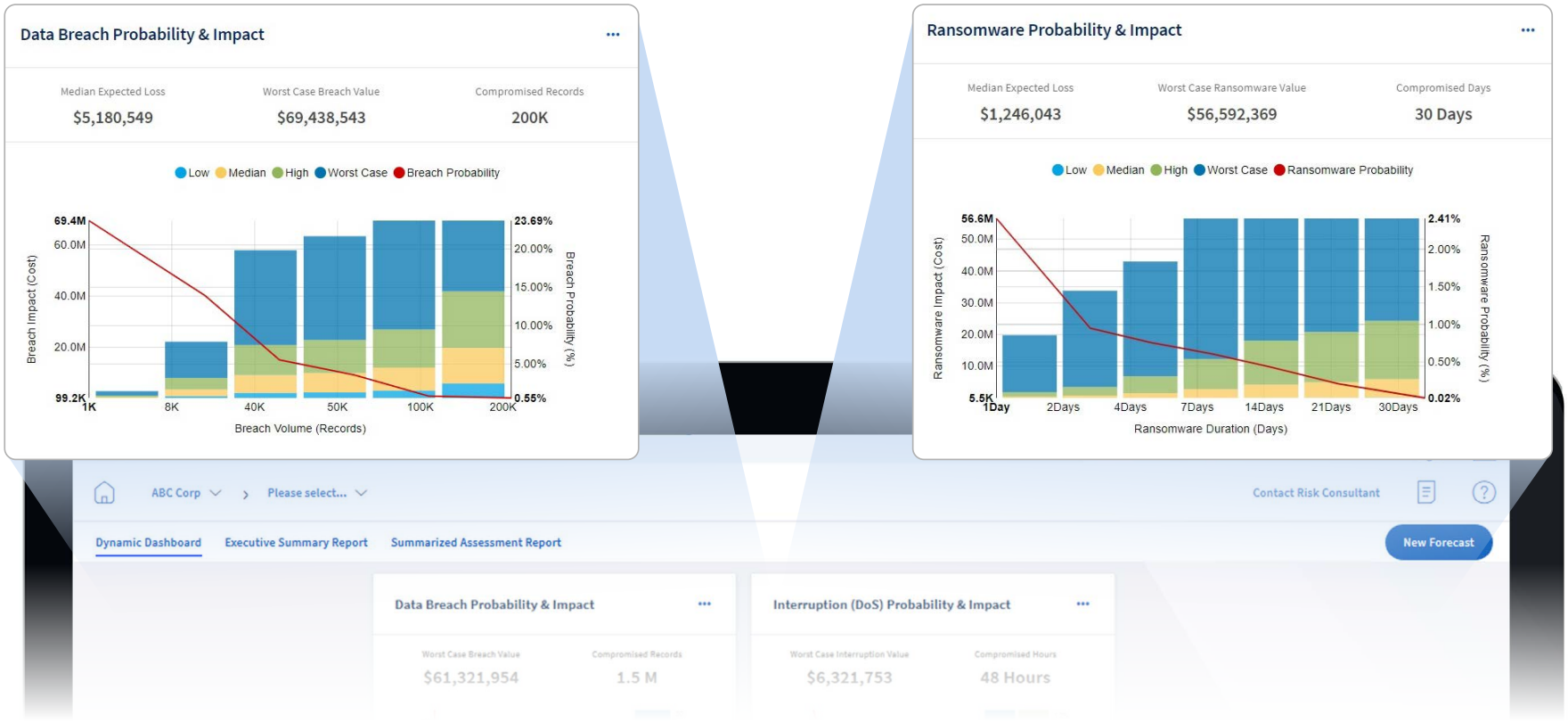
CyberMatics itemises the top risk-reducing practices which the organisation has not implemented and provides a relative rating of the expected risk reduction of implementing each practice. This dynamic perspective updates with the organisation's changing cyber risk landscape, which CyberMatics describes by listing the top risk scenarios facing the organisation and the level of cyber risk presented under each threat category.



