cutting through complexity

Testing Australian Cyber Security Practices

2015 Key Fears

DDoS Attack
DDoS
Ransomware
1 1 Ø 1 1 Ø Ø Ø 1 Ø Ø 1
Attack through cloud
SOFTWARE •••
1001100
010 101
010010
Malware and Exploits
7
1,496
Reputational Risk
Siloed Communication

Collective defence

The cyber security landscape is changing. The traditional reactive perimeter defence is making way for a proactive collective approach to security, in response to the large-scale cyber breaches in 2014. In addition, there has been an uptake in collective defence, characterised by:

- the proactive cross-industry sharing of intelligence
- comparative analysis of threat data to enable prediction of risk, and
- development of models to hinder malicious actors.

It moves away from the traditional fear of exposing company weaknesses, and moves towards collaboration between other organisations and stronger intent to share data. Whilst application of this model would improve cyber security, it is challenged by:

- increased risk of information leakage
- lack of interoperable standards
- validation of data quality and reliability, and
- legal and data confidentiality requirements.

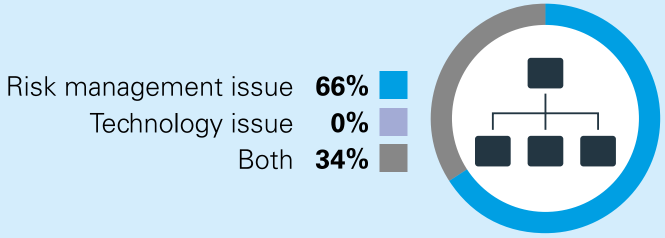
Currently, Australian organisations are divided on collective defence.

Approximately half of organisations are conducting collective defence.

50% collective security

This is the proactive sharing of intelligence between organisations in an effort defend better against cyber criminals.

Is cyber security a risk management or a technology issue?



33% of organisations estimate the risk posed by their supply chain high. This is due to the inability to identify weak links until it is too late, combined with the new technologies employed by other organisations in the supply chain.

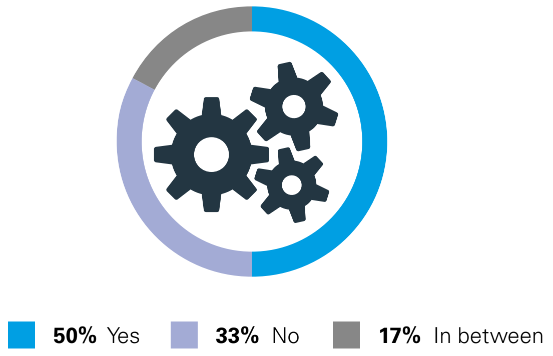
Threat Intelligence

An intelligence driven security approach should foster the development of a proactive, information-sharing model. This model should enable analysts and security experts to identify threats, purpose, intentions, and weaknesses in security in an effort to hinder emerging risks.

The current challenge in creating valuable intelligence is that it needs to be actionable, enabling clients to combat malicious actors. Its merits are derived from how a company incorporates cyber threat analysis into their existing work flow. Threat intelligence is commonly misunderstood, incorrectly labelled as a non-essential part of security practice or not utilising existing tools properly to successfully integrate threat intelligence into current security risk models.

The observed challenges within intelligence driven cyber security means that organisations are still in the process of changing, ranging in terms of progress from exemplary to limited intelligence incorporation.

% Organisations creating actionable intelligence



The primary challenges to incorporate threat intelligence are:

- Inconsistencies in definition of intelligence across peers in the industry and internally. We are commonly seeing intelligence being confused with information data, which leads to organisations being inundated with raw and unfiltered data.
- Not having access to an adequate scope of information to assess the threat and produce solid actionable intelligence.
- Lack of trained cyber analysts.
- Ineffective use of technology through a lack of training, no emphasis on its value and lack of incorporation into existing security practices.

Insights to mitigate these challenges:

- Investment in research and development (R&D) initiatives to enable cyber security researchers to play a larger role in designing security software and practices.
- Training of cyber analysts to filter information and create actionable intelligence.
- Incorporation of specifically designed technology into cyber intelligence and training analysts in its use.
- Further development of collective security practices and models, shared between industry peers to provide a larger scope of intelligence to organisations.

Contact us

Gary Gill
Partner
Advisory
+61 2 9335 7312
ggill@kpmg.com.au

Mark Tims
Partner
Advisory
+61 2 9335 7619
mtims@kpmg.com.au

Stan Gallo
Director
Advisory
+61 7 3233 3209
sgallo@kpmg.com.au

Tim Miller
Director
Advisory
+61 2 9455 9182
tjmiller@kpmg.com.au

kpmg.com.au

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Liability limited by a scheme approved under Professional Standards Legislation.

July 2015. NSWN12995ADV.