INFORMATION RISK
BUILDING BLOCKS

Our information risk framework provides the foundation upon which we architect the strategy to support business objectives and the subsequent information risk programme. The modular nature of the framework furthermore provides an agile environment to allow the organisation to continuously re-evaluate their priorities and approach as the business and threat landscape evolves.

WOLFPACK INFORMATION RISK:

INFORMATION AND CYBER SECURITY | PRIVACY | BUSINESS RESILIENCE

Information Risk Strategy and Framework

The purpose of an information risk strategy and framework is to determine how to recognise, manage and decrease the impact of information and cyber risks effectively, and in a repeatable manner.

This will be tailored to the industry, size, intricacy, risk profile, and culture of the organisation and informed by the constantly changing cyber threat and vulnerability landscape.

Governance and Compliance

Effective governance structures reinforce accountability by defining clear responsibilities and lines of reporting and escalation.

Cyber security compliance requirements need to be identified and addressed to prevent reputational harm or financial penalties incurred should an incident occur. Oversight departments should establish the cyber risk tolerance for the organisation and oversee the design, implementation, and effectiveness of related information risk programmes.

Risk and Control Assessment

As part of the enterprise risk management capability, the organisation should evaluate the inherent risk presented by people, processes, technology, and underlying data that supports each identified business unit, activity and service.

All functions should then identify and assess the existence and overall effectiveness of controls to protect against the cyber risks identified and determine an acceptable residual risk.

Continuous Learning and Awareness

Information protection needs to be implemented across our people, process and technology domains.

A clear majority of breaches are due to human involvement, either malicious or accidental and not due to a lack of technology protection and controls.

Business culture plays a significant role in setting the standards for behaviour throughout an organisation, starting at the top with all levels of management and with each employee or third party involved in the organisation.

Information Sharing and Collaboration

No single company or government organisation can effectively withstand the rapid increase of cyber threats; collaboration is key. Sharing sanitised technical information, such as compromise indicators or details on how weaknesses were exploited, allows entities to maintain current defences and stay abreast on emerging methods used by attackers.

This allows organisations to move from a constantly reactive state to begin adopting a more proactive approach to reduce vulnerabilities. Organisations and public authorities such as law enforcement or regulatory bodies such as the information regulators should identify and address impediments to information sharing.

Performance Measurement

"If you cannot measure it, you cannot improve it". A critical requirement for any cyber security programme is verifying the effectiveness of established controls. At regular intervals, organisations should evaluate their security controls to determine whether they are operating as intended.

There are several processes to monitor information risk control performance and effectiveness:

1. Establish and regularly review security metrics
2. Run vulnerability assessments and red team tests to ensure controls are effective
3. Conduct an internal audit or independent assessment to evaluate overall cyber risk management.

Monitoring and Threat Intelligence

Connecting your organisation to cyberspace makes it vulnerable to the full spectrum of global threats.

Without constant monitoring, you have no way of knowing when you are under attack.

Establish systematic monitoring processes to detect reconnaissance scans, attempted intrusions and actual incidents and periodically use this valuable information to evaluate the effectiveness of controls.

Subscribing to external threat intelligence feeds is another method of gaining insight into updated techniques used by threat actors or new malicious software strains.

Incident Response

All the previous elements focused on implementing preventative and detective controls which help to improve the maturity of an organisation's defences.

It is, however, not possible to deter every attacker or successfully block all malicious activity. Based on the premise that "it's not if but when you have a major incident", it logically follows that the organisation should have an incident management framework in place. Incident management preparedness begins with maintaining a business-aligned incident response plan and a skilled incident response team.

Recovery and Resilience

Should all previous controls fail, the organisation is left with no other choice but to implement business continuity management. Once business continuity and disaster procedures are invoked, operations are stabilised and information integrity is assured, prompt and effective recovery of full critical business systems may commence.

This should be based on prioritisation of critical business areas and systems in accordance with objectives set by prior planning sessions with senior management.