Case study @data*Belt*®

An international digital marketing company was keen to bring together **cyber security, data protection** and **data valuation** as part of its **digital transformation journey –** Aim deployed its data governance solution **data*Belt*®** to meet the challenge

Situation

Following an external audit, an international B2B digital marketing company was tasked with improving its general posture in cyber security and data protection during its digital transformation journey.

The company was also progressing application rationalisation and cloud-first programme, so was keen that any new platform should ideally be a framework solution.

The company was keen to look at alternative cyber security tools to replace its 1st generation on-premise security platform and had been looking at a 2nd or 3rd generation tool with full endpoint protection and detection capability.

Given its industry, data protection compliance was very important, and the company had ensured compliance in terms of GDPR by using a well-known off the shelf GDPR audit tool. However, the Data Protection Officer found that the process of data handling remained manual and time consuming, and she was keen to look at some GDPR 'doing' tools rather than just box ticking audits.

Finally, the CFO had been following the rise of infonomics and how the data they had accumulated could be used to add indirect value to the organisation.

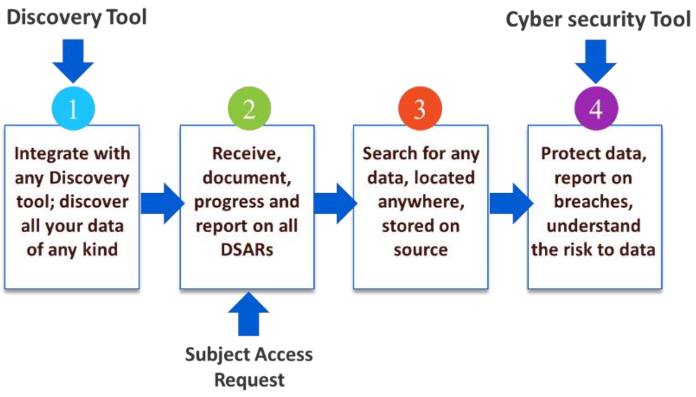
AiM was asked to help.

Solution

AiM demonstrated that the direction of travel for data in digital transformation was towards 'one data', moving to a centralised federation, in which operational barriers were breaking down between disciplines such as cyber security, data protection, risk and compliance. AiM recommended its one platform framework solution data***Belt***® would manage all these challenges.

Data***Belt***® was demonstrated with its cyber security end-point feed, showing how suspicious behaviours and malicious operation attacks (malops) could be countered and eradicated. But it also showed how data***Belt***® was able to map datasets through its data classification tool with vulnerability to suspicious behaviour or malop cyber-attack. This meant that any cyber event could be assessed in terms of true business impact – eg business importance rating, sensitivity and fiscal value. This feed proved very useful for the Security Operations Centre to understand the importance and value of business data and records.

For data protection, data***Belt***® was able to offer its classification and deep search tools that enabled automated data subject access requests (DSARs) searching the dataset index, redaction of data, seeking consent, data protection impact assessments, right to be forgotten - and GRC whereby compliance audits could be made against GDPR and other jurisdictions' data protection legislation.


Discovery Tool
Cyber security Tool
1
Integrate with any Discovery tool; discover all your data of any kind
2
Receive, document, progress and report on all DSARs
3
Search for any data, located anywhere, stored on source
4
Protect data, report on breaches, understand the risk to data
Subject Access Request

The same data auto-valuation capability demonstrated with cyber security was also used to assess the value of data held to allow them to decide what and how to use it better internally and in the market place. It also assisted them with their cloud first strategy – providing invaluable information on the type and use of data, importance, sensitivity, how often it was accessed and the most cost-effective and secure location for storing it.

Results

The data***Belt***® implementation ensured a leap forward in data governance maturity as well as greater efficiencies and reduced risk/liabilities surround its data and operations. The subsequent audit was successful, and an observation was made by the auditor of how the company had embraced new technologies to drive positive digital change.

The data***Belt***® framework solution was cloud deployed – complying with the cloud first strategy - and allowed the company to migrate away from the off the shelf GDPR audit tool – rationalising its software tool base too.

Finally, data valuation enabled the company to understand the value of its data and to allow a programme of how the strategic data could be used to improve internally processes and shared with partners on their supply chain. A future plan is to assess the market value.