5 REASONS ORGANISATIONS ARE STRUGGLING TO MANAGE CYBER RISK **AND WHAT TO DO ABOUT IT!**

Discussion Paper

Author: Karen Darling

September 2021

ROI Solutions

Introduction

Much has been said about Australia's vulnerability to cyber-attack.

Since COVID, and the move to working from home, the vulnerabilities have only increased. To quote Rachel Falk, CEO, Cyber Security Cooperative Research Centre "with heightened stress and anxiety surrounding COVID, people's emotions and stress have been exploited."

But, regulation, standards and other strategies to manage the risk are not new. And the number of organisations still struggling with risk management, is high.

We are way behind where we need to be.

So, in this discussion paper we unpack some of the problems.

Increased compliance requirements is not the only way to address the issues.

For organisations across sectors, there are several key challenges which are not being addressed now and could be.

We hope you find the information useful.

Reason 1: People risk is not being managed effectively (or, in some cases, at all!)

There have been many studies over past years which show clearly that "people risk" ie the risk of your technology users being the entry point for a cyber-attack, is the most important risk to manage.

So, let's get to why people risk isn't being managed. Mostly, it's because it's **hard**. Installing a piece of software which automates a process for risk management is, by comparison, easy. But, convincing users to be more aware, then to change their behaviours, is hard!

People are complicated. They may lack confidence in their ability to use or understand the technology they work with. Their reason for technology use may just be because they are required to use it for whatever role they work in. They may be completely disinterested in technology. They may also feel as though there is already enough to manage and be responsible for. COVID has just added to any pressure of work which was already there.

The problem is however, you can spend as much budget as you like and install technical solutions galore, but if you don't address **the biggest risk**, your people risk, you won't successfully manage cyber risk in your organisation.

What to do:

- Ensure your Cyber Security Strategy addresses your people risk sufficiently. Balance the activities required and the importance of managing people risk, back against the investment of time and budget you're making in technical solutions.
- And, see what to do about reasons 2 to 5 following...

Reason 2: The leadership is not engaged with IT, to enable the organisation-wide change required

Successful implementation of the strategy to manage people risk requires engagement and support from the Board and the leadership team.

Yes, cyber security is everyone's responsibility. However, ultimately the responsibility for governance rests with the Board, and responsibility for the day to day management of risk, with the leadership team.

But, you've been unable to get engagement because you're not being heard. Boards and leadership teams everywhere have limited time and budget, and extended lists of competing priorities.

To add to that there are still IT teams, who are not enabled much beyond day to day tactical work...so, just getting your message heard is difficult.

There also isn't detailed awareness. In some organisations cyber security is still treated as an IT problem rather than a business problem. The reality is that the risk of a cyber-attack is a key operational risk.

Technical understanding is low. Many Boards and executive leaders still have low technical knowledge and limited information about the way attacks can occur.

On top of all of that, transformation is driving many organisations to move to the cloud, without fully understanding the risks involved. The level of technical knowledge within the leadership, also affects whether cyber risk is being balanced with the rush to digital transformation.

What to do:

- Use a planned approach to secure engagement from your leadership team.
- Build awareness and discuss the biggest risk, the people risk, with your leadership.
- Create trust between IT and your leadership team and work with an influencer to persuade.

Reason 3: Policies and procedures required are not being updated and/or developed

Policy documentation and other written artifacts are the foundation to engage the help of users to manage cyber security risk.

They are the tools people need to access, to understand your organisational requirements and follow through with behaviour change.

Most organisations have a collection of documents written by a range of people using different styles and inconsistent language. Sometimes, the documents are also years out of date.

Leaders typically tell us they don't have staff with the writing skills, or the time, to create or update effective policies.

Documentation should be developed using a governance model to save time and streamline the task.

Some organisations also don't have the staff to understand and interpret compliance requirements to tailor an ISMS (information security management system). Documents based on a standard ie ISO 27001 should be tailored to your organisation's requirements. Otherwise, overly complex and lengthy documentation will not be adopted by users.

What to do:

- Ensure your governance model for documentation is well understood and adopted.
- Ensure your team have support for the task of writing.
- Provide your team with support to understand the compliance requirements and how to tailor policies and procedures to the relevant standards.

Reason 4: Good training hasn't been developed or purchased

There is some terrible training around and mostly it's "online" training; the default delivery mode used to address cyber security risks.

Most people – if you actually ask – don't enjoy online training, but organisations persist in using this mode for delivery. **Why?**

There are many reasons for deciding to invest in online training, one of which is that it's cheaper than other modes. Cheap could be ok if you still achieve your outcomes, but if not, **cheap is a false economy.**

Online training often focusses on referring to "compliance" requirements as the reason for learners to support the organisation to manage risk. Whilst compliance may be a motivator for people in certain roles...the reality is, that it is simply not a motivator for many.

All of these issues occur because the success of the training is not being measured and continuously improved.

Lastly, there are many other points to consider when developing or purchasing good training. But overall, it requires considerable thought, planning and business analysis.

What to do:

- Develop or buy training which is relevant to learners. That is, it's tied to something the learner knows, understands, and finds interesting.
- Ensure the training is tailored for your environment and culture.
- Measure and evaluate to assess the effectiveness of the training.
- Continuously improve the training content and/or delivery.

