blueCentral™

A BlueCentral Whitepaper

Risk management: ensuring the security of your hosted information

By Simon Oliver, General Manager Clients and Strategy, BlueCentral
with Kevin Fitzgerald, Principal at Fitzgerald InfoSec

Contents

Data security

Data security is a current global issue and there's no question that all businesses are at risk in some way or another. Recognition of and a proactive approach to managing a company's security risk needs to be a part of today's standard business management practices.

Technology is an integral part of the way we do business. We live and work in a global economy and our customer base is the rest of the world, no matter where we're physically based or the hours we "officially" work.

Organisations of all sizes are becoming victims to cybercriminals, data breaches, information theft and security risks. But before you go out and spend a fortune on security software, solutions and consultants, the starting point is to identify and measure your business's exposure to those risks. That's the first big step in the battle.

While measuring risk exposure is not an exact science, establishing a consistent measurement tool will enable the discussion of results with a common understanding. It allows organisations to have the conversation and acknowledge the risk by bringing it out into the open. That's another significant step. Too many businesses take the "it won't happen to me" approach and pretend the risk doesn't exist, but don't be fooled – denial is the enemy!

BlueCentral, in conjunction with Kevin Fitzgerald, a 30 year veteran on Information Security, have teamed to co-author a three-part series on Risk Mitigation Strategy. As a hosting provider, it is critical for us to ensure that not only our systems but our customers' hosting systems and solutions meet the wide range of criteria required by Australian Standards. These include areas such as compliance with data privacy standards, the highest information security levels, and the reassurance for customers that the systems on which their data is hosted are reliable, scalable and robust enough
to repel any threat.

In this first paper, **"Exploring, Identifying and Measuring"** risk, we examine how to identify risk and share an approach for identifying and measuring risk in your organisation.

Identifying, recognising and measuring risk

When establishing a risk management strategy for your business, there are a few standard principles to adhere to, for ensuring the best outcome for your business. The Risk Management strategy should:

- create and protect value
- be an integral part of all organisational processes
- be part of decision making
- explicitly addresses uncertainty
- be systematic, structured and timely
- be based upon the best available information
- be tailored to the organisation's context and risk appetite
- take human and cultural factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- facilitate continual improvement.

How to establish a risk profile

One methodology that has been used since the 80s to help organisations understand their risk exposure profile is based upon a simple spreadsheet, where Threats are in columns and Assets are in rows (see figure 1 as an example).

Threats should be grouped into the following three areas:

- Information Confidentiality: for example physical theft, physical loss, logical theft
- Information Integrity: for example fraud and embezzlement, errors and omissions
- Information Availability: for example natural disaster, hardware damage, power failure.

Assets typically include areas which are vulnerable to any of these potential security threats. For example: databases, server rooms, paper files, laptops, email assets and website content.

The information inserted into this spreadsheet should be based upon workshops or discussions with operations level managers who are guided to:

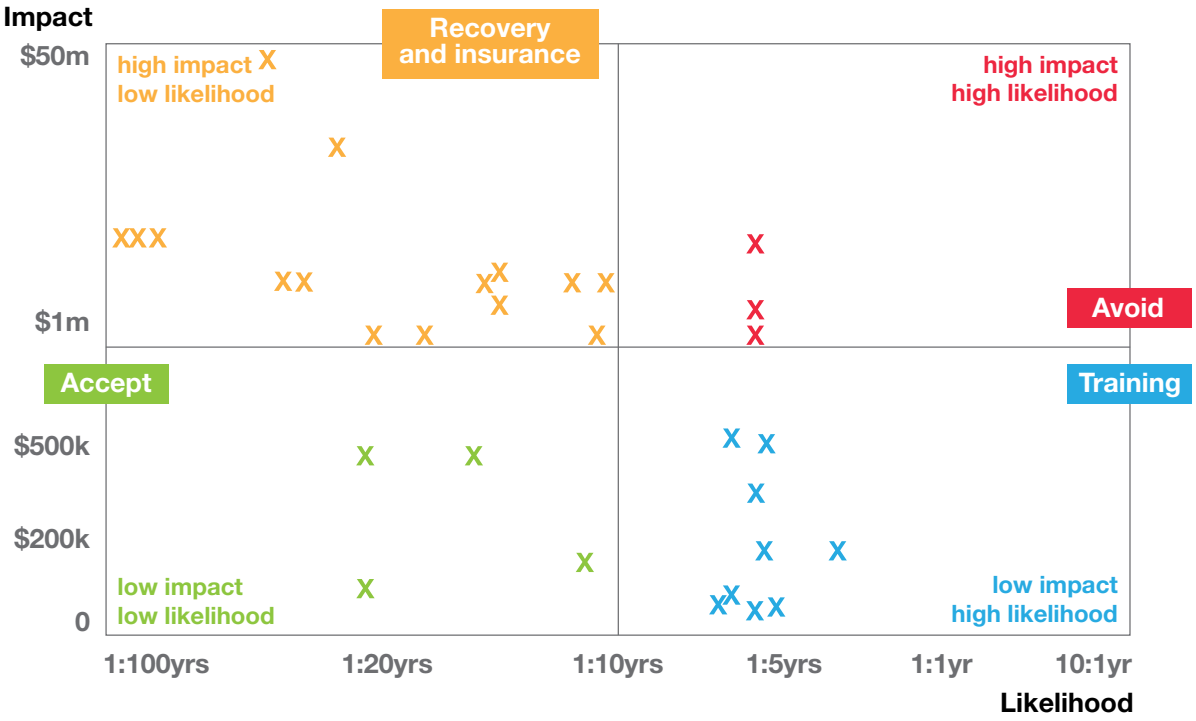
- Identify potential and existing threats to business assets
- Use approximation tables to identify the likelihood and impact of each threat. For example, a threat may be approximated as a likelihood of once every 10 years (1:10 years) and an impact of $1 million
- Create annual risk exposure (ARE) costs for each threat over each asset. Using the above figures 1:10 yrs and $1 million would result in a $100k ARE
- When all cells in the matrix have their AREs calculated each row and column should be totalled and sorted into descending order. This will provide the company's Threat Exposure Profile via the column totals and the Asset Vulnerability Profile via the row totals.
- Businesses can then create a scatter diagram (see Figure 2 below) from which to define a Mitigation Strategy which is then used to apply a mix of appropriate controls to address the exposures recognized.
- Finally, the company needs to establish a Risk and Mitigation Register to monitor and manage the risk.

