CyberPrism

Fully Comprehensive Cyber Security Risk Assessment

- Cyber crime is the fastest growing crime in Ireland and globally
- CyberPrism addresses the threat of cyber attack
- The most comprehensive, cost effective cybersecurity service available

- Calculates the cyber inherent risk based on your business model
- Produces a cyber risk rating
- Measures cybersecurity controls in place
- Identifies any gaps in IT security controls
- Provides a fully comprehensive cyber risk assessment report
- Provides a roadmap to address any issues identified

Capital ISS
Capital ISS Linked Solutions

Email: info@capitalissgroup.com Phone: 01 6877095

Cyber Threat Overview

The statistics surrounding cyber related crime in Ireland and globally are very stark. According to the most recent economic crime research carried out by PWC more than one in three Irish organisations (34%) experienced such crime within the last two years, up from a quarter (26%) two years ago.

The research also found that cyber attacks experienced by Irish organisations have almost doubled in frequency since 2012. The cost of these attacks is considerable with nearly one in five (18%) of those affected incurring losses of between €92,000 and €4.6 million as a result.

"It is estimated that less than 5% of Cyber Crime is reported to the Gardai."

"Cyber crime losses amount to almost 1% of Global income."

The global statistics are even more stark with the European Commission estimating global financial losses due to cybercrime at €350 billion a year currently and rising to €1.9 trillion by 2019. Furthermore, the Commission believes that cybercrime has already led to the loss of 150,000 jobs across the EU.

Indeed, such is the growing prevalence of cybercrime that many companies are now recording the ransoms paid as a business expense in their accounts. Cybercrime presents a number of challenges for management and accountants, who must ensure that cybersecurty risks are fully assessed and mitigants put in place.

What is CyberPrism?

CyberPrism is the innovative method of conducting a cyber risk assessment and report on your business, which will assist in protecting your organisation against cyber attack through the following:

- We provide you with a self assessment software package, which consists of multiple questions. We make this assessment as easy as possible by providing yes/no or multiple choice questions.
- When all questions are completed, we supply you with a fully comprehensive cyber security risk assessment report.
- We arrange a meeting to discuss the report. We then provide you with an executive summary and assist you on the path to compliance.

What are the risks of cyber crime?

- Cyber crime presents a number of challenges for accountants. Management and accountants who have a responsibility to protect their organisations from economic crime generally and cybercrime in particular, while accountants in practice must protect their clients as well as their own firms.
- You can be targeted from any part of the world.
- Consequences can cause major damage to your business, both reputation and financial.

What are the benefits of CyberPrism?

- Identifies gaps in IT security controls and provides you with a cyber risk rating.
- Provides you with a road map to address these gaps.
- Cost effective, easy to use solution.
- Comply with regulatory and legal obligations.
- Support other functions such as the Enterprise Risk Managment (Privacy, Compliance, IT and Legal).
- Supports managment in making informed decisions based on understanding current inherent cyber risk.
- Provide peace of mind for clients, vendors, shareholders and other stakeholders.
- Gain evidence and assurance for third-parties (including regulators) in relation to cyber risk status.
- A strong status can be a differentiator in winning and maintaining business.
- Develop strategy and budgets for future business plans and objectives.

Frequently asked questions

Q. *Why do I need CyberPrism?*

A. Most businesses feel that if they have their networks assessed and their firewalls in place, they are protected. This simply is not true. Cybersecurity relates to every area of your business, for example suppliers, invoicing, payments etc. CyberPrism analyses each area of your business.

Q. *We have our own IT person/department, why do we need CyberPrism?*

A. Cybersecurity is far more than IT systems and infrastructure. CyberPrism is a support to your exisitng IT person/department. It analyses your entire business to identify any potential cyber risks and provides the mitigants to address these risks.

Q. *We have spent a lot of money on IT system upgrades, does this make us compliant?*

A. Unless your business has completed a cybersecurity risk assessment, you will not know the extent of your business vulnerability. As a result you may not be utilising your IT budget effectively.