GO BACK

Business Impacts

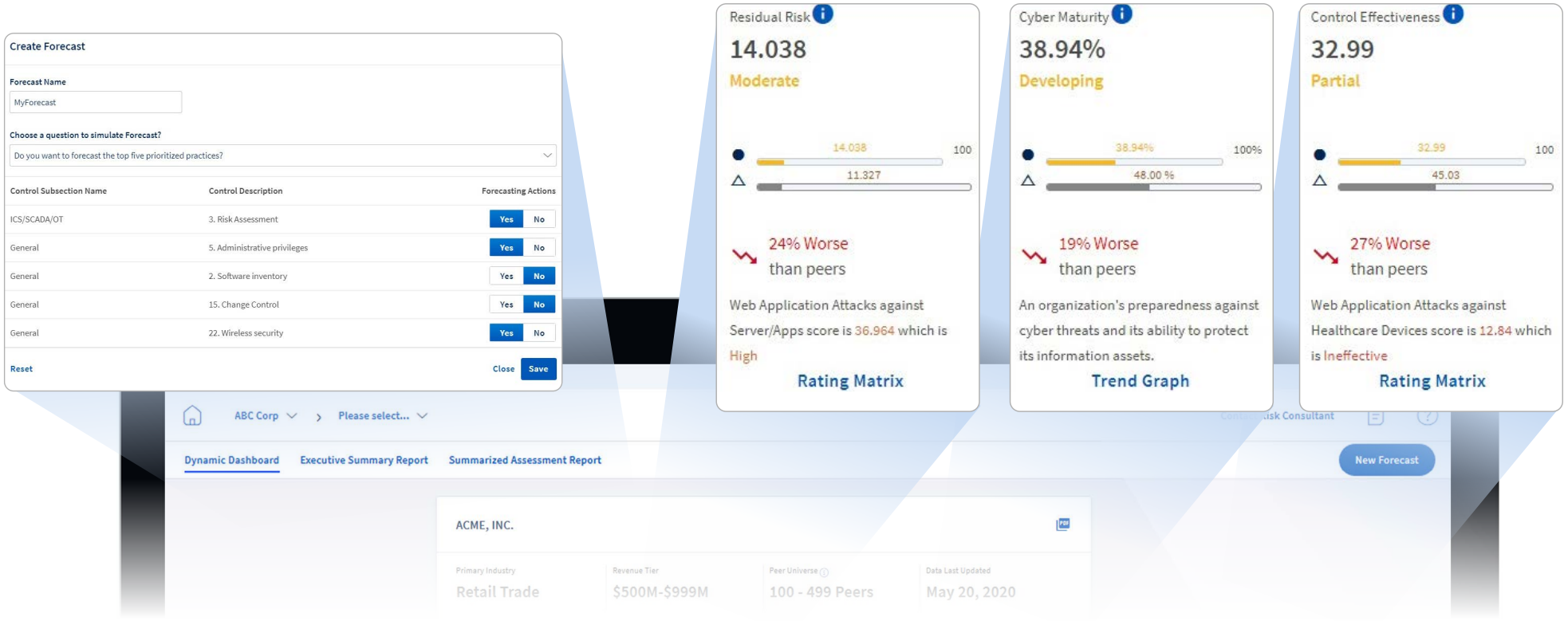
CyberMatics delivers continuously updated assessments of the threat vector and potential impacts facing the business. The organisation's threat likelihood is benchmarked against that of similar organisations, while the probabilities and financial impacts of data breaches and ransomware facilitate low, medium, high and worst case scenario modeling.