This exercise may be simple in some cases, but much more complex for other organisations or government departments. But it's necessary to establish and identify the risks. This process also gives rise to a Risk Committee with auditors and managers discussing risk within a conversation that they all can understand and acknowledge.

Figure 1:

Threats	Confidentiality		Integrity		Availability		Total ARE p.a.
Assets	**Theft (c)**	**Loss (c)**	**Change (I)**	**Errors (I)**	**Fire… (A)**	**DOS attack (A)**	
Product Database	1:10yrs $100k $10k pa	1: 20 yrs $200k $10k pa	1: 40 yrs $1m $25kpa	1000:1yr $50 $50kpa	1:100 yr $2m $20kpa	1:5 yrs $1m $200kpa	$315k
Server Room	1:20 yrs $100k $5k pa	Not applicable	1:20 yrs $1m $50kpa	20:1 yr $1k $20k	1:100 yr $2m $20kpa	Covered in row 1	$95k
Paper Files	10:1yr $1k $10k pa	2:1yr $1k $2k pa	1:10 yrs $30k $3kpa	10:1yr $1k $10kpa	1:100 yr $500k $5kpa	Not applicable	$30k
Laptops	2:1 yr $100k $200k pa	1:1 yr $50k $50k pa	1:5yrs $5k $1kpa	Covered in row 1	Inconsequential	Covered in row 1	$251k
Email	Covered in row 1	1:20yrs $100k $5k pa	Not applicable	Not applicable	Inconsequential	Covered in row 1	$5k
Website	1:2 yrs $100k $50k pa	Covered in row 1	Not applicable	Not applicable	1:100 yr $2m $20kpa	1:5 yrs $1m $200kpa	$270k
Total ARE p.a.	$275k	$67k	$79k	$80k	$65k	$400k	$966

Figure 2: Risk Scatter Diagram



A Risk Profile

A Risk Profile moves an organisation into a proactive approach to security, which is the best position from which to address threats.

The information security landscape is changing rapidly, with:

- The proliferation of storage-rich mobile technology – everything is at our fingertips, but is it secure?
- The gen-Y (and soon-to-be later generations) workforce who have grown up with technology – they want it now, but is it safe to do so?
- Freedom of expression in social media – is what you're saying really being kept private?
- Convenience of working outside traditional office hours to suit an individual's lifestyle – how does this flexibility compromise the security of the IT system behind it?

No matter your generation or how you use the technology, the ownership of information does not carry the same clear accountability it once did when there were physical and behavioural boundaries and clear organisational leadership structures.

Having a Risk Methodology in place like the one above provides the opportunity for organisations of any size to recognise risk in the way business is conducted and transactions are recorded, captured and processed.

By going through the methodology process, companies may identify potential risk exposures that could happen in future – even if they're not a threat now. These can simply be added to the Risk Register for later measurement, which then provides an official avenue to register concern that can be assessed and controlled at a later date.

Standards

The above approach complies with the ISO 31000:2009 Risk Management – Principles and Guidelines certification standard.

The ISO 31000 standard claims that when implemented and maintained in accordance to the standard, the management of risk enables organisations to:

- increase the likelihood of achieving objectives
- encourage proactive management
- be aware of the need to identify and treat risk
- improve the identification of opportunities and threats
- achieve compatible risk management practices between organisations in the same supply chain
- comply with legal and regulatory requirements and international norms
- improve financial reporting
- improve governance
- improve stakeholder confidence and trust
- establish a reliable basis for decision making and planning
- improve controls
- effectively allocate and use resources for risk treatment
- improve operational effectiveness and efficiency
- enhance health and safety and environmental protection
- improve loss prevention and incident management
- minimise losses
- improve organisational learning
- improve organisational resilience.

This whitepaper brief is a consolidated paper taken from an extensive 65-page Information Security Risk Management project workbook. If you would like to receive the full workbook please visit www.fitzgeraldinfosecmentoring.com, email Kevin Fitzgerald at kevin@fitzgeraldinfosec.com.au.

About BlueCentral

BlueCentral is an Australian hosting company offering managed infrastructure and business-grade hosting services to private and public sectors. It guarantees high-availability of clients' services through active management of critical online infrastructure including networking, server, data storage and security technologies. The company has been delivering IT managed hosting services for 15 years and has over 150 clients across Australia and New Zealand. BlueCentral is an IPMG business, an integrated group of marketing services business with over 20 companies across print, digital and communications.

For more information, visit BlueCentral's website at www.bluecentral.com.

Contact us

Phone: 1300 258 323
Email: sales@bluecentral.com
www.bluecentral.com