Q. *My IT provider looks after penetration tests etc. Is this not sufficient?*

A. Penetration tests cover as little as 3% of what needs to be risk assessed in terms of cybersecurity.

Q. *My IT provider assures me that we are covered under cybersecurity, is this sufficent?*

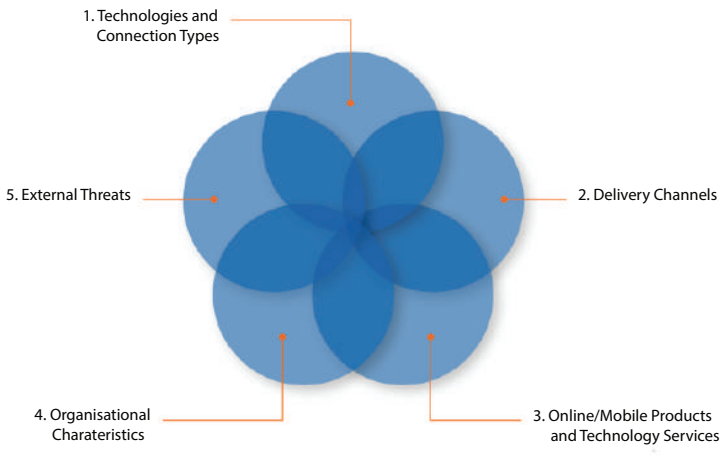
A. Look for written confirmation that your provider has carried out a fully comprehensive inherent risk assessment of your total IT security procedures and processes and get a copy of the full report.

Q. *I am happy that we are doing all we can regarding cybersecurity, surely this is enough?*

A. All elements of IT security must be fully assessed, with all risks and threats identified in the report provided. Managment are responsible for all cybersecurity matters. So while you can delegate, you cannot abdicate responsibility for cyber security.

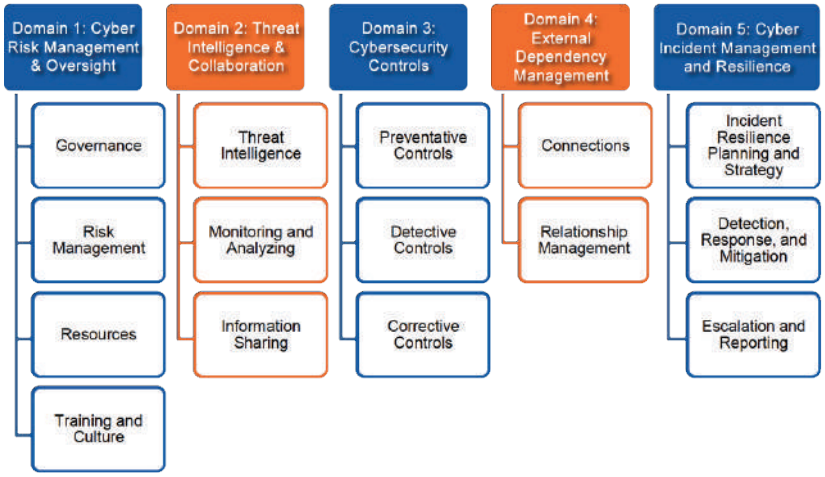
Cyber Inherent Risk Domains Calculated

Cyber inherent risk inludes the possibility that some human mistake, criminal activity or natural event will adversely affect an organisation's assets or customers. CyberPrism measures the inherent risk in a cyber environment across 5 different domains.

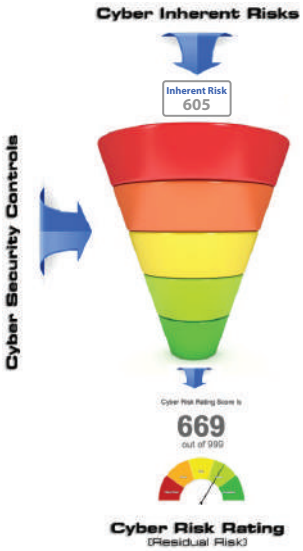


1. The organisations networks, software, third-party access and data storage systems.
2. Any channel that is used for communication, advertising and services e.g. website, mobile app etc.
3. Services such as debit cards, P2P payments, wire transfers and trust services.
4. Employee access to critical systems, changes to staff and the locations of branches and data centres.
5. Cyber attacks that can occur within an organisation e.g. network attacks and reconnaissance attempts.

Cyber Maturity Assessment Domains



CyberPrism Overview



- Identifies risks
- Easy to use
- Can be completed quickly and efficiently
- Cost effective solution
- Empowers management to make informed decisions
- Improves regulatory audits
- Supports IT security, risk and compliance functions

Summary Dashboards

CyberPrism evaluates the cyber security inherent risk of your business and the security controls that are in place. It then compares the two to assess where your business is in terms of it's cyber security. For example, if your business has a lower level of inherent risk, then the security controls in place should be within a baseline or evolving stage of maturity. CyberPrism provides a way to assess cyber threats and create a clear plan of action to increase the strength of it's cyber security maturity.