TALION

Cyber Risk Assessment

Understanding your cyber risk is the cornerstone of any cyber security programme.

TALION.NET

e. hello@talion.net

t. +44 (0) 800 048 5775

Cyber Risk Assessment

Challenge

In this rapidly changing, interconnected world it is increasingly difficult for a business to understand the risks they are exposed to from cyber. The digital age has made data, IT credentials and intellectual property almost a currency in their own right, where the exchange rate is very good for the seller holding the keys, even where that ownership is through illegal means. Growing trends in external cyber-attacks, business interruption, ransomware incidents, regulatory exposure and even nation state-sponsored attacks make understanding your exposure to cyber ever-more important. Yet for many organisations, the question often asked is where do I start, and how do I make sense of the findings, with real actions that will improve my position.

Solution

Our Cyber Risk Assessment (CRA) helps organisations to make better decisions about their cyber security programmes and practices. CRA helps organisations with:

- Prioritisation and alignment of security resources to business objectives
- Informing a business case or security improvement programme
- Demonstrating security return on investment (ROI)

Organisations must carefully and diligently assess the cyber risks posed to its technology, systems and data assets; this assessment should be as stringent as any other business risk it may face. Organisations must also assess their obligations to comply with regulatory and compliance requirements.

We use our experienced and independently certified cyber security practitioners, to help analyse and evaluate your cyber risk. We use open, and recognised guidelines and standards so our results are portable and comparable.

The CRA helps measure an organisation's cyber risk by performing a series of consultative exercises including:

Risk Tolerance

We will conduct focussed interviews with C-level, board, audit and risk leaders to clearly establish what the organisation's cyber risk tolerance is.

To quantify risk the Risk Tolerance exercise will express the risk level or limit under which risk should be managed. For example, "as a business we are comfortable with a 10% probability of a £100k loss."

This method of risk assessment allows the organisation to quantify the risk and once quantified the risk can be managed.

Risk Identification

Our consultants contribute to and use an open-source project called the Open Information Security Risk Universe. This project allows our consultants to ensure that we consider a full spectrum of risks and the events that they may lead to and have consequences for your organisation.

We will identify risk scenarios relevant to your business and communicate these scenarios in business-terms; we avoid the use of technical terms and vulnerabilities so that our findings can be understood at all levels of the organisation. By doing this you benefit from a structured approach to risk identification, that aligns and explains the context of the risk.

Risk Analysis

Working with key teams and individuals within your business, we understand the drivers for primary and secondary risks and possible outcomes should these risks become reality.

We use historical and current information as well as forecasted expectations to inform our risk analysis work. Previous incidents can be used to help to calibrate our work. We also draw on open source intelligence to refine estimates and assumptions.

Using mathematical models and Monte Carlo simulations we will quantify our risk scenarios:

> There is a X% probability of event occurring that results in consequences greater than £Y.

We will record and track the outcomes of risks around:

- Expected losses (things that are known to happen, e.g. "we lose data stored on a laptop every three months")
- Unexpected losses

Our Risk Analysis helps:

- Identify where efforts to improve operational efficiency should be focussed
- Financial planning
- Risk management and transfer

Risk Evaluation

We evaluate the risk assessment against your risk tolerance and criteria set at the beginning of the engagement. This finds areas where the business may have unacceptable exposure to cyber risk. The evaluation may result in:

- No further action being taken
- Further work to consider risk treatment options
- Additional risk analysis to refine and better understand the scenario
- Maintaining existing controls
- Reconsider the business objectives

Continual Improvement (optional)

We work with C-level staff and NEDs — over longer periods of time to deliver real and measurable outcomes and improvements, rather than one-off deliverables.

As well as one-off point in time engagements our consultants can deliver recurring assessments on a quarterly, bi-annual or annual basis. The team can also offer training and guidance for your security staff and projects.

Cyber Risk Assessment

Deliverables

A Cyber Risk Assessment delivers a report that includes:

- Details on your risk tolerance in clear, defined terms
- Summary of the risk tolerance workshop with board/audit committee
- Risk scenario identification
- Analysis of the risk posed by those scenarios
- Evaluation of results, relative to your risk tolerance
- Summary of recommendations to help reduce the frequency and magnitude of the losses you face from your cyber risk.

Our Cyber Risk Assessment enables an understanding of your risk at multiple levels:

For business leaders:

- Understand how to meet and demonstrate you are meeting your legal, regulatory, and contractual requirement.
- Through quantification we can provide comparisons with other enterprise risks such as financial, operational and compliance risk.
- Identify areas where risk reduction and operational efficiency gains may be found.

For security leaders:

- An objective understanding of the cyber risk faced by your organisation.
- Confidence that resources are being prioritised in the right areas.
- Identification of new risk areas and gaps in security that may need mitigation.
- Business case support for new and improvement security programmes.

For colleagues:

- A shared understanding of the organisation's cyber risk.
- Improved communication between business and technical teams.
- Better decision making.

About Talion

At Talion, we're changing the way organisations interact with their Managed Security Service Provider. Born out of BAE Systems, our service is built on first-hand knowledge of military engineering and defence-grade security, together with an in-depth understanding of the threat landscape facing the commercial world today.

When it comes to cyber security, we believe every organisation deserves full visibility and complete control over how threats are monitored, how decisions are made, and how their business is protected. That's why we prioritise transparency and collaboration across our service lines, implementing security programs that give businesses the control and freedom to pursue ambitions and realise goals, safe in the knowledge that we've got their back, 24 hours a day, 7 days a week.

HQ
The Hub, Fowler Avenue
Farnborough GU14 7JF

Security Operations Centre
Marshall's Mill
Marshall Street
Leeds LS11 9YJ

Engineering Centre
Unit 32-01, Level 32
The Vertical Corporate Office
Tower B, Avenue 10
Bangsar South, No 8
Jalan Kerinchi, 59200
Kuala Lumpur, Malaysia