GO BACK

Forecasting

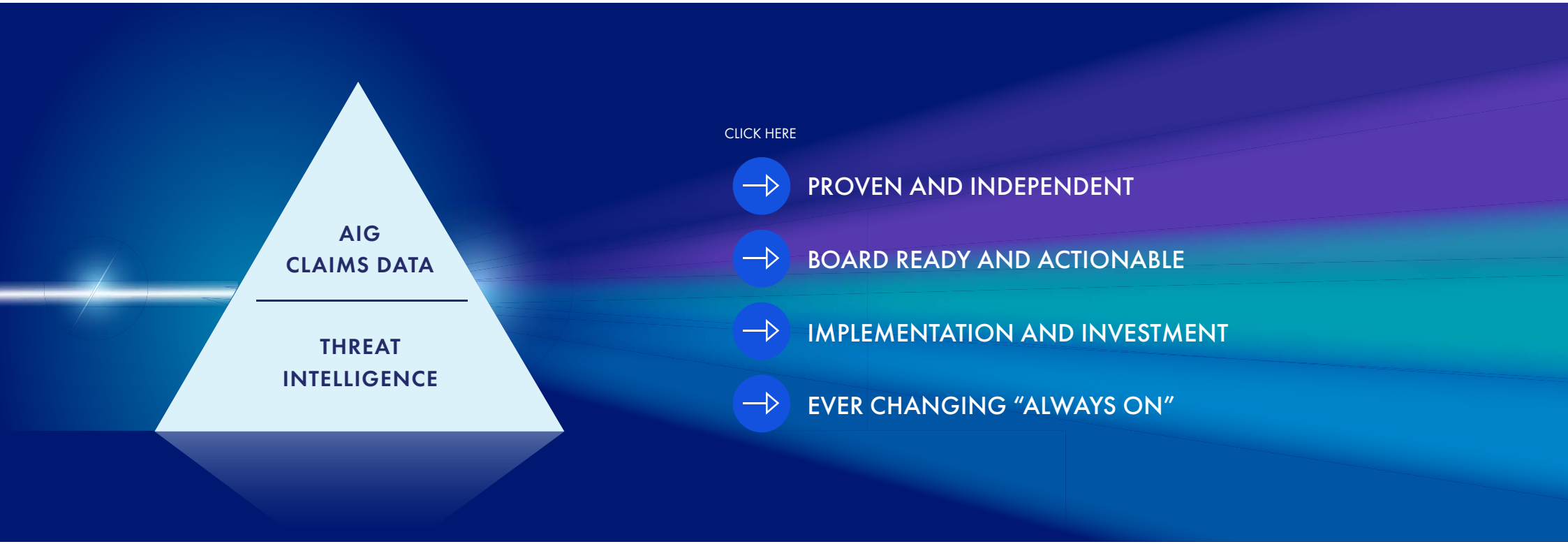
This powerful functionality allows Information Security Officers to select specific cyber controls, or combinations of controls, and forecast the beneficial impacts on the organisation of implementing them. The forecasting tools will reconfigure the organisation's threat likelihood, cyber maturity and control effectiveness as well as the risk scenarios facing the business and the recommended prioritised cyber risk control practices.



GO BACK

Business Benefits

CyberEdge injects measurable understanding into an organisation's cyber risk. Operationally it helps prioritise the implementation of control measures. Strategically it informs investment decisions around its overall cybersecurity program. In these ways it delivers tremendous insights and valuable benefits to, Information Security Officers, Risk managers, Board Directors and the organisation itself.



GO BACK

Proven and Independent

Although Cybermatics is a highly differentiated cyber risk assessment tool, there is nothing experimental about it – it is an established technology that was award-winning in 2018. As a cyber insurer AIG's interests are completely aligned with our clients, we have "skin in the game" and the risk scoring of clients' cyber maturity, control systems and potential business impacts is completely objective, regardless of the systems and software that they have purchased.

We believe that this is a unique service from AIG, no other carrier that we are aware of is prepared to validate and benchmark an organisation's cyber posture in this way. All of this means that each participating organisaton benefits from a proven, independently verifiable, analysis of one of the most volatile risks they face – continuously updated and complimentary to eligible AIG customers.*

