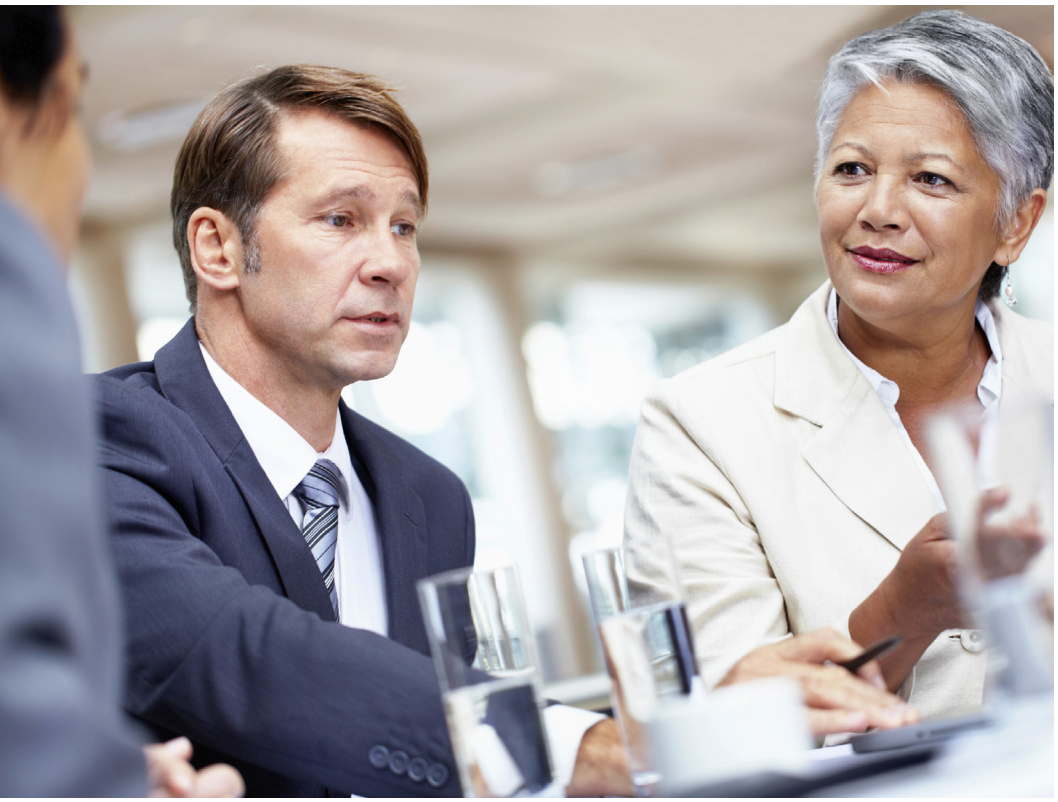
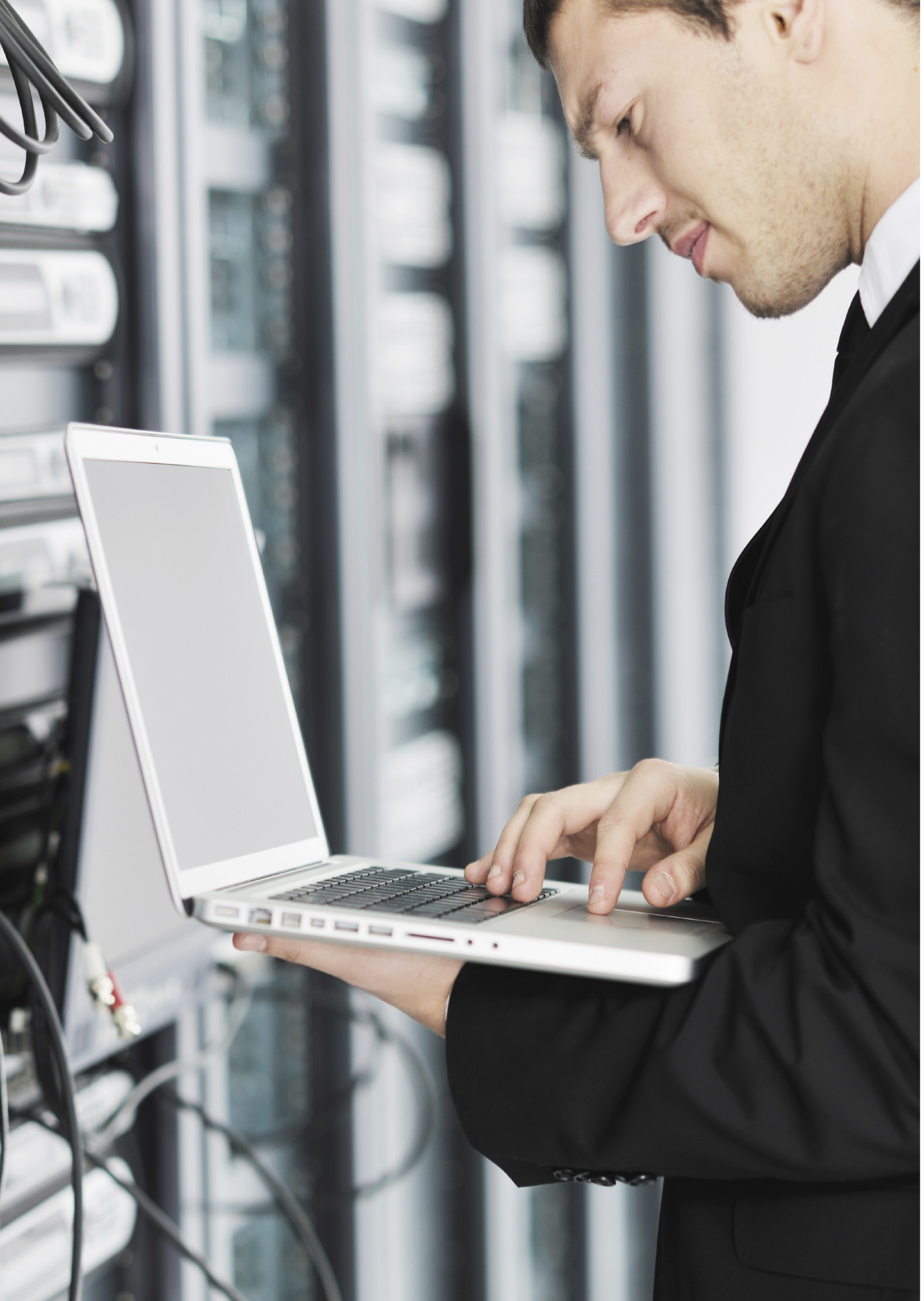
Cyber Risk – Enlightenment through information risk management



