SoluxR
ENHANCING STRATEGY EXECUTION

Cyber Risk Assurance

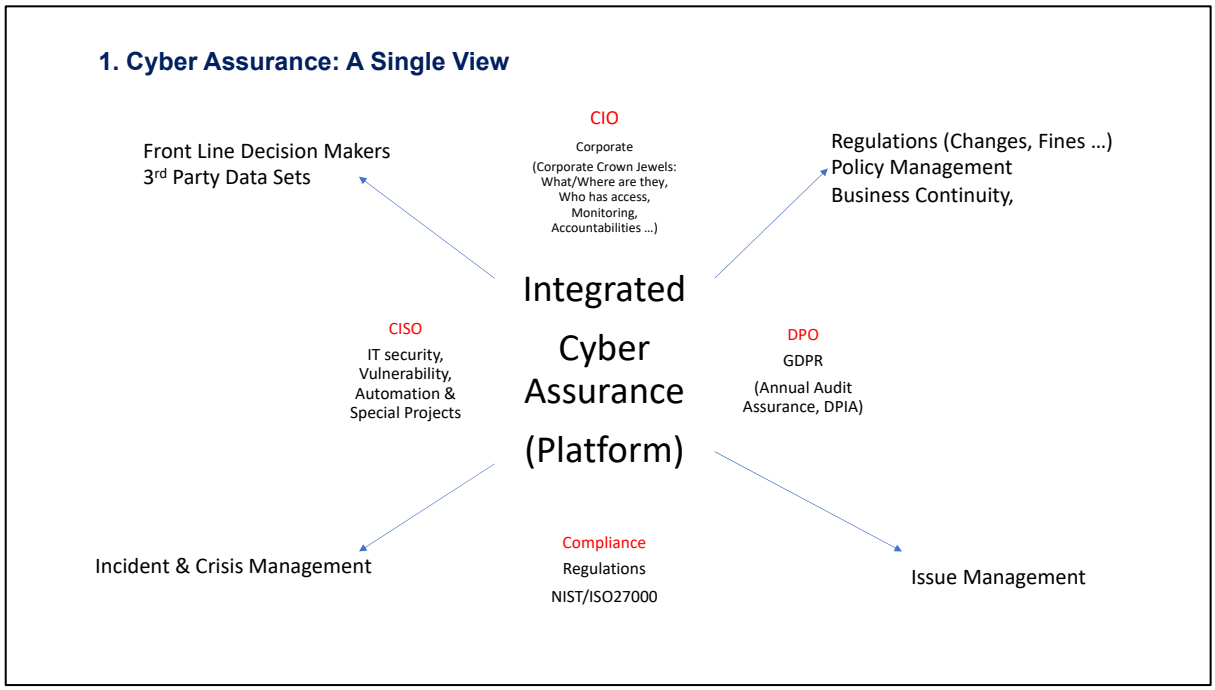
Cyber breaches (personal data, business secrets etc.) are increasing in frequency and scale and so will remain a major concern for boards and their management teams for the foreseeable future.

Cyber assurance however is typically distributed and siloed across functions and organisational structures. Other than at a policy level, cyber assurance is typically not joined up in any consistently structured way and is almost never joined up at a systems/platform level. For this reason cyber assurance is more of a challenge for management teams reporting to boards than it is a challenge for IT departments working to individual operational and compliance requirements.

The Venn below illustrates what good cyber assurance looks like. On the other hand if you remove the centre circle and replace it with high level policy statements, and perhaps a conceptual governance framework, you get a representation of what actual cyber assurance looks like in very many organisations today.

Registered address: Windsor House, Windsor Terrace,
Dun Laoghaire, Co Dublin, A96 A065,
Ireland

Email: Info@soluxr.com



The distributed nature of cyber assurance is compounded further as:

1. Different functions and different departments have different taxonomies and measure risk differently. This can result in sub-optimal, and sometimes deeply flawed, cyber risk reporting up to boards.

2. Front-line decision makers (1st line of defence[1]) see cyber risk as somebody else's problem. They have no easy to use effective way of identifying and measuring cyber risk within their areas of responsibility. They can do little other than be responsive to periodic or event lead IT security, risk and compliance (2nd line of defence) engagements. As a result the 'soft underbelly' of cyber risk, PEOPLE, remains vulnerable to social engineering and a multiplicity of increasingly innovative cyber-crime tactics,

3. Different systems, with limited to no interoperability, are procured to meet different functional requirements with low-no ability to present an organisation wide aggregated view and understanding of cyber risks across the enterprise,

The Challenge:

The distributed nature of cyber assurance summarised above results in:

- Poor cyber risk management capabilities
- Poor organisational agility to respond to many cyber related crises
- Poor business continuity and contingency planning
- Poor resilience within the deeply interconnected and independent ecosystems resulting in systems failures across critical activities

[1] Note IIA Three Lines of Defence https://tinyurl.com/n5tgazt

Organisations need to find a way to align disparate systems in a way which results in the receipt of 'always-on' reliable, relevant actionable information to provide effective cyber risk assurance,

Choices include:
Combining publicly available data and internal systems[2] analytics algorithms to seek to illuminate possible vulnerabilities facing organisations over a period of time; or crowdsourcing trusted front line information infused with third party data sources for more immediate results.