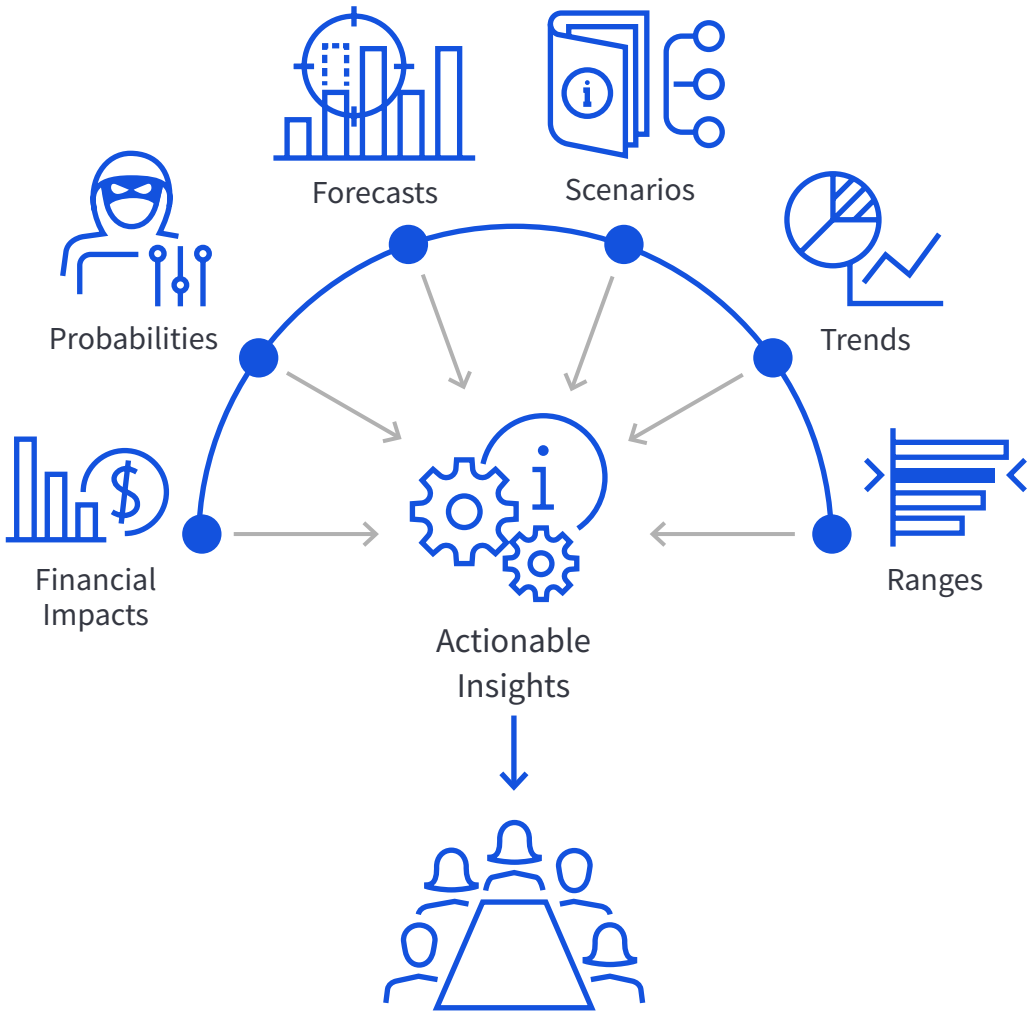
* See **Getting CyberMatics** section for eligibility

GO BACK

Board-Ready

CyberMatics empowers CISOs by equipping them with information in the right language for their board directors. CISO's will already have command of technical and analytical specifics and may typically present in such terms to their boards. (Such as the numbers of patches implemented, the percentages of endpoints protected, the percentage of employees trained etc.)

CyberMatics goes a lot further and presents the technical analysis in practical expedient contexts that board directors boards can access, consider and act upon such as: the probabilities of an attack, the potential financial impacts on the business and benchmarking comparisons with organisations of similar size, sector and markets.



GO BACK

Implementation and Investment

CyberMatics helps organisations evaluate their selection and implementation of cyber risk controls. By feeding back regular risk scores specific to each control, it helps CISOs ascertain whether they have the right controls in place, whether they were implemented correctly and whether they are having the impacts that were anticipated when they were purchased.

