PATHFINDER™

Data Protection and Breach Risk Analysis

90% of all data ever created has been created in the last 2 years.

Over 2 billion user records were breached in just 10 major incidents.

Over 90 Class Action lawsuits for data breaches in the US alone in 2016.

Increase in regulatory fines for the breach of European Citizen Data to either €20million or 4% of global turnover.

Mandatory breach notification for all EU Members by May 2018 and already in force in 47 US States.

Increasingly complex global regulatory and legal framework.

New rights for data subjects.

Organisations are required to default to privacy and be able to evidence data protection as a core function within business operations.

INTRODUCING PATHFINDER™

WHAT IS PATHFINDER?

The DPG Pathfinder is a comprehensive risk assessment framework to assess an organisation's ability to meet regulatory data protection requirements and to protect their data throughout all business operations.

Deployed via simple to use software, the Pathfinder interrogates six key business areas including 74 business processes via 1,300 questions. This information capture is the most extensive and valuable assessment of how data, infrastructure and relationships are managed to ensure they meet data protection requirements and help decrease the likelihood of a data breach.

DEVELOPMENT OF PATHFINDER

Evolved over a three years' period, the Pathfinder analysis includes and exceeds recognised standards such as ISO 27001, PCI DSS, Cyber Essentials and more. Developed by security practitioners, leading academics and data protection experts, the Pathfinder delivers superior business intelligence to improve process management, enterprise risk management, and internal operational controls.

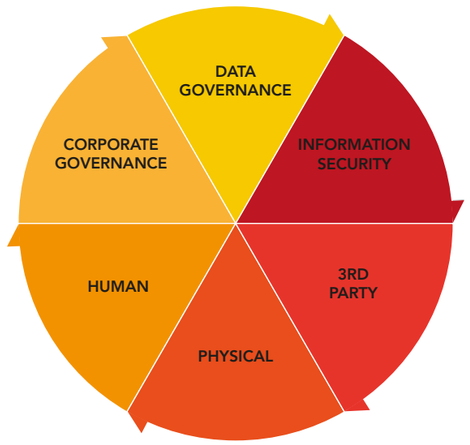
WHO IS PATHFINDER FOR?

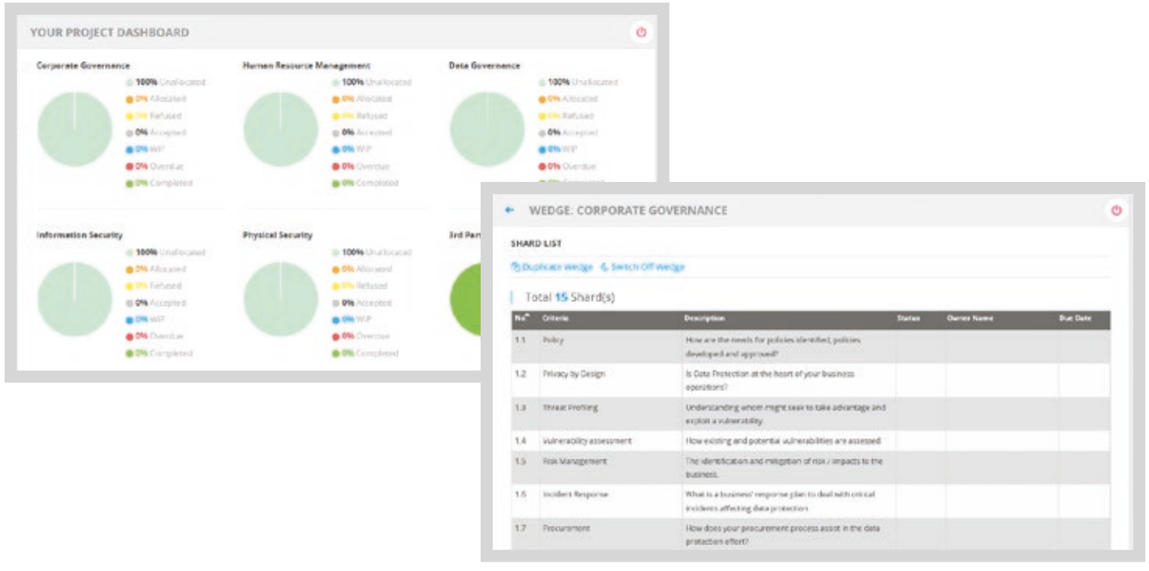
- Any organisation that wants to quickly understand their exposure to data breach risk.
- Any organisation that has not performed a thorough data breach risk assessment and would like to understand and prioritise the risks faced.
- Any organisation that wishes to reduce its financial exposure to increased regulatory action and litigation.
- Any organisation that wants to understand the return on investment of a specific remedial action.
- Any organisation that is governed by increased compliance necessities and stakeholder scrutiny.