Using ***Agile Risk Management (ARM)*** practices SoluxR delivers results at scale, in less time, at less cost, more effectively and more reliably than other methods.

Immediate results begin to emerge when practical issues are concretely addressed against an internationally proven and accepted technique assessing emerging risks, for example using:

World Economic Forum (WEF) Cyber Resilience Framework[3] comprised of 200 questions (including inferred questions from ISO 27000) against 10 (WEF) Principles:

Principle 1 *Responsibility for cyber resilience.* The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2 *Command of the subject.* Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3 *Accountable officer.* The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4 *Integration of cyber resilience.* The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5 Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The Board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6 *Risk assessment and reporting.* The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

[2] Note Venn diagram
[3] https://tinyurl.com/j65huzo

Principle 7 *Resilience plans.* The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8 *Community.* The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9 *Review.* The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10 *Effectiveness.* The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Integrated with:

1. **SWOT** analysis: Organisational Str**engths, Weaknesses, Opportunities and Threats,**
2. **Importance to economic integrity**

Powerful insights from such automated integrated assessments conducted across large numbers of front line decision makers have a hugely positive on the quality of thinking and decision making.

Steps

Dynamic links are distributed across the organisation to:

3. Initially map and scope application of the 10 WEF-ISO2700 principles, SWOT and economic impacts. The more links that are shared across senior decision makers the more automated assessments are undertaken and the more complete the 360 review,
4. Thereafter undertake deep business impact analysis leading to enhanced scenario development and stress testing,
5. Leading to enterprise wide cadenced assessments, across the senior echelons of the organisation such that it can competently assess the efficacy of its risk and resilience posture.

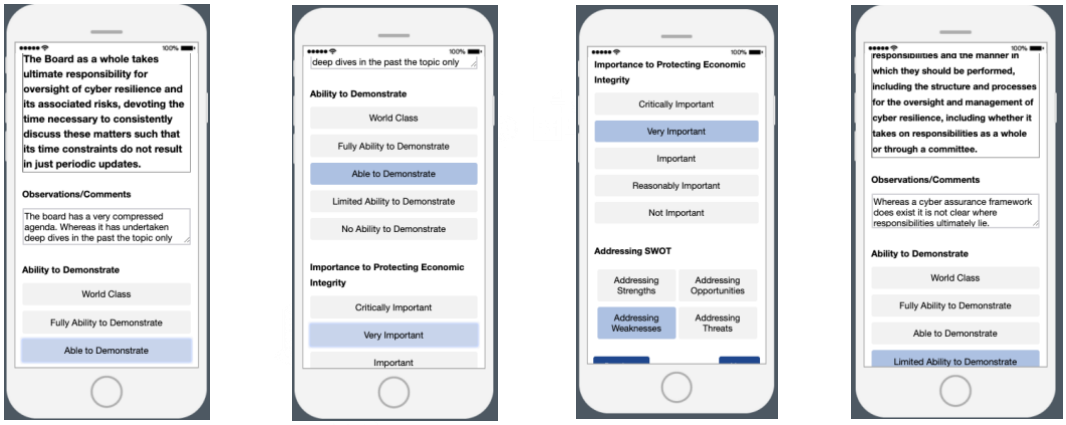
Useful Approaches

1. **Point Solutions for small numbers of people:** You know and understand your issues. They are complicated but you have a plan. You know what WEF Cyber Resilience questions to ask and the people who can answer them. You just want information fast so you can make a concrete decision now. Examples include Board/Risk/Audit cyber assurance query which requires attention now.

2. **Extended Solutions for an unlimited number of people:** Issues are arising and they are complex. There is little or no precedent so the right path is not always clear. You need different people, from different departments and different countries/locations to pool knowledge and experience to help arrive at the right decisions for management consideration. Examples include a range of Board/C-suite cyber assurance queries arising from breaches reported in the press, own near misses or internal concerns which have been raised

3. **Enterprise Solutions:** Yours is a complex and distributed organisation. You are spread across countries and operate in a highly competitive industry sector. You are agile and data driven. You want a consistently reliable way of solving complex and complicated problems. You need scenario driven insights underpinned by evidence based, actionable information to provide sufficient certainty that business objectives can be achieved. Examples include multiple combinations of the above delivered in a seamless and structured way.