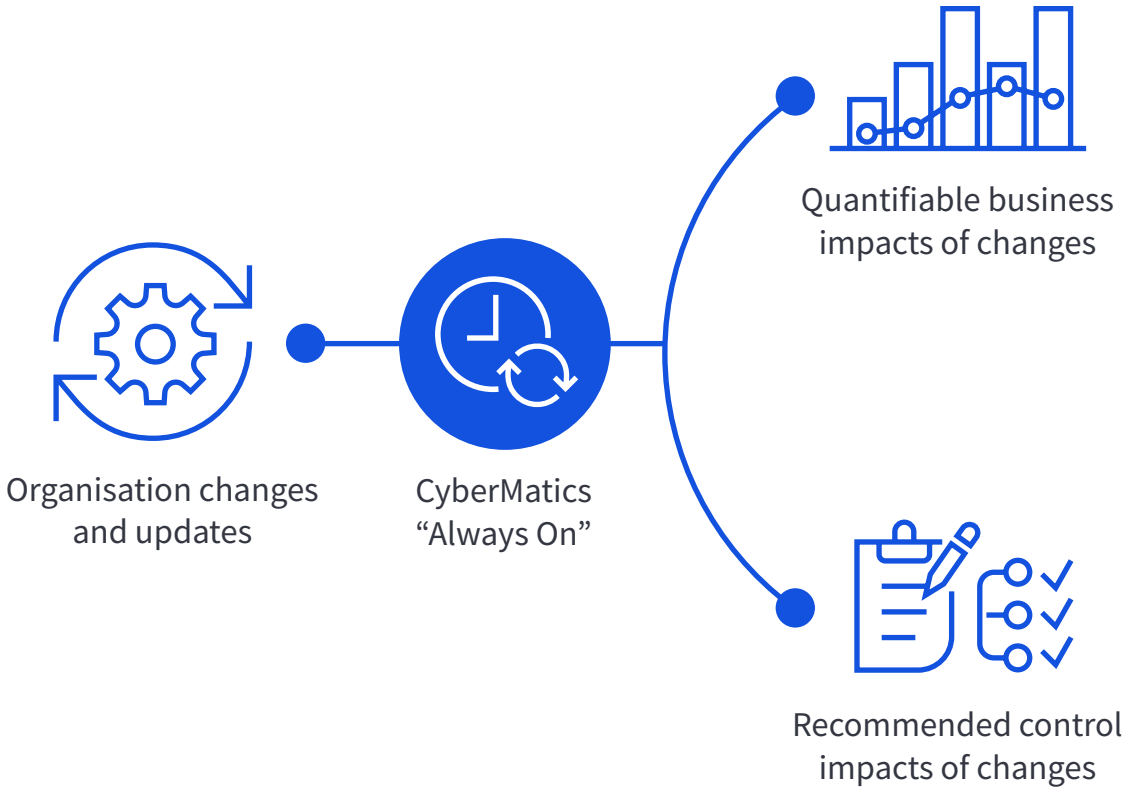
Looking forward, CyberMatics also helps optimise cyber programme investment decisions. Not only does it presents and prioritise control actions for risk improvement based on the organisation's risk profile, but its powerful forecasting functionality can then be deployed to quantify how the organisation's risk position would change in response to these selected control actions.

GO BACK

Ever Changing "Always On"

Cyber risks are dynamic and ever-changing and so, by neccessity, are organisations' system control strategies. Because Cybermatics is continuously updated, it allows businesses to track the impact of any changes to their security protocols during the policy period. For instance by using Cybermatics, an organisation could see the quantifiable impact on its cyber posture of adopting a new procedure (such as data encrption) during the year.

Not only that, as a result of any change in procedures, Cybermatics will also change the recomended security practices for the organisation. This provides valuable insights for Information Security Officers and Risk Managers, by highlighting the most important security aspects and procedures to focus on as their organisation's threat landscape continues to evolve.



