CYBER SECURITY PRIORITIES AND INVESTMENTS WITH AN OUTCOME-DRIVEN APPROACH

2022 DISCUSSION PAPER

Up until recent years, Cyber Security wasn't at the top of executive agendas alongside more widely embraced matters such as GDP outlook, climate change, fiscal policy and EBITDA.

The complex nature of Cyber Security makes it difficult to embed into executive agendas, particularly for organisations that don't have the needed subject matter expertise at their disposal internally.

Further, the highly specialised nature of expertise surrounding Cyber Security makes it difficult for organisations outside of the industry to find and retain talent.

In combination, these factors are provoking doubt, fear and decision making inertia - causing executives and board members to develop overwhelming perceptions about Cyber Security.

To make matters worse, the growing market of profit-hungry providers promising to solve all cyber risks, through a single software or one-size-fits-all online training course, are gaining success at inducing vulnerable decision makers to expedite procurement processes and achieve, what is often, a false sense of security.

ABSTRACT

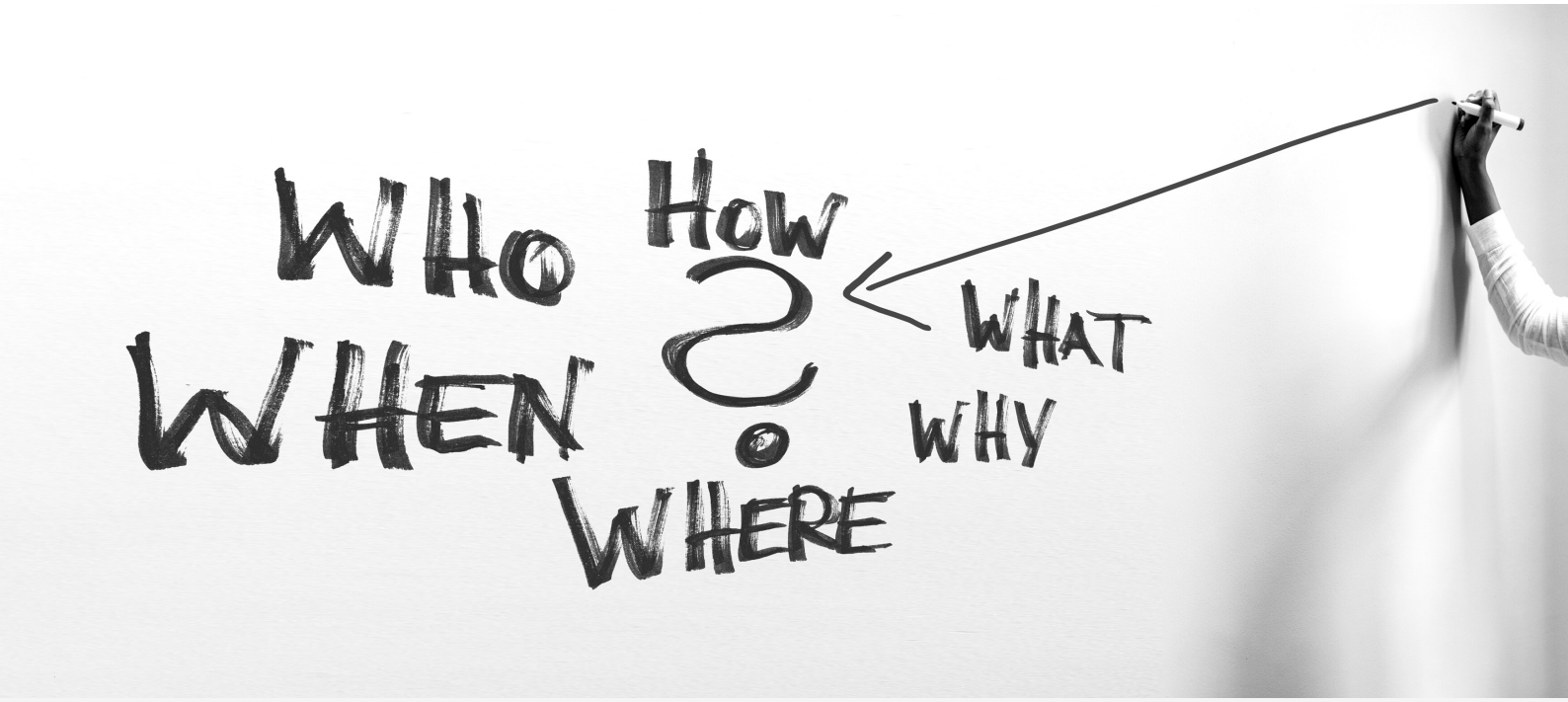
Readiness to detect, contain and respond to Information Security threats is measured by an organisation's state of Cyber Maturity. The Cyber Maturity journey requires strong leadership direction and sustained action - it's not a software procurement matter that can be left solely in the hands of IT departments or Information Security generalists.