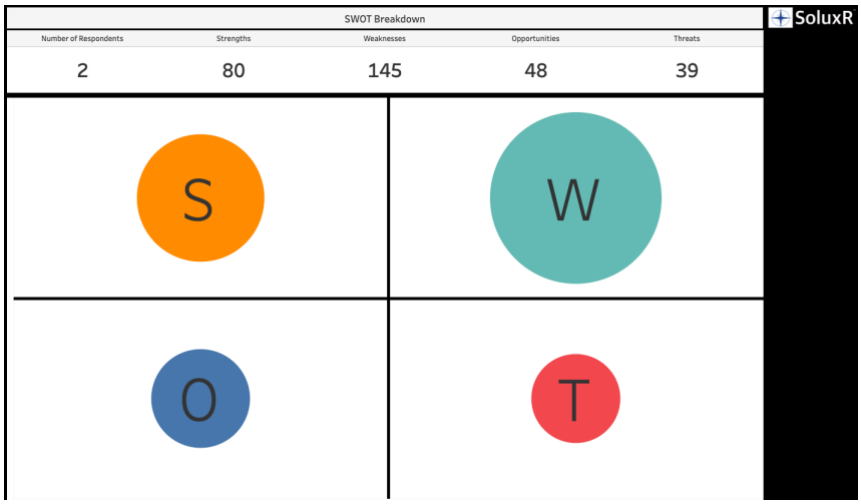
Cyber Risk Assessments (Mobile Screen Captures)



1 2 3 4

 12

SWOT: Overall Position

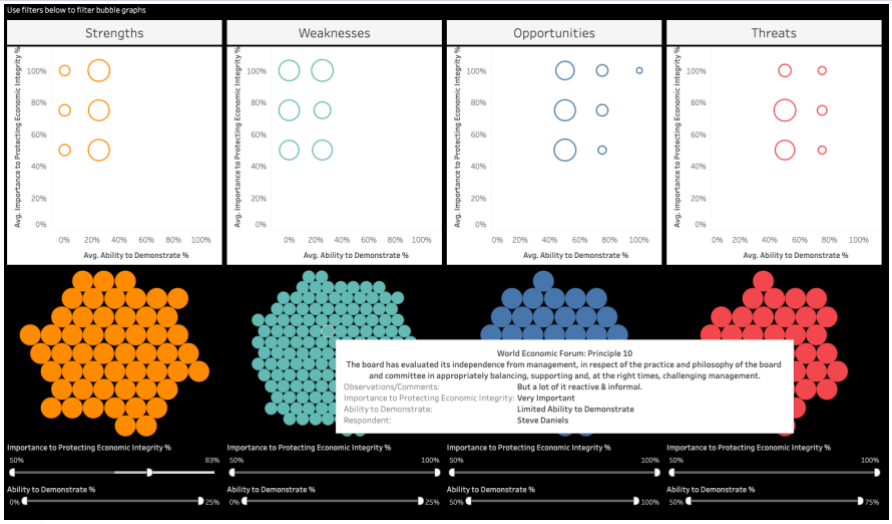


 13

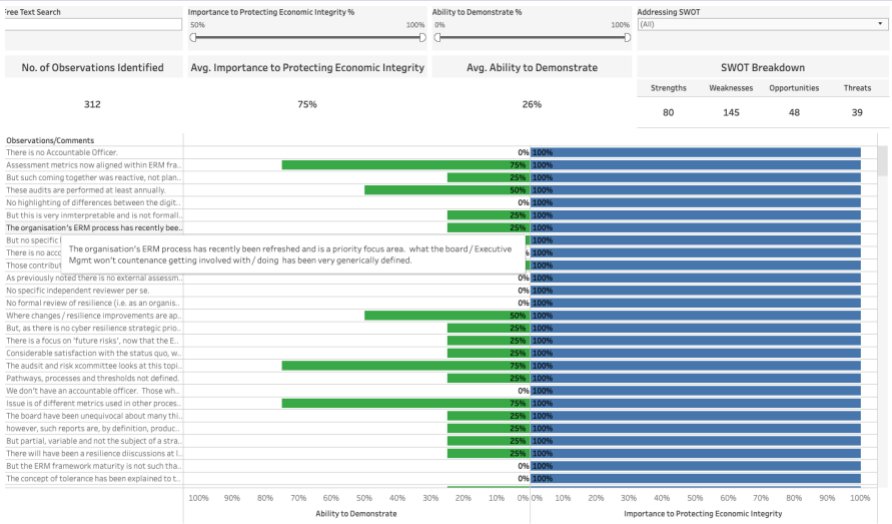
Registered address: Windsor House, Windsor Terrace,
Dun Laoghaire, Co Dublin, A96 A065,
Ireland