pwc

www.pwc.com.au



Cyber Risk – Enlightenment through information risk management

Managing cyber risk in a way that makes sense to everyone in the organisation by using a meaningful information risk management framework

Imagine you're discussing cyber risk with the Board Audit and Risk Committee. There's a story in the morning news about another major corporate hack. Everyone's a bit on edge.

The presentation goes something like this: "So here's our cyber risk in business dollar terms, here's how far off it is from the organisation's risk appetite, and here's the investment we're asking for to treat the risk."

Sounds good, no? Unfortunately, it's unlikely the meeting would go as smoothly as this.

In Australia, cyber risk is often not well understood, often represented in inconsistent ways, and highly subjective. It's one area of risk that's yet to be translated from 'geek speak' to the language of senior management and boards.

A recent ASX* survey of Australia's Top 100 organisation showed that Australia's boards still don't have the visibility they need to manage this growing and complex issue effectively. For instance, only 11% have a 'clear understanding of where the company's key information or data assets are shared with third parties.'

Now, more than ever, organisations need a better way of identifying, analysing, quantifying and communicating cyber risk at all levels. Too often conversations are bogged down in technical details or debate about whether a risk is high or low. Critical questions about how best to manage the risk get overlooked.

Technicians, risk managers, executives and directors all need to be on the same page about cyber risk. Only then will companies be able to develop and resource appropriate treatment options.

This paper provides a framework for doing just that. It explains some of the common misunderstandings about cyber risk, the critical principles for developing a robust information risk management framework based on metrics – not subjective assessments, and key questions to ask to check whether your current approach is up to scratch.

*ASX 100 Cyber Health Check Report

Get your definition right

Let's start with the basics. A common challenge for organisations is the fact that "cyber risk" has never been clearly defined. As a result, identifying the extent and nature of the risk, who's accountable for it, and the ways it needs to be analysed and messaged becomes a maze in itself.

Here's a succinct definition that should make sense to people at all levels in the organisation:

Cyber risk is any risk associated with financial loss, disruption or damage to the reputation of an organisation from failure, unauthorised or erroneous use of its information systems.

Examples of cyber risks to the business include cyber-crime, cyber-terrorism, accidental loss of confidential data, as well as liability for an organisation's online activity.

To put it another way, cyber risk is the probable frequency and probable magnitude of future loss that relates to an organisation's information systems and associated assets, both physical and informational.

Understand what you're protecting

The next step – and possibly the most important – is to understand what it is you're trying to protect.

For most organisations, this is typically some form of information asset, as well as the systems that support it. But in some industries, the key asset could well be physical infrastructure.

In the world of cyber risk, too often the focus is on the 'threat' itself rather than the target of the threat – the organisation's asset. But without a clear focus on the asset that the risk relates to, risk management doesn't make much sense.