An organisation's state of Cyber Maturity, at any point in time, determines its level of Cyber Resilience - which is the organisation's ability to recover from a cyber crisis when it happens.

We hosted a series of leadership discussions, for executives and board members, with 9 Cyber Security experts in Australia to unpack modern security perspectives and reflect on contemporary misconceptions.

This discussion paper summarises key insights shared by 9 Cyber Security experts including:

- Executive responsibility for preventable crises
- The Cyber Maturity continuum and building Cyber Resilience
- Navigating business risks at the speed of software
- Unique risks associated with cloud services
- Creating engagement through training and awareness
- TrustedImpact's Cyber Security Training and Awareness Program Pillars
- Limitations of Penetration Testing



THE BIG PICTURE OUTLOOK

EXECUTIVE RESPONSIBILITY FOR PREVENTABLE CRISES

From 2006 to 2022 the number of internet users has grown by more than 420%, reaching 5.2 Billion worldwide and netizens are more active than ever before. The ubiquity of the internet threatens traditional concepts of business security with no way of knowing how many netizens in different locations may be looking for windows of opportunity to do malicious things to an organisation and it's true malicious activity is often underway long before an organisation becomes aware.

> **It's okay to feel overwhelmed by all of this - previously executives didn't have to deal with these business challenges.**
>
> Damien Manual, Chairman, Australian Information Security Association (AISA)

Australian Institute of Company Directors (AICD) Director Sentiment Index Survey for H2 2021:

- **41% of directors say cyber crime and data security are front of mind in the small hours of the morning**
- **53% of executives believe their board has enough oversight over cyber threats**

In 2006 many security professionals were trying to have Information Security recognised as its own distinguished discipline instead of being bundled in the bowels of IT as a matter than many CIO's didn't even really understand.

Now, Information Security is most certainly a business challenge for executives and board members as evidenced by the executive stand downs we're already seen, including:

- Chairman and Chief Executive Officer of Target - 2014
- Chief Information Officer and Chief Security Officer of Equifax - 2017
- Founder and Chief Executive Officer of LandMark White - 2019

Whilst legislation might be young and, in some cases, pending - the Corporations Act already mandates punishment of executives and board members for preventable ransomware crises.

> **If executives and board members still don't believe this is relevant to them - all they need to do is ask those already stood down.**
>
> Tom Crampton, Managing Director, TrustedImpact

IT IS NOT BINARY, IT IS A STATE OF BEING

THE CYBER MATURITY CONTINUUM AND BUILDING RESILIENCE

Up until recent years, many were certain with the belief they could protect against digital risks. It is now widely understood and increasingly accepted, albeit reluctantly by many, that the requirement for an organisation to respond to a cyber crisis is not a matter of if but a matter of when.

Akin to how professional sports teams develop a plan and practice, organisations must do the same for digital risk management by having, among other things, an Incident Response Plan and practicing that plan - this is fundamental to resilience, which is the ability to recover from and continue operating in the event of a crisis.

Cyber Resilience isn't binary - it's not a yes or no. It's a state of being and a continuum. It is principles and risk based, measured in terms of maturity. An organisation's Cyber Maturity should improve over time continuously. Fundamentally, continuous improvement is the goal.

Cyber Maturity is not easy to measure and there are many indicators that can be considered, such as click rate in a Phishing email exercise, however single indicators are not a holistic or conclusive measure.