HOW DOES IT WORK? INFORMATION CAPTURE

Before you embark on the project of improving your data protection position you must first analyse your current business operations in order to understand where to prioritise focus and spend.

The Pathfinder's six key business areas include all processes which directly impact or influence data protection. In order to capture your business's performance in these areas, the Pathfinder Software is deployed to identified personnel or partners who are required to answer a series of questions on their specific activity. This approach ensures that the business intelligence is received directly from those people who perform key tasks. This helps analyse day-to-day decision-making and business activities which in turn can impact on data protection. Each question is afforded a status which is unseen by the user. This allows a hierarchy of responses to be created and permits the prioritisation of technical or operational vulnerabilities or regulatory / legal non-compliance which persist within your business.





HOW DOES IT WORK? IDENTIFICATION OF CRITICAL ISSUES

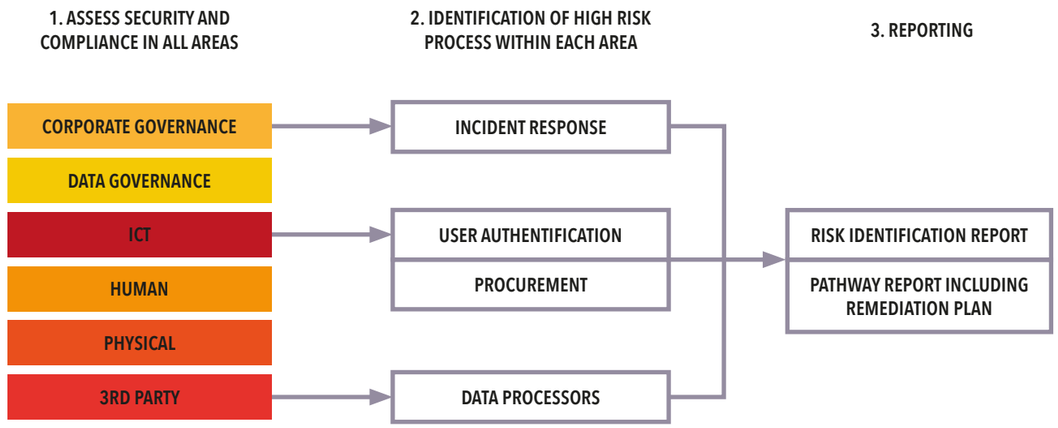
The Pathfinder Software uses the status of each question to provide dashboard reports which show where there are critical, elevated and standard issues within the business. There are two types of report; the Risk Identification Report which is system generated and becomes available immediately on the completion of the project and the full Pathway Report which includes an analysis of unique business influences and proposed corrective actions required.

CRITICAL QUESTION: A "no" answer leaves a vulnerability which requires minor capability to exploit OR is a major organisational failure / potential legal non-compliance.

ELEVATED QUESTION: A "no" answer leaves a vulnerability which requires moderate capability to exploit OR is a minor organisational failure / regulatory non-compliance.

STANDARD QUESTION: A "no" answer leaves a vulnerability which would require significant capability to exploit. OR an operational weakness which on its own may not be a direct security weakness but when used in conjunction with other factors could be viewed as a catalyst for the creation of a vulnerability which could be exploited.

HOW DOES IT WORK? ASSESS, IDENTIFY AND REPORT



PATHFINDER™

BENEFITS OF PATHFINDER

- Capture of business intelligence on all processes, identification of key process owners, and analysis on current operational performance which can impact on data protection.
- Identification of technical and operational vulnerabilities which can be exploited.
- Helping to build a framework which will show clear and measurable improvements.
- Overlaying data protection regulation with business performance.
- Encouraging and managing transformational change.
- Controlling risk and building corporate resilience within data protection.
- Assessing impact of third party relationships on the overall data protection position.
- Providing metrics to improve decision making, spending and resource allocation.
- Identifying requirements for training and services from within.
- Extending the scope of data protection away from Information Technology and into the heart of business operations.

FIND OUT MORE

+44 207 998 3531
info@dpgovernance.com
dpgovernance.com