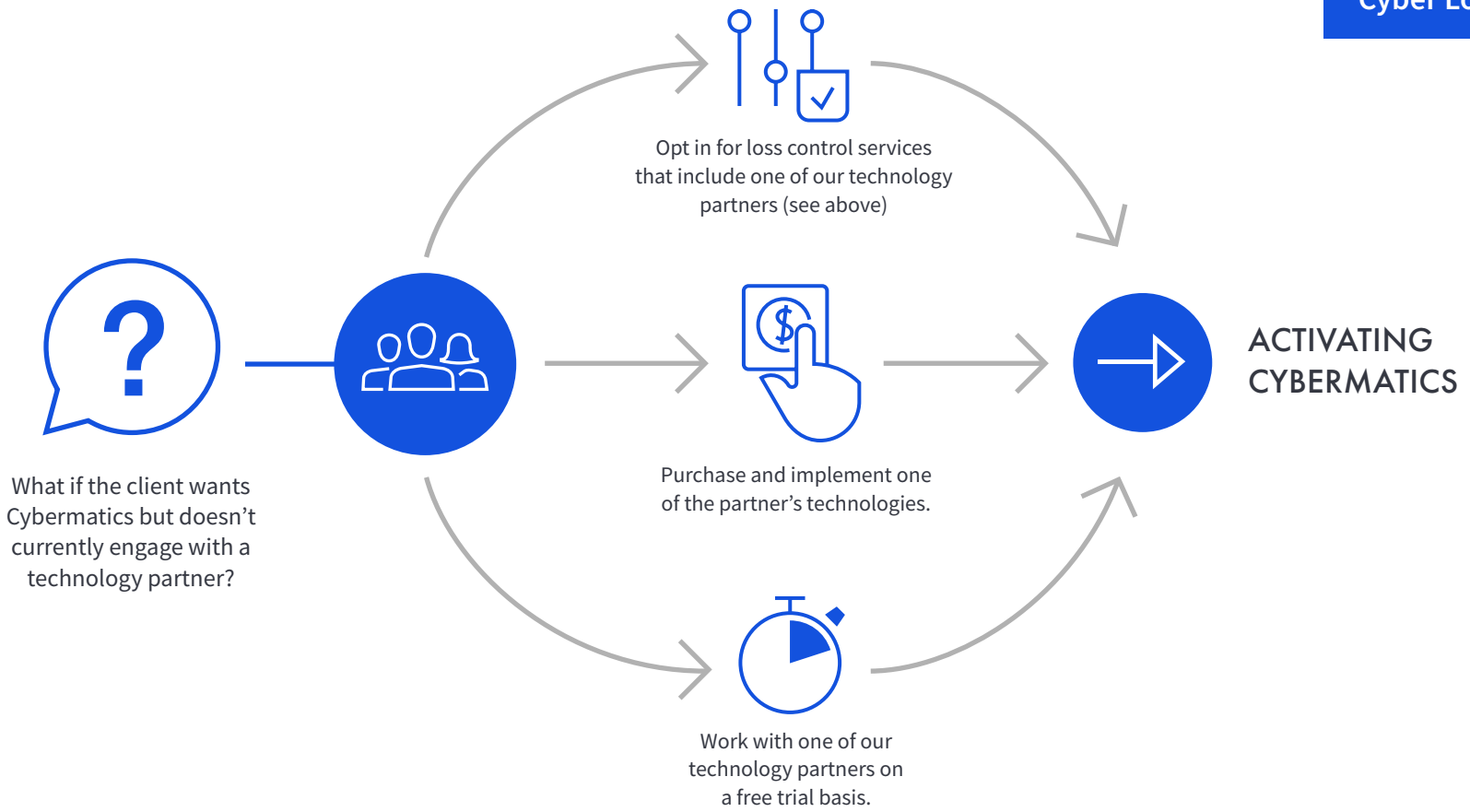
GO BACK

Getting CyberMatics

CyberMatics is available to any AIG CyberEdge policy holder that has engaged one of our technology partners.

Cyber Tech Partners

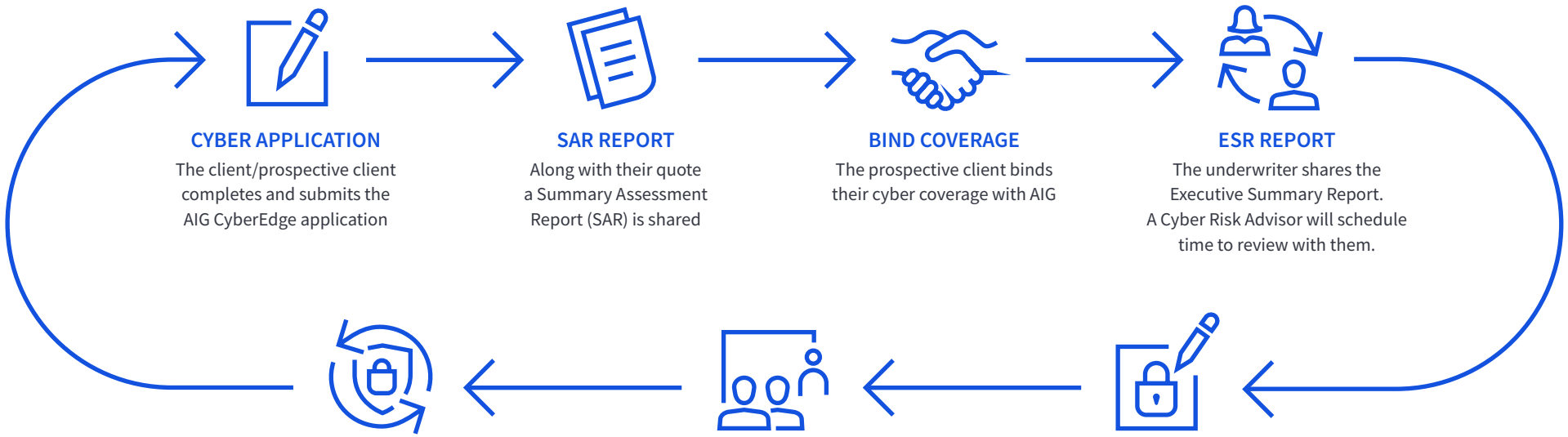
Cyber Loss Control Services



GO BACK

Activating CyberMatics

The **AIG smart application** needs to be completed in order to establish the initial risk model baseline needed for CyberMatics. This triggers the full activation process below:



GO BACK

www.aig.be

GBL00003749 0920