Digital risks are not solely the responsibility of technology to solve. It requires an organisation wide effort to manage digital risks across business units, teams, departments, systems, applications and geographies.

Ashutosh Kapse, General Manager Cyber Security and Technology Risk, IOOF Holdings Ltd

Does your organisation

- Allow someone without a visitor pass to walk through the building and do what they want?
- Diligently review user access profiles routinely to ensure user access is cut off as required?
- Empower and enable employees to minimise risk when switching between applications?

Cyber Maturity can only be achieved through organisation wide effort connected to a holistic, inclusive and enabling Cyber Security culture designed with maturity in mind and every person's behaviour and ways of working considered.

CONTEMPORARY THREAT LANDSCAPE

NAVIGATING BUSINESS RISKS AT THE SPEED OF SOFTWARE

The digital risk landscape continues to change rapidly and drastically - every day new threats emerge, particularly across cloud and software environments.

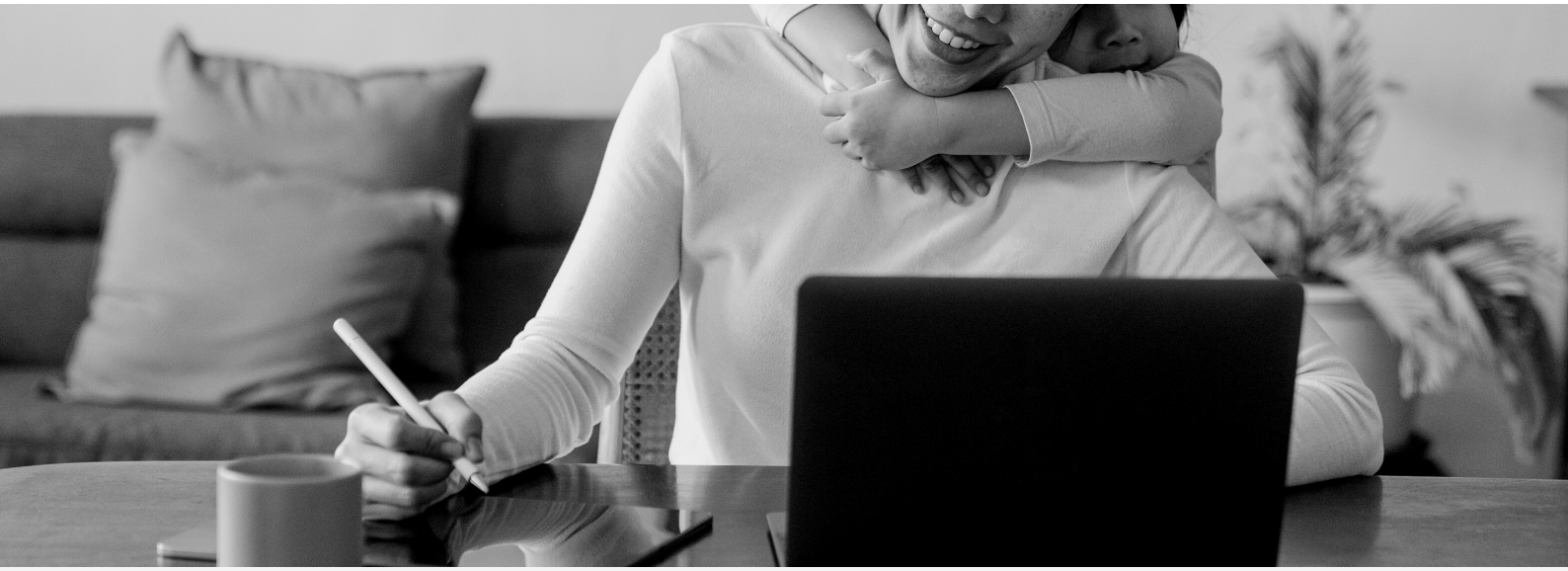
In conjunction with the stresses of the COVID-19 pandemic, we saw a rise in social engineering attacks, rapid growth of ransomware incidents and increased business email compromise (BEC) threats. These aspects of the threat landscape were exacerbated by foreign government attacks on organisations and commissioning of criminal syndicates.