Reason 5: The strategy hasn't been implemented effectively

The Industry Advisory Panel in their report to the Australian Government for the 2020 Cyber Security Strategy commented, **"...stakeholders made it clear that the only good strategy is one that is implemented effectively."**

Any strategy to manage people risk is a major change initiative. The plan should include ongoing activities and repetition of training. We often see organisations which have not yet committed to compulsory training, and training is only delivered at the time of induction.

Therefore resources, ie the right people with the right skills, the right amount of time and actual budget dollars must be planned for, sought and approved each year to fund the ongoing work.

Australian Internet Security Association (AISA) research in the second half of 2020 showed **"A hefty 80% of infosec executives believed their organisations were under-resourced."**

This is a vicious cycle, if the strategy is not implemented effectively, budget may not be approved, at the level required, in the following years.

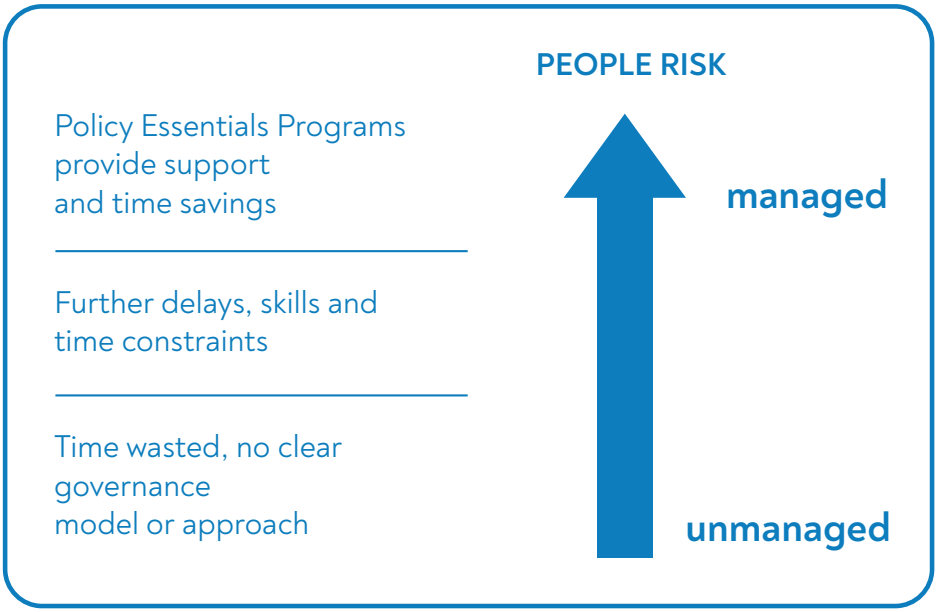
Also essential is leadership by example. If individual leaders are not seen to be changing behaviours and complying with policy, the whole strategy for risk management is undermined.

What to do:

- Treat implementation of the strategy as a major change initiative.
- Ensure the strategy includes approval for compulsory training and for training to be delivered regularly so that users benefit from repetition.
- Lead by example; promote cyber risk policies and be seen to comply.

How to manage people risk and achieve time savings

Everyone is busy and we often talk with organisations where leadership say "we've been too busy to make a decision about how to get our policies and procedures up to date." **Unfortunately, delaying the decision to manage the risk, means a decision is made to accept the risk!**



The model above shows the movement from unmanaged risk to managed risk through support for staff to progress the development and updating of policies and procedures.

Providing support also delivers immense benefits through time savings; staff work effectively to complete the documents when provided with an approach and mentoring.

Our Documentation Programs

Policy Essentials Programs

Level 1. We show you how to develop and deliver the documents
A brief and highly valuable program creating the foundation for effective documentation into the future. Includes our approach and governance document, review and 2 x training sessions.

Level 2. We help you to actually do the development and delivery
Upskill your team to develop and deliver effective documentation, retaining the skills in-house. Includes webinar, templates, 4 x one on one mentoring sessions and review of documents.

Level 3. We do the development and delivery for you
Retain our expertise to do as much of the work as possible. We work with your leadership team and subject matter experts from the discovery phase to implementation. Run over 3 months.

About ROI Solutions and Karen Darling

ROI Solutions provides services to support effective governance, reduce risk and meet compliance obligations for clients. Our focus is on cyber and information security risk.

Karen has more than 20 years' experience working with senior leaders and technical teams.

She is an accomplished consultant and mentor, and is passionate about organisations' managing people risk to successfully implement cyber security strategy.

Karen has deep expertise tailoring and developing compliance documentation and training to manage cyber security risks.

She delivers our Policy Essentials Programs with her team. The Programs are designed to provide a consistent approach for development of policy documentation and to support successful implementation.

See Karen's LinkedIn Profile ***https://www.linkedin.com/in/roisolutions-karen-darling/***

SOME OF OUR VALUED CLIENTS:

Federal and State Government funded organisations, Local Government, NAB, ANZ, Sydney Airport, Melbourne Airport, Adelaide Airport, Metropolitan Fire and Emergency Services Board (MFB), Coca-Cola Amatil, Coopers Brewery, Arnott's, Nestle Peters,
Victorian Aboriginal Child Care Association (VACCA), McMillan Shakespeare and AlfredHealth.

- Contact us at -

www.roisolutions.com.au

or email pcb@roisolutions.com.au

or 1300 264 946

ROI Solutions