Knowing the asset you are trying to protect, where it's stored and who has access to it – is fundamental to effective data governance and management. It's the starting point for cyber security: everything else builds from there.

Put the right controls in place

Once you've identified the asset you're aiming to protect, you need to ensure that the appropriate controls are in place to either minimise its vulnerabilities, decrease the likelihood of the threat, or minimise the impact of a loss if the risk is realised.

It's important to recognise that while controls are taken into consideration in the analysis of cyber risk, a lack of, or deficiency in, a control is not a cyber risk in itself. For example, it's not uncommon to see risk entries such as "Networks IPS signatures not updating" as a form of cyber risk. Even though this problem may well increase the likelihood or impact of a risk being realised, it should be reviewed as part of the risk analysis, rather than considered a stand-alone risk.

Capture it in the formal risk register

It might come as a surprise to know that cyber risks are often not captured in a formal risk register. And when they are captured, they're frequently relegated into an operational IT-style register, which records the technical aspects of the risk and is mainly intended to benefit the technical community within the organisation.

All cyber risks must be captured and monitored in the organisation's risk register and given the same level of focus as any other risk.

Risk or threat?

Often fuelled by public incidents and breaches, organisations sometimes incorrectly refer to cyber threats as cyber risks – adding to the confusion about the representation of risk. So what's the difference?

A cyber threat is an event where an asset may be harmed, typically due to a vulnerability relating to the asset. Only when a plausible cyber threat is mapped to an asset does it become a cyber risk.

Quantify risk – in business terms

One of the major barriers to managing cyber risk effectively is the fact that it's often not translated into language that allows executives and the board to gain a meaningful appreciation of the risk or its potential impact on the business.

This is compounded by the way cyber risk is measured, which is typically based on qualitative models like High-Medium-Low, Red-Amber-Green, or a rating of 1 to 8, etc. These models, despite their simplicity, have some drawbacks when it comes to cyber risk:

- They are subjective in nature and open to interpretation (e.g. one person's High may be another's Medium)
- They cannot be easily aggregated where a holistic view of cyber risk is required (e.g. 10 x Amber + 5 x Red risks equals what overall level of risk?)
- They are difficult to prioritise (e.g. which High is highest?)
- It's hard to determine the actual effectiveness of controls (e.g. we spent $x on these controls to reduce a risk that was High, but even though the money was well spent the risk is still High)
- When treatment options involving the transfer of risk are required (the increasingly popular option of cyber insurance), qualitative models do not provide enough guidance as to the level of coverage required
- It's difficult to align qualitative ratings to the organisation's actual risk appetite, which is generally expressed in financial terms.

Effectively communicating cyber risk to key executives and the board requires framing it in a way that aligns to business imperatives. This means translating into dollar terms.

Qualitative	Quantitative
"The risk of a Distributed Denial of Service is High."	"We are confident that should the risk of a targeted and malicious Distributed Denial of Service affecting our core Internet facing sites be realised, the annual loss exposure would range between $800k to $1.2M."
"We know this because while the likelihood of the threat occurring is low, the impact to the organisation if it were to be successful is High."	"We know this because the combined aspects of productivity and reputation loss for the average number of times this risk could occur through a given year equates to the above loss range for the business."
"We have some network security controls in place, but we don't believe they would be effective as controls to stop the threat."	"The organisation's risk appetite as it relates to our public facing Internet sites is $150K (or a maximum outage window of 15 minutes). We can reduce the current assessed risk to align with the organisational risk appetite through the application of appropriate process and technology controls which will require an annual investment of $200K."
"We need to reduce the Risk by acquiring some specific DDoS controls to reduce the risk from High."	"That is, through investment, implementation and ongoing governance of the controls to manage this risk, we believe we can demonstrate an average Return on Security Investment of approximately 4 times."

Take for example the statements above about a common cyber risk scenario. One is based on a qualitative risk assessment, the other on a more robust quantified risk analysis.

Quantification removes a large amount of ambiguity and subjectivity from the assessment of cyber risk. While it doesn't guarantee that the analysis will be accepted by all parties without debate, it does allow for a robust conversation about the variables that were used to derive the quantified output

Other benefits of using an effective information risk management framework that has a quantitative based approach to cyber risk analysis include:

- Aggregating risk by asset type, threat type, organisational area, etc. so a holistic view of risk can be obtained
- Prioritising risk based on quantified loss values as opposed to trying to figure out how to prioritise 15 "High Risks"
- The ability to determine the effectiveness of controls based on the required investment
- The ability to monitor trending of the quantified risk – especially as the risk is being treated on an ongoing basis.

Incorporate Threat Intelligence, but don't solely rely on it

There has been a lot of noise recently about the importance of threat visibility and threat intelligence as the new means to address cyber risk.