> **Having a trusted advisor to provide guidance relevant to your organisation is crucial and executives should avoid software product purchases in reaction to the overwhelm.**
>
> Damien Manual, Chairman, AISA

Contemporary threats interact with each organisation uniquely and the ways in which executives and board members need to assess, manage and monitor threats and trends will vary.

Organisation attributes influencing how digital risks will be navigated include, but are not limited to:

- Risk appetite of executive committees
- Data exposure across systems and applications
- Sector and geographical spread of operations
- Types of information assets managed and or accessible



IT'S SIMPLY SOMEONE ELSE'S COMPUTER

UNIQUE RISKS ASSOCIATED WITH CLOUD SERVICES

The optionality and scalability of cloud services is highly attractive for modernising operations and unlocking customer and shareholder value. Information Security communities are known for saying "there is no cloud, it's just someone else's computer" because of the deceiving comfort often established by organisations as a consequence of adopting cloud services.

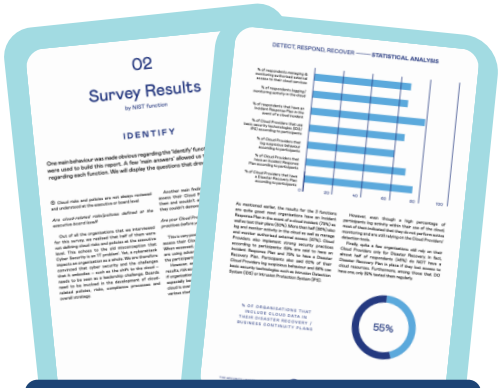
Generally, cloud services do offer substantial security benefit to, in particular, small to medium sized enterprises (SME) that historically haven't prioritised security - whether because of budget constraints or simply because it hasn't been considered a business challenge. However, SME's, as well as larger organisations, can't afford to ignore the unique risks associated with cloud services.

> **During our Cloud Migration Survey, 100% of organisations said they're embracing the cloud yet only 57% said they discuss cloud risks at the board level.**
>
> Tom Crampton, Managing Director, TrustedImpact

During TrustedImpact's 2020 Cloud Migration Survey of Australian organisations, 100% of respondents said they are embracing the cloud and reported 40% of the information and data moving to the cloud is sensitive.

Yet, 43% of the respondents reported their organisation does not discuss cloud risks at the board level.

Further, 80% of respondents believed their cloud provider(s) had Disaster Recovery Plans in place and 90% believed the same for Incident Response Plans, whilst nearly 60% didn't know if any plans have ever been tested to ensure they're actionable.



Click to access the survey

> **Often when I ask an executive if a service provider's Continuity Plan has been practised, they don't know, which is worse than having no plan.**
>
> Ben Scheltus, General Manager, Continuity Matters

Failure to test Disaster Recovery and Incident Response Plans creates a false sense of preparedness which ultimately puts an organisation and its executives at greater risk.

ENABLING A TEAM EFFORT

CREATING ENGAGEMENT THROUGH TRAINING AND AWARENESS

Cultural environments substantially influence how the people immersed in them behave which is why a strong Cyber Security culture, connected to a holistic Cyber Maturity plan, is fundamental.

Harnessing a right fit Cyber Security Training and Awareness Program will normalise safety and security discussions amongst the people within an organisation, which ultimately enriches the organisation's ability to successfully develop Cyber Maturity over time.

> **I frequently get stopped in the corridor by staff to let me know they have recognised a Phishing email exercise. And often, these staff are describing a real Phishing email, not a training exercise. This provides me with the opportunity to congratulate the person for recognising the real Phishing attempt. These interactions don't happen because we conducted one Phishing Test years ago - it's because we have a consistent program commitment to sustain this type of behaviour change and build Cyber Security awareness.**
>
> Tim Barlow, Director Technology Innovation, St Leonard's College

By helping each person to understand their role in protecting an organisation (subsequently themselves and their personal data) Security Awareness Programs achieve higher engagement and drive long lasting behaviour change. Using relatable training and awareness content enables people to connect what they learn to relevant areas of their personal and professional lives, resulting in skill development and a higher likelihood of changed behaviour day-to-day.