Email: Info@soluxr.com

SWOT Settings – Risk Appetites



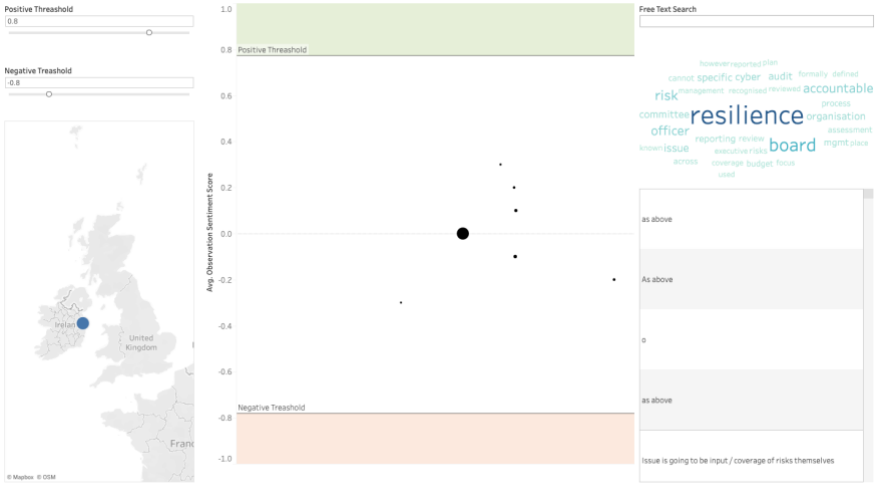
Ability to Demonstrate Impacts



Registered address: Windsor House, Windsor Terrace,
Dun Laoghaire, Co Dublin, A96 A065,
Ireland

Email: Info@soluxr.com

Sentiment Analysis



Sentiment analysis should only be used as an additional tool which can occasionaly add value in larger data sets. Soluxr reccomends setting the positive threashold at 0.8 and to only consider points above this as 'positive' and to set the negative threashold at -0.8 and to only consider points below this as 'negative'. This sentiment analysis tool may be inaccurate especially for values with a sentiment score of between -0.8 and 0.8.

Cyber Risk Register

Issue	Type of Issue	Importance to Protecting Economic Integrity	Ability to Demonstrate	Treatment	
There is no Accountable Officer.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
No highlighting of differences between the digital systems that are involved in the operational aspects of the business as opposed to the classical IT systems that are used for support functions. This analysis not performed.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
There is no accountable officer as such	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
As previously noted there is no external assessment done of th organisation's resilience maturity, nor are there resources internally to do such a thing.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
No specific independent reviewer per se.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
No formal review of resilience (i.e. as an organisational whole) undertaken so plans for what it recommends cannot be approved.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
We don't have an accountable officer. Those who today contribute to resilience delivery in our organisation get their 'resources' from their core teams working in the margins.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination & Selection/"Red Team Review" Required/TBD	25
But the ERM framework maturity is not such that it can specify tolerance or appetite.	Addressing Weaknesses	5	5	More Detailed Brexit Impact Assessment Required/Contingency Planning Assessment Required/Ready for Strategy Determination &	25

Ability to Demonstrate
Importance to Protecting Economic Integrity
Section Name
Addressing SWOT
Business Unit
Respondent

Registered address: Windsor House, Windsor Terrace,
Dun Laoghaire, Co Dublin, A96 A065,
Ireland

Email: Info@soluxr.com

What do you get from SoluxR?

1. Robust scenario analysis and modelling impacts, risks and mitigations
2. Early foresight and insight of issues and opportunities before they develop
3. Significantly lower cost, faster and better analysis and planning
4. A single comprehensive view of what's actually going on across organisations and wider ecosystem
5. Ability to understand, anticipate, respond, recover and quickly adapt as further cyclical pandemics occur
6. Rapidly assess the impact and effectiveness of urgent remediations
7. Detect systemic issues across the organisation.
8. Dynamically fulfil regulatory & compliance obligations/requirements

Why use SoluxR?

1. Secure, fully mobile optimised, easy to use and manageable
2. Very fast deployment
3. Greatly reduced costs
4. No interruption to business-as-usual
5. More reliable information
6. Seamless infusion with other data sets

SoluxR Return on Investment:

1. Ability to maintain effective and efficient battle readiness for emerging cyber risk events, issues, opportunities, challenges and scenarios,
2. Sustainability of organisational resilience by aligning and shifting organisational decision making from top-down hierarchical to the front line distributing fast, data driven, scenario based pathways to long-term viability,
3. Increased buy-in of people up and down the decision chain of command with continuous feedback, testing, failing and learning during execution.

Method of Delivery

SoluxR automated solutions are delivered on a Risk as a Service (RaaS) subscription basis

Request a Demo