These capabilities, which provide early detection of potential threats, are an important means of enhancing the analysis process as well as providing ongoing governance. But if they are not applied through the lens of an information risk management framework, the risk cannot be effectively treated. It would be like having the most up to date and accurate weather forecast but not really knowing where you're going, why you're going and what you're going to be bringing with you.

For threat intelligence to be effective, threats need to be modelled to the key organisational assets. Once this has been done, the intelligence is immensely beneficial to provide timely detection and validation of the metrics used in the risk analysis.

Ongoing risk visibility, reporting and governance: the Cyber Risk Scorecard

Once a quantification model has been successfully adopted in an organisation – and cyber risks are now well understood, quantified, tracked and have a robust treatment plan – the next question from executives and boards typically is: "Well, how effectively is the risk being managed?"

It's a fair question. And one of the most effective means of answering it is through a Cyber Risk Scorecard. The scorecard provides a current, reliable and easy method for communicating the state of risk governance. But it's important to get the metrics right.

Most often, risk managers use Key Performance Indicators on their scorecards. However, for risks to be monitored (both lead-risks and lag-risks) and to determine whether the risks are being effectively managed, three perspectives need to be applied: Key Performance Indicators, Key Risk Indicators and Key Control Indicators.

These three types of indicator are interrelated and don't necessarily require three times the effort. Rather, each provides a particular perspective supported by a set of metrics to help the organisation understand: Are we achieving what we set out to (KPIs)? Are we functioning within an acceptable level of risk and do we know if we are deviating from it (KRIs)? Are our internal controls effective in moving us in the right direction (KCIs)?

Which metrics are used under each category, how they are derived and how they align back to our overall perspective of risk is critical. The risk quantification methods identified in this framework provides the context for which metrics are required and how they can be correlated to effectively report on both cyber risk and how its governance is supporting key organisational performance objectives.

Taking the next step

If you're considering whether you need to develop – or update – an information risk management framework, ask yourself whether you can answer these core questions:

- What are your top 10 cyber risks based on priority?
- What is the actual impact (loss) to the business if these cyber risks were to be realised?
- How are these cyber risk impacts aligned to the organisation's risk appetite?
- How effective are the controls in place to treat the identified cyber risks?
- How are cyber risks governed on an ongoing basis to ensure treatment is successful?
- How are cyber risks communicated to the exec and board so they clearly understand risk impact, ownership and governance?

If not, you might want to think about how you can evolve the existing risk management approach in your organisation.

But where to begin? Start by assessing your current risk management framework and how cyber risks are identified, analysed and articulated. Is it in a way in which stakeholders outside of Information Security understand?

Take two or three important risk items – or ones that are challenging or ambiguous – and attempt to apply a quantitative information risk management analysis approach to determine whether the risks are well analysed and the impact is meaningful. We recommend the use of FAIR (Factor Analysis of Information Risk) as the basis for this.

And what do you stand to gain? An information risk management framework with quantitative analysis may not solve all your cyber security problems, but it will ensure that:

- The organisation's cyber risk has been captured in alignment with key assets of importance that align to the organisation's strategic and business imperatives
- The risks relating to those assets are not just understood but are quantified and aligned to organisational risk appetite
- The effectiveness of existing controls can be measured, and appropriate investment can be justified to treat the risk in alignment with risk appetite
- Quantified risk that cannot be managed internally can now be more easily transferred (cyber insurance) as the amount of risk that needs to be transferred is well quantified.

And if you're typical of most Australian businesses, that's likely to be a significant improvement on the way cyber risks are managed today.

"An information risk management framework should be viewed as an investment that pays big dividends over time in terms of a more clearly defined risk landscape. I would also argue that without this effort, an organisation stands a much better chance of overlooking important parts of its risk landscape. This process also improves an organisation's ability to explain/defend the risk management choices it makes."

– Jack Jones,
Creator of the Open Group,
Open FAIR Standard

For further information on how PwC can assist your organisation please contact:

National and Melbourne

Peter Malan
Partner
03 8603 0642
peter.malan@pwc.com

Jason Ha
National Lead, Information Risk Management
Director
03 8603 0266
jason.ha@pwc.com

Adelaide

Kim Cheater
Partner
08 8218 7407
kim.cheater@pwc.com

Brisbane

Ryan Ettridge
Partner
07 3257 5373
ryan.ettridge@pwc.com

Canberra

Shad Sears
Partner
02 6271 3438
shad.shears@pwc.com

Perth

Volven D'Souza
Director
08 9238 3174
volven.dsouza@pwc.com

Sydney

John Hines
Partner
02 8266 0379
john.hines@pwc.com

www.pwc.com.au

127050203