> **When people feel engaged in a program they retain information and contemplate the information. Plus we have also discovered people feel safe to raise security concerns they come across because they understand their role and the impact they can have.**
>
> Jasmin Krapf, Head of Security Awareness and Enablement, Bupa

THE 5 PILLARS FOR A SUCCESSFUL TRAINING AND AWARENESS PROGRAM

HOW TO CREATE SUSTAINED EMPLOYEE BEHAVIOUR CHANGE

1

Top Down Leadership

Executive sponsorship and evangelism of the key program messages are crucial to maintaining engagement and lasting behaviour change.

2

Reinforcement

Consistent repetition of information in digestible formats maximises engagement and retention, resulting in sustained behaviour change.

3

Operant / Instrumental Conditioning

Using rewards and remediation for behaviour creates associations between behaviours and consequences (whether positive or negative).

4

Measurement

Measuring trainee participation, completion and performance ensures improvement, because you can't improve what you can't measure.

5

Diversity

Accommodating different personality and learning types through various training mediums, gamification and content relevance.

> **Our methodology allows the organisation to embed Cyber Maturity practices, without friction, into daily routines for employees. We also measure performance throughout the program, which has proven to ensure improved and sustained behaviour change.**
>
> Charline Quarre, Research Analyst, TrustedImpact

RECOVERY READINESS

ROLE AND LIMITATIONS OF PENETRATION TESTING

Cyber crisis planning is quickly becoming an ordinary business challenge for executives to manage - with science fiction theories and concepts, from Hollywood films, about cyber space emerging rapidly as material and devastating real world possibilities for organisations of all shapes and sizes.

Cyber Security is not a technology issue, people and processes must be considered too. This is why Penetration Testing (Pen Test) can only fulfil a very specific set of needs within the overarching digital risk management strategy for an organisation.

> **In Cyber Security, your Pen Test team are a part of your offense - trying to find the holes in your defense that can be breached. Your Incident Response Planning teams, who should be practicing and exercising routinely, form part of your defense.**
>
> **If your organisation is only completing Pen Tests, whether routinely or irregularly, you're only committing to one aspect of the battle.**
>
> **In no way do Pen Test outcomes provide a holistic view of whether or not your organisation could recover from a cyber crisis - instead, they only provide you with a point in time view of how a cyber crisis could potentially start for your organisation.**
>
> Genio Maiolo, Principal Consultant, TrustedImpact

Following an adverse cyber incident, whether a data breach, ransomware attack or other, many organisations suffer from a second crisis because their communications weren't managed well. This is why board level planning is a critical practice to ensure the representatives likely to front the media are prepared and can minimise reputation damage when the time comes (because it will).

> **If your organisation has remote teams, whether domestically or internationally, all of those people need to be aware of how to notify their counterparts in response to a cyber crisis that may be localised. For example, in the event of a breach or attack, does your team in Australia know what and how they must notify the team in London? If these plans aren't ready, actionable and understood, your organisation could fail to contain an issue.**
>
> Ian McKenzie, Information Technology Manager, RightShip

Contributing Information Security and Cyber Experts

Managing Director, TrustedImpact - Research Analyst, TrustedImpact - Principal Consultant, TrustedImpact - General Manager, Continuity Matters - Head of Security Awareness, Bupa Health - Information Technology Manager, RightShip - General Manager Cyber Security & Technology Risk, IOOF Holdings Ltd - Technology Innovation Director , St Leonard's College - Chairman, Australian Information Security Association (AISA)

TrustedImpact
PROTECTING DIGITAL

BECOME PREPARED

THE IT DEPARTMENT CAN'T DO IT ALONE

TrustedImpact is one of Australia's highest regarded Cyber Security consultancy firms with more than 15 years experience helping organisations strengthen their Cyber posture.

Trusted by executives, TrustedImpact has an accomplished reputation for enabling its 300+ clients to establish robust security practices, develop Cyber Maturity to ensure resilience and operate with confidence in the digital age.

Click to visit website

TrustedImpact
PROTECTING DIGITAL

THE REBOOT SHOW